International

CIIP Handbook 2004

An Inventory and Analysis
of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

Critical

Information

Infrastructure

Protection

Edited by
Andreas Wenger and Jan Metzger

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, virtual, 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 was on the basis of these premises that the "Comprehensive Risk Analysis and Management Network" (CRN, www.isn.ethz.ch/crn) was launched in the year 2000 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 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 Protection and Emergency Planning (DSB), Norway,
- The Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland,
- The Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland.

The International Critical Information Infrastructure Protection (CIIP) Handbook is the product of a joint effort within the CRN partner network. The first edition of the CIIP Handbook, published in 2002, provided an inventory of national protection policies in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the US.

The 2002 Handbook proved to be such a success that it had to be reprinted soon after first publication. However, the need for an update had been generally recognized even earlier, a need that became even more pressing due to the dynamics in the field in the aftermath of 11 September 2001. This edition offers updates on the existing country surveys, additional country surveys, overview chapters on international protection efforts, legal issues, and current trends in research and development, as well as a more profound methodological section and more in-depth analysis in general. The expert base and the number of staff working on the Handbook were both expanded.

It is planned to include additional country surveys, models, and international initiatives in future updates of the CIIP Handbook. 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. Please see the front inside cover for contact information. The entire publication, with additional features, is also available on the Internet (http://www.isn.ethz.ch/crn).

The editors would like to thank the authors, Myriam Dunn and Isabelle Wigert, both researchers at the Center for Security Studies at the ETH Zurich (Swiss Federal Institute of Technology), for their efforts and their high-quality contribution to this important topic. Additionally, the editors would like to thank all the partners involved, in particular the national experts who generously shared their experience and knowledge with us.[1] We are looking forward to continuing the development and coordination of the CRN partnership.

Zurich, January 2004

Prof. Dr. Andreas Wenger
Director,
Center for Security Studies,
ETH Zurich

Dr. Jan Metzger
Senior Researcher, CRN Coordinator,
Center for Security Studies,
ETH Zurich

1 We also thank the following for their help in the completion of this project: Daniel Bircher and Stefano Bruno (Ernst Basler + Partners Ltd.), Christiane Callsen, Christopher Findlay, Myriam Käser, Reto Wollenmann, Marco Zanoli (Center for Security Studies, ETH Zurich).

Foreword

Dear Reader,

One of the most important lessons we can all learn about Critical Information Infrastructure Protection can be summarised in one word – interdependency.

We *depend* on our systems and networks. We *depend* on our staff. But, most importantly as professionals, we *depend* on each other. And that's why information-sharing is the key to the success of all our endeavours around the world.

At the National Infrastructure Security Co-ordination Centre (NISCC) for instance, we have developed a warning and alert system that highlights the latest vulnerabilities, and we also have a policy of ensuring responsible disclosure at the appropriate time.

This has only been possible by building trusted relationships right across the various sectors of our Critical National Infrastructure (CNI). We have also been able to enhance this work by conducting our own research – actively looking for problems before they arise. We already have strong international links. NISCC is an outward facing organization. My people have built effective working partnerships across the globe.

I am therefore delighted to support the second edition of the International CIIP Handbook and I would commend it to your libraries. In some circles it is regarded as the 'bible' in its field. I have seen it referred to in research work. Among many CNI professionals, it is considered essential reading, providing an invaluable guide to the international scene.

Whether you view CIIP from government, academia, or the private sector, it has something to offer.

Before closing, I'd like to mention that NISCC is currently developing an International CIIP Directory, based on G8 CIIP Experts' initiative. It will be linked to the Handbook. For more details please email ciip-directory@niscc.gov.uk

Stephen Cummings, Director NISCC
www.niscc.gov.uk

Abbreviations

ABMS	Agent-based Modeling and Simulation
ACIP	Analysis and Assessment for Critical Infrastructures Protection (Germany)
ACIS	Advisory Committee for Information Security (Finland)
ACIS	Analysis of Critical Infrastructural Sectors
ACSI 33	Australian Communications-Electronic Security Instruction 33 (Australia)
AFP	Australian Federal Police (Australia)
AGD	Attorney General's Department (Australia)
AG KRITIS	Interministerielle Arbeitsgruppe Kritische Infrastrukturen (Germany)
AgIO	Cabinet Office Workgroup on Information Operations (Sweden)
AHG	Ad Hoc Group (NATO)
AHTCC	Australian High Tech Crime Centre (Australia)
AIPA	Authority for IT in the Public Administration (Italy)
AIVD	Algemene Inlichtingenen Veiligheidsdienst/General Intelligence and Security Service (The Netherlands)
AKSIS	Arbeitskreis Schutz Kritischer Infrastrukturen/Working Group on Infrastructure Protection (Germany)
AMSD	Accompanying Measure System Dependability (EU)
ASIO	Australian Security Intelligence Organisation (Australia)
A-SIT	Center for Secure Information Technology Austria (Austria)
AS/NZS	Australian and New Zealand Standard for Risk Management (Australia/New Zealand)
AusCERT	Australian Computer Emergency Response Team (Australia/New Zealand)
BAKOM	Bundesamt für Kommunikation/Federal Office for Communication (Switzerland)
BAS	Protection of Society (Norway)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Federal Office for Civil Protection and Disaster Response (Germany)
BCS	British Computer Society (United Kingdom)
BfV	Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution (Germany)
BIT	Bundesamt für Informatik und Telekommunikation/Federal Office of Information Technology, Systems, and Telecommunication (Switzerland)
BITKOM	Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien (Germany)
BKA	Bundeskriminalamt/Federal Office of Criminal Investigation (Germany)
BMBF	Bundesministerium für Bildung und Forschung/Federal Ministry for Education and Research (Germany)
BMI	Bundesministerium des Inneren/Federal Ministry of the Interior (Germany)
BMJ	Bundesministerium der Justiz/Federal Ministry of Justice (Germany)
BMVg	Bundesministerium der Verteidigung/Federal Ministry of Defense (Germany)

BMWA	Bundesministerium für Wirtschaft und Arbeit/Federal Ministry of Economics and Labour (Germany)
BMWi	Bundesministerium für Wirtschaft and Technologie/Federal Ministry of Economics and Technology (Germany)
BND	Bundesnachrichtendienst/Federal Intelligence Service (Germany)
BSI	Bundesamt für Sicherheit in der Informationstechnik/ Federal Office for Information Security (Germany)
BVA	Bundesverwaltungsamt/Federal Office of Administration (Germany)
BWL	Bundesamt für Wirtschaftliche Landesversorgung/Federal Office for National Economic Supply (Switzerland)
BZK	Ministry of the Interior and Kingdom Relations (The Netherlands)
CanCERT	Canadian Computer Emergency Response Team (Canada)
CAPC	Civil Aviation Planning Committee (NATO)
CART	Computer Analysis and Response Team (United States)
CAS	Complex Adaptive Systems
CBA	Canadian Bankers Association (Canada)
CCIP	Centre for Critical Infrastructure Protection (New Zealand)
CCPC	Civil Communication Planning Committee (NATO)
CCS	Civil Contingencies Secretariat (United Kingdom)
CEA	Canadian Electricity Association (Canada)
CEN	European Committee for Standardization
CEP	Civil Emergency Planning (NATO)
CERT	Computer Emergency Response Team
CERTA	Computer Emergency Response Team (France)
CERT-Bund	German Computer Emergency Response Team for Federal Authorities (Germany)
CERT-FI	Computer Emergency Response Team Finland (Finland)
CERT-IST	Computer Emergency Response Team Industry, Services, and Trade (France)
CERT-IT	Italian Computer Emergency Response Team (Italy)
CERT-NL	Computer Emergency Response Team of the Netherlands (The Netherlands)
CERT-PA	Computer Emergency Response Team for the Public Central Administration (Italy)
CERT-RENATER	Computer Emergency Response Team (France)
CERT-RO	Computer Emergency Response Team – Central Government (The Netherlands), renamed in 2003 to →VCERT.NL
CESG	Communications-Electronics Security Group (United Kingdom)
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)
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CIOS	National Centre for IO/CIP Studies (Sweden)
CIP	Critical Infrastructure Protection
CIPG	Critical Infrastructure Protection Group (Australia)
CIPTF	Critical Infrastructure Protection Task Force (Canada)
CIRCA	Computer Incident Response Coordination Austria (Austria)
CIS	Center for International Studies (Switzerland)

CISSI	Inter-Ministerial Committee for Information Society (France)
CISU	Critical Infrastructure Studies Unit (Sweden)
CLUSIF	Club de la Sécurité des Systèmes d'Information Français (France)
CLUSIT	Italian Association for Security in Informatics (Italy)
CNES	French Space Agency (France)
CNI	Critical National Infrastructure
CNIPA	National Center for Informatics in the Public Administration (Italy)
COBIT	Control Objectives for Information Technology (United States)
COMSEC	Communications Security (Finland)
CPC	Civil Protection Committee (NATO)
CRC	Communications Research Centre (Canada)
CRN	Comprehensive Risk Analysis and Management Network (Switzerland)
CRS	Congressional Research Service (United States)
CSD	Computer Security Division at NIST (United States)
CSE	Communications Security Establishment (Canada)
CSIA	Central Sponsor for Information Assurance (United Kingdom)
CSIRT	Computer Security Incident Response Team
CSIS	Canadian Security Intelligence Service (Canada)
CSTARC	Cyber Security Tracking, Analysis and Response Center (United States)
CSTI	Strategic Advisory Board on Information Technologies (France)
CT	Counter-terrorism
CTEPA	Canadian Telecommunications Emergency Preparedness Association (Canada)
CTI	Commission for Technology and Innovation (Switzerland)
CTOSE	Cyber Tools On-Line Search for Evidence (EU)
CWIG	Critical Infrastructure Working Group (United States)
CYCO	Swiss Coordination Unit for Cybercrime Control (Switzerland)
CYTEX	Cyber Terror Exercise (Germany)
DARPA	Defense Advanced Research Projects Agency (United States)
DCSSI	Directorate for Security of Information Systems (France)
DdoS	Distributed Denial of Service
DDPS	Swiss Federal Department of Defense, Civil Protection, and Sports (Switzerland; →VBS)
DDSI	Dependability Development Support Initiative (EU)
deNIS	German Emergency Preparedness Information System (Germany)
DESS	Domestic and External Security Secretariat (New Zealand)
DepAuDE	Dependability for embedded Automation systems in Dynamic Environment
DFS	Swedish Information Processing Society (Sweden)
DGTP	Telecom and Post Directorate (The Netherlands)
DHS	Department of Homeland Security (United States)
DIA	Defense Intelligence Agency (United States)
DICO	Dipartimento di Informatica e Comunicazione/Department of Informatics and Communications (Italy)
DISCEX	DARPA Information Survivability Conference and Exposition (United States)
DoD	Department of Defense (United States)
DoE	Department of Energy (United States)
DSB	Directorate for Civil Protection and Emergency Planning (Norway)
DSD	Defence Signals Directorate (Australia)

DSG	Datenschutzgesetz/Data Protection Law (Austria)
DSK	Datenschutzkommission/Commission on Data Protection (Austria)
DSO	Departmental Security Officer (New Zealand)
DSTL	Defence Research Centre (United Kingdom)
DSTO	Defence Science and Technology Organisation (Australia)
DTI	Department of Trade and Industry (United Kingdom)
EBIOS	Expression of the Needs and Identification of Security Objects (France)
ECP-NL	Electronic Commerce Platform in the Netherlands (The Netherlands)
EIA	Electronic Industries Alliance (United States)
EJPD	Eidgenössisches Justiz und Polizeidepartement/Federal Department of Justice and Police (Switzerland)
EMP	Electromagnetic Pulse
ENFSI	European Network of Forensic Science Institute on Computer Crime (Austria)
ENISA	European Network and Information Security Agency
EO	Executive Order (United States)
ERA	European Research Area (EU)
ESCG	E-Security Coordination Group (Australia)
ETH	Eidgenössische Technische Hochschule/Swiss Federal Institute of Technology, ETH Zurich (Switzerland)
ETSI	European Telecommunications Standards Institute
EU	European Union
EVD	Eidgenössisches Volkswirtschaftsdepartement/Federal Department of Economic Affairs (Switzerland)
EXYSTENCE	Complex Systems Network of Excellence (EU)
FAPC	Food and Agriculture Planning Committee (NATO)
FBI	Federal Bureau of Investigation (United States)
FDCA	Finnish Data Communication Association (Finland)
EFD	Eidgenössisches Finanzdepartement/Swiss Federal Department of Finance (Switzerland)
FedCIRC	Federal Computer Incident Response Center (United States)
Fedpol	Federal Office of Police (Switzerland)
FERC	Federal Energy Regulatory Commission (United States)
FFI	Norwegian Defense Research Establishment (Norway)
FICORA	Finnish Communications Regulatory Authority (Finland)
FIRST	Forum of Incident and Security Response Team (Canada)
FISCAM	Federal Information Systems Control Audit Manual (United States)
FMV	Swedish Defense Material Administration (Sweden)
FOI	Swedish Defense Research Agency (Sweden)
FOIA	Freedom of Information Act (United States)
FP6	Sixth Framework Program (EU)
FRA	Swedish National Defense Radio Establishment (Sweden)
FS/ISAC	Financial Services Information Sharing and Analysis Center (United States)
FSK	Forschungsstelle für Sicherheitspolitik/Center for Security Studies (Switzerland)
G8	Group of Eight
GAO	General Accounting Office (United States)
GCSB	Communications Security Bureau (New Zealand)
GdIN	Gruppo di Interesse Nazionale (Italy)

GEA	Swedish Alliance for Electronic Commerce (Sweden)
GIP RENATER	National Network of Telecommunications for Technology, Education, and Research (France)
GoL	Government-on-Line (Canada)
GOVCERT.NL	Government-wide Computer Emergency Response Team (The Netherlands)
HERT	Hacking Emergency Response Team (The Netherlands)
HHM	Hierarchical Holographic Modeling
HSPD	Homeland Security Presidential Directive (United States)
HSAPRPA	Homeland Security Advanced Research Projects Agency
IA	Information Assurance
IAAC	The Information Assurance Advisory Council (United Kingdom)
IABG	Industrieanlagen-Betriebsgesellschaft (Germany)
IAG	Infrastructure Analysis Group
IAIP	Directorate for Information Analysis and Infrastructure Protection
ICCP	Committee for Information, Computer, and Communications Policy (OECD)
ICS	Secretary of the Interdepartmental Committee on Security (New Zealand)
ICT	Information and Communication Technologies
IDC	Interdepartmental Committee on the Protection of the National Information Infrastructure (Australia)
INFOSEC	Information Systems Security (Australia, New Zealand)
IOWG	Information Operations Working Group
IPC	Industrial Planning Committee (NATO)
IPs	Infrastructure Profiles
IPSC	Institute for the Protection and Security of Citizen
IPTS	Institute for Prospective Technological Studies
IRAM	Infrastructure Risk Analysis Model
IRItaly	Incident Response Italy (Italy)
ISACF	Information Systems Audit and Control Foundation (United States)
ISACs	Information Sharing and Analysis Centers
ISB	Informatikstrategieorgan Bund/Federal Strategy Unit for Information Technology (Switzerland)
ISCTI	Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (Italy)
ISDF	French Dependability Institute (France)
ISIDRAS	Information Security Incident Detection Reporting and Analysis (Australia)
ISIT	Inter-Ministerial Board for Security (Germany)
ISN	International Relations and Security Network (Switzerland)
ISP	Internet Service Provider
ISPA	Federation of the Austrian Internet Service Providers (Austria)
IST	Information Society Technologies (EU)
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria (France)
ITSEC	IT Security (Norway)
KIG	Coordination Group for Information Society (Switzerland)
KLPD	Korps Landelijke Politiediensten (Cyber Crime Unit of the Dutch Police) (The Netherlands)
KTH	Royal Institute of Technology (Sweden)
LCCI	Large Complex Critical Infrastructure

LUTIS	Lucerne Information Assurance Days (Switzerland)
M&S	Modeling and Simulation
MBG	Militärbefugnisgesetz (Austria)
MBRA	Model-Based Risk Assessment
MCDA	Multi-Criteria Decision Approach
MEI	Minimal Essential Infrastructure
MELANI	Reporting and Analysis Center for Information Assurance (Switzerland)
MIE	Minimum Essential Infrastructure
MISA	Municipal Information Systems Association (Canada)
MoD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NAZ	Nationale Alarm Zentrale/National Emergency Operations Center Agency (Switzerland)
NBED	National Board of Economic Defense (Finland)
NCC	National Coordinating Center
NCE	Networks of Centres of Excellence (Canada)
NCI	National Critical Infrastructures
NCIAP	National Critical Infrastructure Assurance Program (Canada)
NCIPP	National Critical Infrastructure Protection Program (Canada)
NCPG	National Contingency Planning Group (Canada)
NCS	National Communications System (United States)
NCSA	National Cyber Security Alliance (United States)
NCSD	National Cyber Security Division (United States)
NCSIP	National CIO Sub-Committee on Information Protection (Canada)
NCTP	National Counter-Terrorism Plan (Australia)
NERC	North American Electricity Reliability Council (United States)
NES	Federal Office for National Economic Supply (Switzerland; →BWL)
NESA	National Emergency Supply Agency (Finland)
NGO	Non-Governmental Organizations
NHTCU	National Hi-Tech Crime Unit (United Kingdom)
NIAC	National Infrastructure Advisory Council (United States)
NII	National Information Infrastructure
NIIS	Networked Information-Intensive System
NIPC	National Infrastructure Protection Center (United States)
NIRA	National Infrastructure Risk Assessment (Canada)
NISAC	National Infrastructure Simulation and Analysis Center (United States)
NISCC	National Infrastructure Security Co-ordination Centre (United Kingdom)
NIST	National Institute of Standards and Technology (United States)
NITAS	National Information Technology Alert Service
NLIP	Branchevereniging van Nederlandse Internet Providers Consortium of Dutch Internet Providers (The Netherlands)
NOIE	National Office for the Information Economy (Australia)
NPB	Swedish National Police Board (Sweden)
NRC	Canadian National Research Council (Canada)
NSA	National Security Agency (United States)
NSD	Industry Security Delegation (Sweden)
NSSC	National Strategy to Secure Cyberspace (United States)
NZCS SigSec	Computer Society Special Interest Group on Security (New Zealand)
NZSA	New Zealand Security Association (New Zealand)
NZSIS	New Zealand Security Intelligence Service (New Zealand)

NZSIT	New Zealand Security of Information Technology (New Zealand)
ÖCB	Överstyrelsen för Civil Beredskam/Swedish Agency for Civil Emergency Planning, now KBM (Sweden)
OCIIP	Office of Computer Investigations and Infrastructure Protection (United States)
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness (Canada)
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation (United States)
ODESC	Officials Committee for Domestic and External Security Co-ordination (New Zealand)
OEA	Office of Energy Assurance (United States)
OECD	Organization for Economic Cooperation and Development
OGIT	Office of Government Information Technology (Australia)
OGO	Office for Government On-line (Australia)
OICT	New South Wales Office of Information and Communications Technology (Australia)
OKOKRIM	National Authority for Investigation and Prosecution of Economic and Environmental Crime (Norway)
OMIG	OCTAVE Method Implementation Guide (United States)
OST	Office of Science and Technology (United Kingdom)
OSTP	Office of Science and Technology Policy (United States)
PAGSI	Government Action Program for an Information Society (France)
PB&C	Planning Board and Committee (NATO)
PBIST	Planning Board for Inland Surface Transportation (NATO)
PBOS	Planning Board for Ocean Shipping (NATO)
PCAST	President's Council of Advisors on Science and Technology (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)
PKI	Public Key Infrastructure
PMRM	Partitioned Multi-objective Risk Method
PPO	Planning and Partnerships Office (PPO)
PRA	Probabilistic Risk Assessment
PreDICT	Predict Defence Infrastructure Core Requirements Tool (Australia)
PSCIOC	Public Sector Chief Information Officer's Council (Canada)
PSM	Protective Security Manual (Australia)
PSS	Public Safety and Security (Sweden)
PTS	Swedish National Post and Telecom Agency (Sweden)
R&D	Research and Development
RAFLS	Relational Analysis For Linked Systems (Canada)
RCMP	Royal Canadian Mounted Police (Canada)
RegTP	Regulatory Authority for Telecommunications and Posts (Germany)
RMA	Revolution in Military Affairs
S&T	Science and Technology (United States)
SAI	Centro Virtuale di Simulazione e Analisi delle Interdipendenze/ Interdependencies Simulation and Analysis Center (Italy)

SÄPO	Swedish Security Service (Sweden)
SCEPC	Senior Civil Emergency Planning Committee (NATO)
SCNS	Secretaries' Committee on National Security (Australia)
SCSSI	Service Central de la Sécurité des Systèmes d'Information (France)
SDLC	System Development Life Cycle
SEI	Software Engineering Institute (United States)
SEMA	Swedish Emergency Management Agency (Sweden)
SFU	Strategische Führungsübung/Strategic Leadership Exercise (Switzerland)
SGDN	General Secretariat of National Defense (France)
SIGINT	Signals Intelligence
SII	Strategic Infrastructure Initiative (Canada)
SIS	Center for Information Security (Norway)
SITIC	Swedish IT Incident Centre (Sweden)
Sitra	Finnish National Fund for Research and Development (Finland)
SLT	Strategic Leadership Training (Switzerland)
SMEs	Small and Medium Enterprises
SNZ	Standards New Zealand (New Zealand)
SONJA	Sonderstab Information Assurance/Special Task Force on Information Assurance (Switzerland)
SPG	Sicherheitspolizeigesetz (Austria)
S.S.E	Secure Electronic Environment (New Zealand)
SSI	Security of Information Systems (France)
SSIT	Statssekretærutvalget for IT/ State Secretary Committee for ICT (Norway)
SWITCH	Swiss Education and Research Network (Switzerland)
SWOT	Strength, Weakness, Opportunities, Threats (Analysis)
TAAATS	The Australian Advanced Air Traffic System (Australia)
Tekes	National Technology Agency (Finland)
TELMO	Finnish Association for Interactive Network Services (Finland)
TIEKE	Finnish Information Society Development Centre (Finland)
TISN	Trusted Information Sharing Network for Critical Infrastructure Protection (Australia)
TKG	Telekommunikationsgesetz (Austria)
TNO	Netherlands Organization for Applied Scientific Research (The Netherlands)
TSA	National Communications Security Group (Sweden)
TSWG	Technical Support Working Group (United States)
UN	United Nations
USA PATRIOT	(Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (United States)
UNIRAS	Unified Incident Reporting and Alert Scheme (United Kingdom)
V&W	Ministry of Transport, Public Works, and Water Management (The Netherlands)
VAF	Vulnerability Assessment Framework (United States)
VAHTI	Steering Committee for Data Security in State Administration (Finland)
VNO-NCW	Confederation of Netherlands Industry and Employers (The Netherlands)
WARPs	Warning, Advice, and Reporting Points (United Kingdom)
WPISP	Working Party on Information Security and Privacy (OECD)
WSIS	World Summit on the Information Society (ITU)
VWS	Ministry of Health (The Netherlands)
ZES	Zentrum für europäische Strategieforschung/Center for Strategic Studies (Germany)

Introduction

Evolution of the Critical Information Infrastructure Protection (CIIP) Issue

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

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

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

3 Cf. Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). *EICAR Conference Best Paper Proceedings 2003*, http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.

4 Dunn, Myriam *Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment.* Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich, 2002).

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

First Steps in the Protection of Critical Information Infrastructure

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

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

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

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

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

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

9 Ibid.

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

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

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

Distinction between CIP and CIIP

A clear and stringent distinction between the two key terms "CIP" and "CIIP" is desirable, but not easily achieved. In official publications, both terms are used inconsistently, with the term CIP frequently used even if the document is only referring to CIIP. Accordingly, the reader will find both terms used in the CIIP Handbook. This is not due to a lack of accuracy or random use of the two concepts. Rather, the parallel use of terms reflects the stage of political discussion in the surveyed countries and points to the deficiencies in understanding conceptual differences between the concepts. But why would it be useful and desirable to arrive at a better distinction between the two concepts of CIP and CIIP? And what is their relation to each other?

10 Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue.* Version 1.0 (Washington, 2000); Clinton, William J. *Executive Order 13010 on Critical Infrastructure Protection.* (Washington, 15 July 1996). http://www.info-sec.com/pccip/web/eo13010.html; Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.* (Washington, 22 May 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.

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

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

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

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

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

13 Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK." *Plenary Address at the Future of European Crisis Management*, Uppsala, Sweden, March 2001.

14 See also Part II of this Handbook.

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

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

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

CIP/CIIP: A Multifaceted Issue

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

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

15 Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK." *Plenary Address at the Future of European Crisis Management*, Uppsala, Sweden, March 2001.

16 Näf, Michael. "Ubiquitous Insecurity? How to "Hack" IT Systems". In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security.* Information & Security: An International Journal, Volume 7, 2001, pp. 104–118.

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

- *The system-level, technical perspective:* CIIP is approached as an IT-security or information assurance issue, with a strong focus on Internet security. In this view, threats to the information infrastructure are to be confronted by technical means such as firewalls, antivirus software, or intrusion detection software. The establishment of so-called *Computer Emergency Response Teams* (CERTs) and similar early-warning approaches in various countries is an example of this perspective.
- *The business perspective:* CIIP is seen as an issue of "business continuity", especially in the context of e-Business. This requires not only permanent access to IT infrastructures, but also permanently available business processes to ensure satisfactory business performance. The means of achieving this coincide, by and large, with the ideas of the technical community outlined above; however, the focus is not solely on the system level, but includes organizational and human factors. This perspective is also reflected in some countries' protection approaches that mainly aim to support the Information Society.
- *The law-enforcement perspective:* CIIP is seen as an issue of protecting society against (cyber-) crime. Cybercrime is a very broad concept that has various meanings, ranging from technology-enabled crimes to crimes committed against individual computers, and including issues such as infringements of copyright, computer fraud, child pornography, and violations of network security. Cybercrime is fought with more or less traditional law-enforcement strategies, especially by adopting appropriate legislation and fostering international co-operation.
- *The national-security perspective*: This is a "grab-bag" view of CIIP. Usually, the whole of society is perceived as endangered, so that action is taken at a variety of levels (e.g., at the technical, legislative, organizational, or international levels), and the actors involved in protection efforts include government officials from different agencies, as well as representatives of the private sector and of the general public. This is the perspective adopted in assembling this Handbook.

In accordance with the different perspectives outlined above, information infrastructures are seen variously as a tool for maintaining a competitive edge over business adversaries, as technical-operational systems, as facilitators

of criminal activities, as defense-relevant strategic assets, or more generally, as objects of national and international security policy. Depending on one's perspective, the issue may be perceived either as the private/corporate sector's responsibility or as the responsibility of specific governmental agencies, ranging from law enforcement to the defense establishment, or a mixture of all of the above; hence the diversity of approaches that can be found in the country surveys in this Handbook.

All of these perspectives have vital implications for protection policies. The discussion leads to the central question of whether CIIP is an issue of ordinary day-to-day politics or belongs to the realm of national or international security[17] – and the answers may vary depending on the scenario –, and subsequently to the question of which protection efforts, goals, strategies, and instruments are appropriate for problem solution.[18] The fact that so many of the critical infrastructures are in the hands of the private sector or of foreign actors in other countries only aggravates the problem of demarcation. It follows that, even if CIIP is perceived as politics of the extraordinary, states can no longer assure security on their own – rather, they must find new ways of interaction and cooperation with different national and international actors that have not traditionally been in the security arena, which is a much wider notion of governance than that which characterized the Cold War.

Key Terms and Concepts

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

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

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

The Meaning of "Critical" in Critical Infrastructure Protection

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

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

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

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

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

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

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

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

Moreover, the question of criticality in the socio-political context is always inextricably linked to the question of how damage or disruption of an infrastructure would be perceived and exploited politically. Actual loss (monetary loss or loss of lives) would be compounded by political damage or loss in basic public trust in the mechanisms of government, and erosion of confidence in inherent government stability.[24] From this perspective, the criticality of an infrastructure can never be identified preventively based on empirical data alone, but only *ex post facto*, after a crisis has occurred, and as the result of a normative process.

The Concept of Infrastructures as Focus of Protection

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

If we compare the two concepts, the most striking similarity is the focus on "essential goods/products and services". That means that the actual objects of protection interests are not static infrastructures as such, but rather the *services*, the physical and electronic (information-) *flows*, their *role* and *function* for society, and especially the *core values* that are delivered by the infrastructures. This is a far more abstract level of understanding essential assets. While infrastructures are constructed, maintained, and operated by humans and can be relatively easily illustrated in terms of organizational

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

24 Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security.* Information & Security: An International Journal, Volume 7 (2001), pp. 67–79.

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

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

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

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

Purpose and Key Questions

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

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

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

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

Structure of the Handbook

The book is guided by two main questions:

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

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

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

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

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

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

Outlook and Planned Updates

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

29 All links last checked on 1 December 2003.

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

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

Part I

CIIP Country Surveys

by Isabelle Wigert

Structure of Part I

Introduction

Part I of this handbook surveys critical information infrastructure protection (CIIP) efforts in fourteen countries, namely Australia, Austria, Canada, Finland, France, Germany, Italy, the Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

For each survey, four focal points of high importance covering conceptual and organizational aspects of CIIP are considered:

(1) Critical Sectors

The first section lists the critical sectors identified by the specific country and provides, when available, definitions of CII and CIIP.

(2) Initiatives and Policy

The second section gives an overview of the most important steps taken at the governmental level since the late 1990s to handle CIIP. The focus is on initiatives and 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) Organizational Overview

The third 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.

(4) Early Warning Approaches

The forth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as *CERTs* (Computer Emergency Response Teams), *ISAC*s (Information Sharing and Analysis Centers), etc. Furthermore, reference is made to plans for the development of comprehensive early warning alert and incident report structures.

The key question underlying Part I is: *What national approaches to critical information infrastructure protection exist?*

The surveys were compiled in a three-step procedure.

1) First, open-source material was collected from online resources, publicly available government papers, workshops, and conference proceedings. This information was used to write a first draft of the country surveys. However, the availability of this open-source information, and especially the availability of documents on the Internet, varies considerably in quantity and quality from country to country. Additionally, a lot of relevant information is only available in the original language.
2) The second and most important step was the collaboration with the national experts from government and government-related organizations in the field. Whenever possible, at least two experts per country were consulted for reviews. The experts were asked to correct, complete, and update the draft country surveys.
3) Finally, all of the national experts' input was worked into the final version of the country studies.

Since expert input was crucial for all country surveys, it is obvious that the individual perspectives and viewpoints of the consulted experts had a significant impact on the end result. This is also one of the major reasons why the individual surveys differ considerably in focus and general direction, and in their understanding of the nature of CIIP.

CIIP Country Surveys

Australia

This Country Survey of Australia 2004 was mainly written by Adam Cobb, Director Stratwise Strategic Intelligence, Australia.

Australia

Critical Sectors

The Australian government defines critical infrastructure as "infrastructure which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on social or economic well-being or affect national security or defence."[32] Australia's national information infrastructure (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.[33] 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".[34]

The scope of Australian critical infrastructure includes the following items:[35]

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity generation and Transmission, Nuclear Research Reactor),
- Finance (Banking, Insurance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Government Services (Defense and Intelligence Facilities, Houses of Parliament, Key Government Departments, Foreign Missions and Key Residences, Emergency Services (Police, Fire, Ambulance)),
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Manufacturing (Defense Industry, Heavy Industry, and Chemicals),
- National Icons (Buildings (e.g., Sydney Opera House), Cultural, Sport, and Tourism),

32 Attorney General's Department National Security Website (http://www.ag.gov.au/). http://www.nationalsecurity.gov.au/www/nationalsecurityHome.nsf/Web+Pages/5C51DE424EB541C2CA256C95000A8DDA?OpenDocument.

33 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), pp. 7–8.

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

- Transport (Air Traffic Control, Road, Sea, Rail and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).

Technology is relied upon to operate, monitor, and maintain these vast, exposed networks and the fragile information grids that underpin them.

In a big country such as Australia with a dispersed resource base, redundancy in distribution networks, and in the information systems upon which they depend, has been kept to a strict minimum due to cost pressures. For example, Australia's biggest city, Sydney, is dependent on three sources of power, not all of which are distributed through redundant networks with backup systems. Another vulnerability may be created when all power lines supplying a metropolis are channeled through a single relay station, making it into a potential choke point.[36]

The air traffic control network has recently been upgraded to a fully computerized and *automated* system called TAAATS (*The Australian Advanced Air Traffic System*). Clearly, business continuity plans are vitally important in the TAAATS concept, and much attention has been paid to ensuring redundancy within and between the two control centers (Brisbane and Melbourne). However the TAAATS website does note that it relies on just three major nodes in its packet switching network.[37]

Both TAAATS control centers also have alternative power supplies. That is not true for a wide range of federal government installations, including key military sites that are totally dependant on civil infrastructure.[38] A study of the power and communication distribution networks in the capital, Canberra, and their limited connections to the rest of the country, suggest that a terrorist attack against just 3 key sites could degrade (possibly severely) the functioning of federal government, including key agencies responsible for national security.[39]

35 Attorney General's Department National Security website, with additions.

36 Cobb, A.C., *Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks*. Foreign Affairs, Defence and Trade Group, Research Paper 18 (29 June, 1998); http://www.aph.gov.au/library/pubs/rp/1997-98/98rp18.htm. See also Cobb, A.C., *Critical Infrastructure Attack: An Investigation of the Vulnerability of an OECD Country*. In: Information Operations. Bosch, J.M.J., H.A.M. Luijjf, and A.R. Mollema (eds.), Netherlands Annual Review of Military Studies (NL ARMS) 1999. ISSN: 0166-9982 (Tilburg, 1999). http://www.tno.nl/instit/fel/refs/pub99/nlarms.html.

37 http://www.airservicesaustralia.com/mediainfo/informationfeatures/abouttaaats/hardwaredetails.htm.

38 Cobb, A.C., *Thinking about the Unthinkable*, op. cit.

39 Ibid.

Many of Australia's assets rely on the country's vulnerable NII. For example, Australia recently signed landmark oil and gas contracts with the People's Republic of China, estimated to be worth more than $50bn over twenty years.[40] The resources for this historic deal will be extracted in one of Australia's most remote, exposed, and infrastructure-poor regions, the North West Shelf. The deal with China is of national significance, but rests on a very fragile basis. The maritime oils fields are spread over a vast stretch of sea; they lie thousands of kilometers north of Perth and far from major defense bases. The regional communications network has very little redundancy, and its fuel distribution system almost none. The North West Shelf is Australia's most critical infrastructure in terms of both vulnerability and value.

Any comprehensive risk assessment requires an evaluation of threats against the vulnerabilities identified. The first such study in Australia, undertaken in 1997 by the *Strategic and Defence Studies Centre*[41], part of the *Australian National University*, assessed terrorism as the most likely form of threat against Australia's critical infrastructure and estimated that while the vulnerabilities were great, the threat at that time was low.[42] That assessment considered all forms of attack, including, but not limited to, cyberattacks. Interestingly, that assessment discussed the possibility of hijacked airliners being used on suicide missions, a proposition considered so outrageous and alarmist at the time that it was edited out of subsequent editions of the paper.[43]

The low threat environment has dramatically shifted to a high threat environment since that first assessment was made. Australia's closest ally and strategic partner is the United States. Australia has been at the heart of all coalition operations in the war on terrorism and in Iraq. Following the Afghanistan campaign, Osama bin Laden has singled out Australia for special mention in most of his public statements.

Cyberattacks have already occurred. Australia's biggest Internet Service Provider (ISP), Telstra, was disabled for over three weeks due to a series of attacks in October 2003. Businesses were forced to go without Internet and

40 http://news.ninemsn.com.au/Business/story_52627.asp; http://abcasiapacific.com/news/stories/asiapacific_stories_974625.htm.

41 http://rspas.anu.edu.au/sdsc/index.html.

42 Cobb, A.C., *Australia's Vulnerability to Information Attack: Towards a National Information Policy*. Strategic and Defence Studies Centre, ANU, Working Paper, No.306, 1997.

43 Cobb, A.C., *Thinking about the Unthinkable*, op. cit, was the next edition of the ANU Working Paper where the airliner scenario was edited out.

e-mail services, causing damage untold, but estimated to be comfortably in the millions of Australian dollars.[44] The crisis demonstrated just how much Australian business has become dependant on a functional Internet system, and hinted at the scale of costs that could be expected to reoccur in future.

Australia has significant vulnerabilities across its critical infrastructure. While the general terrorist threat against Australia has increased dramatically, it remains to be seen to what extent groups like al-Qaida and Gema'ah Islamiyah will turn to cyberattack as a modus operandi.

Initiatives and Policy

Reassessing Australia's National Security Policy

The attacks in the US on 11 September 2001 and on Bali on 12 October 2002 have prompted a thorough reassessment of Australia's national security policies, organizations, and laws. Some of these changes have had some impact on CIIP initiatives, but the core focus has been on counter-terrorism (CT) and CIP. Interestingly, by 2001 a number of important changes had already been made in the CIIP field, such as the establishment of the E-Security Coordination Group, which was charged with creating the E-Security National Agenda in September of the same year (see below).[45]

CIIP funding in the May 2001 Budget was AUS$2m. This jumped to AUS$6m the following year.[46] Compared to the AUS$2bn devoted to all counter-terrorism arrangements, these are trivial amounts. They reflect the government's continuing skepticism about the possibility of cyberattack, but also the fact that government has a limited "moral leadership" role to play insofar as Australia's critical infrastructure is operated almost entirely by private companies.

Early developments included legislative reform, such as the *Australian Security Intelligence Agency* (ASIO*) Amendment Act* (1999)[47] and the *Cybercrime Act* (2001)[48]. Developments in 2003 include the creation of

44 'Storm on BigPond, users attack Telstra', *The Sydney Morning Herald*, 21 October 2003, http://www.smh.com.au/articles/2003/10/20/1066631346473.html?from=storyrhs.

45 http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm.

46 The 02–03 Budget reported the increase as AUS$24.9 million over four years.

47 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

48 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

49 National Counter-Terrorism Plan, http://www.nationalsecurity.gov.au/www/nationalsecurityhome.nsf/AllDocs/RWPCD8501294925DA06CA256D42001C1A4C?OpenDocument.

the National Counter-Terrorism Plan,[49] the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), and the Australian High Tech Crime Centre (AHTCC). The latter two developments are extensions of existing arrangements. TISN takes over from the Consultative Industry Forum, and the AHTCC is a new national policing initiative run by the Australian Federal Police.

National Counter-Terrorism Plan (NCTP)

The introduction of a *National Counter-Terrorism Plan* (NCTP)[50] in June 2003 added a new policy dimension to CIIP insofar as it outlined national responsibilities, albeit in a cursory way, with respect to CIP. Because almost all of Australia's vulnerable CI is operated by networked computers connected through communication nets that comprise a key part of CI, the absence of specific policy direction with respect to CIIP in the NCTP is highly ambiguous. Consequently, the government needs to clarify the interrelationship between the *E-Security National Agenda* (see below) and the NCTP. Indeed, neither document is very specific on a range of matters. It is not known if the classified versions are more specific and robust, and better conceived than those that can be accessed publicly.

In November 2003, Australian authorities said they had discovered a suspected al-Qaida terrorist cell in Sydney.[51] Its alleged bomb-maker, Willy Brigitte, a former French soldier, reportedly owned photographs of Australia's only nuclear reactor.[52] The Australian Radiation Protection and Safety Agency reported that a successful attack on the Lucas Heights medical research reactor, located in a Sydney suburb, could contaminate the entire population of Australia's largest city (4 million people).[53] The head of ASIO, Australia's peak security agency, told a parliamentary enquiry that, while there were "many unanswered questions", Brigitte could indeed have intended to harm

50 Ibid.

51 Australian authorities had been monitoring Gema'ah Islamiyah, which was responsible for the 2002 Bali, and 2003 Jakarta, bombings. JI had established "mantiki 4", a regional operation based in Australia, and there have been unconfirmed reports of efforts as far back as before the Sydney Olympics to attack Australia. http://quickstart.clari.net/qs_se/webnews/wed/ad/Qindonesia-hambali.Rpc1_DSB.html.

52 Terrorists could radiate Sydney: report, *The Bulletin Magazine*, 12 November 2003, http://news.ninemsn.com.au/National/story_8377.asp; see also http://bulletin.ninemsn.com.au/bulletin/eddesk.nsf/0/F990BCFC4B94A14ECA256DD60008E5B7?open.

53 Ibid. See also, "Ruddock silent on 'plot to attack reactor' claim", *Sydney Morning Herald*, 10 November 2003 http://www.smh.com.au/articles/2003/11/10/1068329468981.html.

Australia.[54] With such potential physical threats against critical infrastructure, it is perhaps understandable that the focus of government has been applied to counter-terrorism and CIP initiatives at the expense of a more robust and, in particular, a more coordinated approach to CIIP.[55]

Organizational Overview

Public Agencies

While the *E-Security Coordination Group* (ESCG) is the overarching governmental agency with particular focus on *policy*, the *Critical Infrastructure Protection Group* (CIPG) is the *operational* arm of government with respect to CIIP.

E-Security Coordination Group (ESCG)

The *E-Security Coordination Group (ESCG)* is the government's core policy development and coordination body on all e-Security matters. Its main tasks are the development of a secure and trusted electronic operating environment, raising awareness of e-Security, reporting of incidents, and information-sharing. The ESCG is chaired by the *National Office for the Information Economy* (NOIE).[56]

The establishment of the ESCG in February 2001 clarified the diffuse structure of government organizations involved in CIIP. Prior to the formation of the ESCG, a range of organizations across government had played some part in CIIP issues, but the system lacked a clearly defined lead organization. With no leader, there was also no chain of command, no clear set of responsibilities, no coordination of disparate CIIP efforts across government and between government and the private sector, and no formal CIIP policy.

In September 2001, the ESCG produced the first national strategy for CIIP: the *E-Security National Agenda*.[57] This is a brief outline of responsibilities

54 "Brigitte 'in plot to blow up reactor'", *Australian Financial Review*, 12 November 2003, http://203.26.51.49/articles/2003/11/11/1068329561183.html.

55 'Australia leaves the hack door open to cyber sabotage', *The Sydney Morning Herald*, 8 April 2003, http://www.smh.com.au/articles/2003/04/07/1049567603965.html.

56 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.

57 http://www.noie.gov.au/projects/confidence/Protecting/nat_agenda.htm.

rather than a thoroughly structured and comprehensive policy document but it is a great leap forward from earlier efforts.[58]

National Office for the Information Economy (NOIE)

The *National Office for the Information Economy* (NOIE), which incorporated the *Office of Government Online* (OGO) in late 2000, is Australia's lead agency for information economy issues. Established in 1997, it was tasked with the establishment of a globally leading online economy and society through developing, overseeing, and coordinating government policy on electronic commerce, online services, and the Internet.[59] For example, it was deemed that all government services should be made available online. NOIE has direct responsibility for the development and coordination of advice to the government on issues related to the information economy.

NOIE is not a security agency, which makes it an unusual choice for the chair of the *E-Security Coordination Group* (ESCG) given the latter's specific role with respect to E-Security matters.

Critical Infrastructure Protection Group (CIPG)

The main task of the *Critical Infrastructure Protection Group* (CIPG) is to conduct threat and vulnerability assessments of key participants in the telecommunications, finance, and electricity sectors, and of air traffic control.[60] The CIPG is chaired by the Attorney-General's Department, and its members include the *Defence Signals Directorate* (DSD), the *Australian Security Intelligence Organisation* (ASIO), and the *Australian Federal Police* (AFP) – all operational military, security, and police intelligence services respectively.

Defence Signals Directorate (DSD)

The *Defence Signals Directorate* (DSD) is Australia's national authority for signals intelligence and information security. DSD is responsible for advising state agencies on how to implement effective IT security. It does so by providing expert assistance to agencies in relation to cryptography and network security, and by developing guidelines and policies on implementing security. DSD's information security (INFOSEC) activities include information and incident collection, analysis, and warning services; setting

58 See the first edition of the CIIP Handbook: Wenger, Andreas, Jan Metzger, and Myriam Dunn (eds.), *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* (Zurich: Center for Security Studies, 2002).

59 Ibid.

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

awareness and certification standards; defensive measures, including protective security measures; response arrangements ranging from technical responses to single incidents to crisis management arrangements; and contingency planning.

Australian Security Intelligence Organisation (ASIO)

The *Australian Security Intelligence Organisation* (ASIO) is Australia's domestic spy agency.[61] 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 ASIO functions include the provision of security assessments and protective security advice. ASIO has a CIP section that is involved in producing assessments of vulnerabilities in, and threats to, critical infrastructure. The section is also concerned with INFOSEC threats, but relies on data generated by DSD for this purpose.

ASIO has the power to covertly enter and search the premises of those it suspects of espionage or terrorism. The *ASIO Act* (1979) was subsequently amended *(ASIO Amendment Act)*[62] in 1999, to give the organization the same covert access to the computers and computer systems of targets. Since the introduction of the *Cybercrime Act* (2001),[63] the ASIO's discretion in terms of targets has widened considerably, and now also pertains to CIIP investigations. Following the introduction of new counter-terrorism legislation in 2003, ASIO can detain and question suspects without charge for up to seven days. Previously, ASIO was unable to interrogate suspects, and relied on the Australian Federal Police to carry out police actions on its behalf or based on the intelligence ASIO had covertly generated.

61 Its functions are set out in the Australian Security Intelligence Organisation Act 1979. The Australian Secret Intelligence Service (ASIS) is Australia's overseas intelligence collection agency, it engages primarily in human intelligence (HUMINT) activities. ASIS's activities were only codified in law in 2001 – *Intelligence Services Act* (2001). The Australian system is based on British intelligence arrangements, and consequently the corresponding departments in the UK are: DSD: GCHQ, ASIO: MI5, ASIS: MI6.

62 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

63 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

The Australian Federal Police (AFP)

The introduction of the *Cybercrime Act* (2001) prompted the Australian Federal Police (AFP) to join forces with state and territory police, to create a national organization to address the threat of cybercrime. The line dividing cybercrime and cyber-terrorism is blurred because many of the tools and techniques are common to both activities. Consequently, the creation of the *Australian High Tech Crime Centre* (AHTCC) [64] is a major and important CIIP measure. AHTCC is the main Australian law enforcement unit involved in the investigation of electronic attack against the National Information Infrastructure.

Public Private Partnerships

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Building on the recommendations of the first *Consultative Industry Forum* (CIF),[65] in November 2001, the prime minister announced the formation of the *Business-Government Task Force on Critical Infrastructure*. The task force recommended replacing the CIF with a *Trusted Information-Sharing Network Infrastructure Protection (TISN)* [66] and associated advisory council. The TISN and council were established on 29 November 2002.[67]

TISN is intended to allow the owners and operators of critical infrastructure to share information on important issues such as business continuity, consequence management, information system attacks and vulnerabilities, e-Crime, protection of key sites from attack or sabotage, chemical, biological, and radiological threats to water and food supplies, and the identification and protection of offshore and maritime assets. It is, however, unclear from public documents how its approach differs from that of the earlier *Consultative Industry Forum* (CIF), which was plagued by the usual problems besting public private partnerships immersed in highly confidential commercial and national security environments.[68]

64 http://www.ahtcc.gov.au/.

65 This Forum resulted from the government's first report in the CIIP field, NII Report 1998, op. cit.

66 http://www.cript.gov.au/.

67 See http://www.cript.gov.au/.

68 The TISN is chaired by the Attorney-General's Department (AGD), which is a security-related agency. Prima facie, it would appear to have made more sense to locate the TISN in NOIE, and correspondingly the ESCG would have been a better fit in the AGD.

Early Warning Approaches

There are two key organizations that provide comprehensive cyberattack early warning services in Australia. The *Defence Signals Directorate* (DSD) provides early warning to federal government IT networks, and AusCERT provides the same services to private sector operators of CI. In addition, the Australian Government has recently launched the *OnSecure* website to strengthen the country's information security.

Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

The *Defence Signals Directorate* (DSD) maintains the rather cumbersomely entitled ISIDRAS scheme (*Information Security Incident Detection Reporting and Analysis Scheme*). ISIDRAS is an IT incident-reporting scheme for Australian government agencies specifically concerned with high-level incidents that could cause damage to the government's IT infrastructures. The type and extent of DSD resources applied to ISIDRAS is unknown. For example, it is not known whether DSD merely reacts to reports of suspect activity, or whether it has a proactive capability. DSD has released a breakdown of the types of incidents ISIDRAS experienced in FY 01–02,[69] but has decided not to release this information for subsequent years.

Australian Computer Emergency Response Team (AusCERT)

The *Australian Computer Emergency Response Team* (AusCERT) is a non-profit organization located at the University of Queensland. 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.[70] In May 2003, the Australian government announced the launch of AusCERT's *National Information*

69 http://www.noie.gov.au/publications/presentations/esecurity/DSD1/dsd5.HTM.
70 http://www.auscert.org.au, and NII Report 1998, p. 2.

Technology Alert Service (NITAS)[71], which is sponsored by the federal government. NITAS provides a free service to subscriber owners and operators of the NII.

OnSecure Website

The *OnSecure* website was jointly developed by the *National Office for the Information Economy* (NOIE) and the *Defence Signals Directorate* (DSD) and allows government agencies to securely report information security incidents online rather than by mail or facsimile. Launched in December 2003, *OnSecure* will make it easier for Government agencies to report any attempted hacking, denial of service or other breaches of information security. It will also help the DSD to analyze incident reports more quickly and effectively, to identify any developing patterns and to assess the resulting threat level.

OnSecure also has a public site, www.onsecure.gov.au, which makes information security resource material available to the general public. The site will help Internet users to understand and respond to potential e-Security threats and will provide access to information and advice on issues such as spam, viruses, and fraud.[72]

Corporate Sector Initiatives

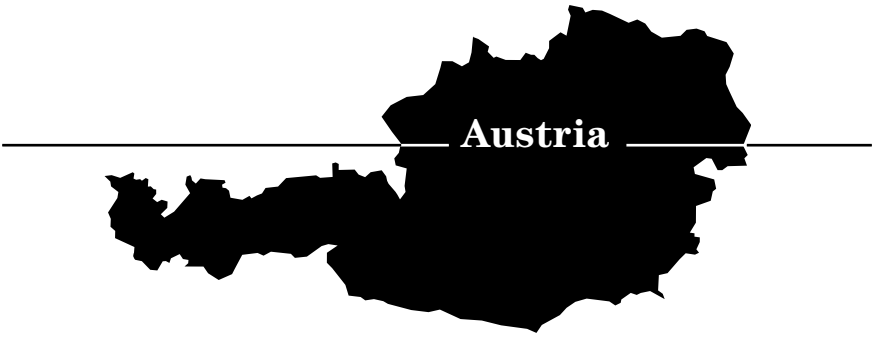
It is notable that in the past few years, a series of major listed telecommunications and IT companies have established private global data monitoring and incident response services of the kind provided by *Defence Signals Directorate* (DSD) and AusCERT, but for corporate clients. Their physical, electronic, biometric, and cyber-/network security measures are highly advanced.[73]

71 http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/0/64534A395BA69AF4CA256D24007BDCA2?OpenDocument.

72 http://www.onsecure.gov.au.

73 Information provided by Adam Cobb.

CIIP Country Surveys



The Country Survey of Austria 2004 was mainly written by Thomas Pankratz, Austrian Federal Ministry of Defence, Bureau for Security Policy. Dr. Pankratz wants to express his gratitude for the research assistance of Martin Leithner. In addition, Gerald Trost, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic of Austria and Otto Hellwig, Former Official of the Federal Chancellery, provided valuable input.

Austria

Critical Sectors

Austria as a modern society and as a small state is particularly vulnerable in the area of information. This includes both the military and the civilian sectors and, increasingly, business and industry as well.[74] Strictly speaking, there is no stringent, congruent, coordinated, CII/ CIIP-concept designated as such in Austria.[75] The following are seen in Austria as critical sectors:[76]

- (Tele)Communication,
- Banking and Finance,
- Broadcasting,
- Emergency Services,
- Energy,
- Information Services,
- Military Defense,
- Police Services,
- Post Systems,
- Public Administration,
- Public Health,
- Social Welfare,
- Transportation,
- Utilities,
- Water Supply.

74 Resolution by the Austrian parliament – Security and Defense Doctrine; Security and Defense Doctrine: Analysis- Draft expert report of 23 January 2001.

75 There is also no clear definition of CII/ CIIP, and the terms "CII/ CIIP" are not commonly used in Austria. Therefore, these terms are used in a broad sense for the purposes of this contribution.

76 Pankratz Thomas, Information warfare – Eine Bedrohung der 'wired society', in: Gärtner Heinz/ Höll Otmar, *Comprehensive Security* (Vienna, 2001).

Initiatives and Policy

There have been several substantial organizational and procedural efforts since the 1990s to manage CII(P) in Austria. The issue of CIIP has mainly been addressed by the government, especially by the *Ministry of Internal Affairs*, the *Ministry of Defense*, the *Federal Chancellery*, and the *Ministry of Public Service and Sports*.

Security and Defense Doctrine 2001

According to the principle of comprehensive security, the Security and Defense Doctrine[77] recommends the development of the existing *Comprehensive National Defense Program* into a system of *Comprehensive Security Provision* by focusing on the new risks and threats and by amending legal provisions.[78] This also includes all measures referring to CIIP.[79] The Doctrine clearly stresses that for small states, full and unimpaired access to the required information is a basis for their freedom of action in security matters.[80]

The implementation of Austria's security policy within the framework of the Comprehensive Security Provision relies on systematic co-operation among various policy areas on the basis of appropriate sub-strategies.

In addition to the sub-strategies, which are mentioned in the doctrine and are currently being elaborated, it was decided to work out a specific sub-strategy dealing with IT security. A project team under the lead of

77 http://www.bka.gv.at/bka/sicherheitspolitik/doktrin.html.

78 Resolution by the Austrian parliament- Security and Defense Doctrine; Security and Defense Doctrine: Analysis – draft expert report of 23 January 2001.

79 The concept of Comprehensive National Defense as developed from 1961 onwards was embedded in the Constitution in 1975. Under Article 9a of the Austrian Constitution, the role of Comprehensive National Defense is to "maintain [Austria's] independence from external influence as well as the inviolability and unity of its territory, especially to maintain and defend permanent neutrality". Together with the constitutional amendment, the Austrian parliament unanimously adopted a resolution in 1975 "on the fundamental formulation of Comprehensive National Defense in Austria" (defense doctrine). These were the foundations of the current national defense plan, which was adopted by the Austrian government in 1983 and identified the "protection of the country's population and fundamental values from all threats" as a basic goal of Austrian security policy.

80 Security and Defense Doctrine. Analysis – draft expert report of 23 January 2001.

the *Chief Information Office Austria*[81] in close co-operation with the *Federal Chancellery* and the *Ministry of Internal Affairs* was set up for this purpose.

Y2K Efforts

A special working group under the lead of the IT coordinator was established in the Federal Chancellery in order to sensitize and mobilize governmental authorities for problems anticipated in connection with Y2K. This group coordinated and monitored the preparedness of the critical infrastructures (e.g. energy, transport, banking). A special working group of the Federal Chancellery called *Federal Crisis Management* was ready for emergencies. From 31 December 2000 until 3 January 2001, the special "Info point 2000" was in charge of gathering status reports and reports on severe problems from all other ministries, the federal counties, and other relevant institutions, namely the critical infrastructures.[82] Yet, all these efforts had only limited consequences for CIIP in the following years. It should, however, be noted that the CIRCA warning system uses comparable structures and methods for its work.

E-Government Program

The government program of the year 2000 recommends the implementation of so-called "e-Government" in Austria. E-Government[83] refers to two channels of communication: First, electronic communication between citizens and public administration (G2C),[84] and secondly, communication between different branches of public administration (G2G).[85] To make the Austrian e-Government secure, the Austrian seal of approval for e-Government was developed by the IKT board.[86] This seal of approval is issued by the Federal Chancellor Office only under certain conditions that have to be fulfilled for three years. After that period, approval can be renewed.

81 http://www.cio.gv.at.

82 *Zivilschutz aktuell*, No. 4/ 1999; pp. 13–19; Anfragebeantwortung 6111/ J XX. GP.

83 On the implementation of e-Government in Austria, see http//www.bka.gv.at and http://www.cio.gv.at/egovernment.

84 Methodology, basic principles, structure, and examples of this topic, see: Hollosi Arno. *Sicherheit mit offenen Standards für die Verwaltung* (Vienna, 2002).

85 E-Government in Austria also includes the pilot project "Bürgerkarte" (citizen card): see below.

86 http://www.cio.gv.at/egovernment/.

One essential part of the whole project is the guideline paper on "Network Safety in the Field of e-Government".[87] This guideline is currently being developed and will mainly deal with the technical aspects of network safety. It will be published after completion by the IKT-Staff Unit and after having passed the IKT-Board.

Official Austrian Data Security Website

The official Austrian data security website,[88] which is coordinated by the Federal Chancellery, serves as an information desk for citizens in important matters such as data security, the Schengen Information System, etc. It also informs the public about the work of the *Commission on Data Protection*. The reports of this commission are available on the website.

Pilot Project Citizen Card

The aim of this pilot project, which was launched in January 2003, is to reconsider the concept of "Bürgerkarten" (Citizen Cards). This is a chip card with encrypted information of the central registration office. This test run was initiated by the national provider of digital signature cards (a.trust), the Austrian Computer Society, and the IKT board of the Federal Chancellery.[89]

Organizational Overview

Public Agencies

Currently, the main responsibility for CIIP lies within the public sector. So far, no single authority is responsible for CII/ CIIP.

Generally speaking, all ministries have their own specific security measures to defend against outside attack and to prevent the unauthorized usage of data, and all ministries have special departments for Information

87 "Netzwerksicherheit im Bereich e-Government".
88 http//www.bka.gv.at/datenschutz/index.
89 *Kurier* newspaper, 28 November 2002.

Technologies. A Chief Information Officer (CIO) leads these departments.[90] Ministerial security concepts rest on two pillars: Pillar 1 refers to organizational and procedural measures to protect the internal network in general. Pillar 2 refers to technical means for the protection for sensitive data.

Ministry of Internal Affairs

Several divisions of the Ministry of Internal Affairs deal with CII/CIIP, especially with aspects of data security and cyber crime. Division V/8, for example, is responsible for data security in general.[91] The Criminal Police's homepage issues information on Internet security. The *Center for the Fight against Internet Crime*[92] was established in August 1999 under the auspices of the Ministry of Internal Affairs.[93] Austrian "Cybercops" represent Austria in the *European Network of Forensic Science Institute on Computer Crime* (ENFSI).[94] As medium-term measures to combat cybercrime more efficiently, the following steps are planned:

- an increase of the personal staff in the department II/BKA/16,
- further rationalization,
- stronger cooperation with the Austrian economy/private sector,
- more information for the public.[95]

Ministry of Defense

In the framework of the Ministry of Defense, Department II (the so called control- department) is responsible for matters concerning all aspects of information warfare. It fulfills its duties in close cooperation with the newly established "Leadership Support Command" and the two military intelligence services.[96]

According to the Austrian constitution, the Austrian army is not only responsible for national defense, the maintenance of internal order, and internal

90 *The Security Handbook of the Federal Government* provides guidelines for CII security measures; these measures are implemented and realized by the ministries at their own discretion. The complete handbook is available at http//:www.cio.gv.at/securenetworks/sihb/.

91 Interview with a BMI representative; see also the portfolio of the Ministry of Internal Affairs.

92 Zentralstelle zur Bekämpfung der Internetkriminalität.

93 The Center for the Fight against Internet Crime has been part of the Federal Criminal Office since 2001.

94 http://www.bmi.gv.at/web/bmiwep.nsf/A11Pages/BMI020211131?OpenDocument.

95 http://www.bmi.gv.at/web/bmiwep.nsf/A11Pages/BMI020211131?OpenDocument.

96 "Heeresnachrichtenamt" and "Heeresabwehramt". Interview with a representative of the Ministry of Defense, December 2002.

security, but also for the protection of the constitutional institutions, their capacity to take legal actions, and the democratic freedom of the Austrian citizens. These duties also include the protection of critical information infrastructures. These protective measures have been subjected to several exercises held in close co-operation with the civilian institutions.

Board of Information and Communication Technology Strategy (IKT Board)

The *Board for Information and Communication Technology Strategy*[97] (IKT Board) was established in July 2001 as part of the *Chief Information Office* and was based on a decision of the Council of Ministers of 6 June 2001 referring to a "restructuring of the government's IT strategy". It is located at the *Ministry of Public Service and Sports*. This institution deals primarily with all aspects of e-Government; including security measures, such as the Austrian IT Security Handbook for the public administration[98] and the seal of approval for secure and trustworthy e-Government.[99]

Government Headquarters for Information and Communication Technology Strategy

The *Government Headquarters for Information and Communication Technology Strategy* was established in July 2001. The main task of this institution is the coordinated implementation of e-Government at all levels of the public administration. It is also responsible for IT security in these areas. Several working groups are tasked with analyzing and advancing awareness of these topics. The *Government Board for Information and Communication Technology Strategy* published an updated version of the IT Security Handbook in 2001. This handbook gives an overview of IT security in general and informs readers in a broad and comprehensive way about fundamental aspects and measures in the field of IT.[100]

Commission on Data Protection (DSK)

The *Commission on Data Protection* (DSK) serves as independent control authority that deals with data processing in the public as well as in the private sector. The DSK is located at the Federal Chancellery; it is chaired by a judge. All citizens have the right to appeal to this commission in case of a (supposed) violation of their rights in the field of data security. The

97 Stabsstelle IKT-Strategie des Bundes.
98 http://www.cio.gv.at/securenetworks/sihb.
99 http://www.guetesiegel.gv.at.
100 The complete handbook is available at http:www.cio.gv.at/securenetworks/sihb/.

commission verifies these claims and takes measures to remedy confirmed violations. A Data Processing Register located at the DSK is the central collecting point for personal data that has to be reported.

Public Private Partnerships

"Security in the Internet" Initiative

The cooperative initiative between the Ministry of Internal Affairs and the chamber of commerce was launched in October 2002. The main aim is to improve the prerequisites for IT infrastructure and to foster the confidence of enterprises and costumers in the Internet.

A first step was the establishment of a common expert working group, composed of representatives of the Ministry of Internal Affairs and 80 of Austria's top 500 companies. Further steps include an information campaign in 2003 ("Telefit-road-show") and further research in the field of the Internet and the economy.[101]

Center for Secure Information Technology Austria (A-SIT)

A-SIT was founded in May 1999 as an association supported by the Austrian National Bank, the Ministry of Finance, and the Graz University of Technology. Its tasks include general monitoring of IT security[102] and the evaluation of encryption procedures.[103]

Early Warning Approaches

Austria has an early warning system for nuclear catastrophes[104] and natural and technical disasters that is primarily based on bilateral treaties and national (public and private) efforts.[105] However, to date, no comprehensive and coordinated early warning system for attacks on critical information systems is in place or planned.

101 Die Bundepolizei, No. 6/ 2002; p. 78, *Die Presse* newspaper, 18 September 2002.

102 A-SIT makes tools and demonstration examples available at the homepage of A-SIT: http://demo.a-sit.at.

103 http://www.a-sit.at/asit/asit.htm.

104 This is primarily provided by the so called "Strahlenfrühwarnsystem", which is in the responsibility of the Ministry for Enviroment and Argiculture.

105 The central institution is the so called Bundeswarnzentrale (Federal Emergency Operations Center), located at the Ministry of Internal Affairs.

Computer Incident Response Coordination Austria (CIRCA)

Computer Incident Response Coordination Austria (CIRCA) is Austria's main organization in the field of IT early warning systems. It is a public private partnership whose main actors are the Federal Chancellery, the *Federation of the Austrian Internet Service Providers* (ISPA), and the *Center for Secure Information Technology Austria* (A-SIT). It is a web of trust between Internet Service Providers (ISPs), IP network operators from the public and private sectors, and enterprises in the field of IT security. The electronic communication network of the private sector is run by ISPA, whereas in the public sector the Federal Chancellery has the lead.

The aim of this Austrian security net is to provide an early warning system against worms, viruses, DDOS attacks, and other threats that endanger IP networks and their users. Therefore, CIRCA issues alerts and risk assessments and provides information about precautionary measures.

The organizational platform was established after the "Love Bug" virus caused significant damage to Austrian IT systems. It took some time to identify the main actors that would be willing to participate in a warning system. The next steps involved the construction of a technical system and a pilot phase.

This pilot system consists of two list servers run by the Federal Chancellery and the ISPA. Depending on the severity of the incident, warning or alarm messages can be released to the subscribers of the system. The subscriber base (between 12 to 15 individuals) is limited to persons that are able to contribute to the system. Furthermore, a help forum and a discussion list have been implemented. In this setting, the system allows specialists to communicate about incidents, be they in the private or the public field. After an assessment, countermeasures can be discussed and put in place.

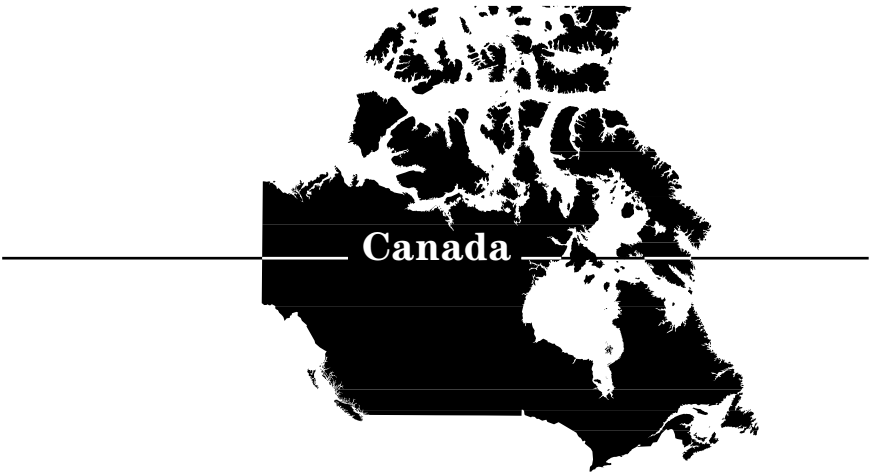
One important measure in the establishment of a reporting system is to agree on codes of conduct. These rules govern the behavior of the participants and especially the handling of sensible information provided by the system. Since members include competing companies, it has to be clear that the messages and information that circulate on the CIRCA system have to be treated confidentially. If this rule were flaunted, nobody would report really interesting facts.

The system is now switching to standard operation, and the positive effects of expert communication in different fields of IT security on the evaluation of incidents and possible countermeasures are evident. The next step is to place more sensors in the net to be able to react faster to possible attacks.

The members of CIRCA participated in the European Commission's efforts to establish a *European Warning System*. CIRCA can be seen as the Austrian part of an international system, and CIRCA will cooperate in the setting of the *European Network Security Agency* (ENISA).

In the aftermath of 11 September 2001, a preliminary crisis group was established that could deal with a situation where the main ISPs or even the net itself would not be operational. The goal was to be able to coordinate measures to minimize the possible Internet downtime.

CIIP Country Surveys



The Country Survey of Canada 2004 was mainly written by Shannon Hiegel, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), Canada. In addition, Louise Forgues, Colin Knight, and Paul Pagotto from OCIPEP as well as Dan Lambert, Solicitor General Canada, provided valuable input.

Canada

Critical Sectors

In Canada, CI is made up of clearly identified components that come together under the heading of National Critical Infrastructures (NCI). "Canada's critical infrastructure consists of those physical and information technology facilities, networks and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."[106]

Canada's NCI is grouped into ten sectors with sub-sectors. The identification of these sectors was a dynamic process of dialog involving domestic stakeholders and the exchange of information on the international scene. The sectors are the following:[107]

- Communications and Information Technology (Telecommunications, Software, Hardware, Networks (Internet)),
- Energy and Utilities (Electrical Power, Natural Gas, Oil Production and Transmission Systems),
- Finance (Banking, Securities, Investment),
- Food (Food Safety, Agriculture and Food Industry, Food Distribution),
- Government (Government Facilities, Government Services (e.g., Meteorological Services), Key National Symbols (Cultural Institutions and National Sites and Monuments),
- Health Care (Hospitals, Laboratories, Pharmaceuticals),
- Manufacturing (Chemical Industry and Defense Production, Defense Industrial Base),
- Safety (Chemical, Biological, Radiological, and Nuclear Safety; Hazardous Materials; Emergency Services (Police, Fire, Ambulance, and others)),
- Transportation (Air, Rail, Marine, Surface),
- Water (Drinking Water, Wastewater Management).

106 http://www.ocipep.gc.ca/critical/index_e.asp.

107 J.E. Harlick (OCIPEP): Understanding Critical Infrastructure Protection. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century'*, Stockholm, 17–18 November 2003.

Initiatives and Policy

Canadian cyber-protection activities focus on awareness and the resilience of information technology systems and assets. This includes components such as telecommunications, computers and software, the Internet, and satellites, as well as interconnected computers and networks and the services they provide.

Policies and programs (such as the *National Critical Infrastructure Assurance Program*, NCIAP) are in place or under development to ensure that Canada is prepared for attacks and has the ability to recover key services as quickly as possible. The government of Canada wants to be in a position to identify threats to vulnerabilities in advance and to disruptions as they happen, allowing it to quickly issue warnings and provide guidance to owners and operators of critical infrastructures.

To provide credible national leadership, the government of Canada must first ensure an adequate level of protection for its own portion of the national critical infrastructure (in the physical realm and in cyberspace). This means having emergency plans, contingency plans, and business continuity plans for government systems, processes, and assets. The Government Security Policy prescribes the application of safeguards (physical and virtual) for federal departments and agencies.

Government-on-Line (GoL)

The government plans to implement 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 *Government-on-Line* (GoL)[108] 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).

The secure channel is a major component of the technology infrastructure that will allow citizens to access federal services over the Internet reliably and securely, and is a key part of the government's plan to get government programs and services on-line by 2005.

108 http://www.gol-ged.gc.ca/index_e.asp.

Information Technology Systems Research and Development

Several federal government agencies have research and development expertise in the area of information infrastructure protection. These include the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP), *Defence Research and Development Canada*, the *Communications Security Establishment*, and *Industry Canada's Communications Research Centre*. These agencies have formed a joint working group to collaborate on information infrastructure research projects and to develop a joint long-term research agenda.

This initiative has led to a more efficient allocation of research funding, better sharing of expertise and awareness of research trends, and an improved understanding of the research capabilities and gaps within the government of Canada. This extensive initiative is expected to expand to include other Canadian government departments, as well as to develop international linkages to other research councils.

National Critical Infrastructure Assurance Program (NCIAP)

The events of 11 September 2001 have accelerated the implementation of the *National Critical Infrastructure Assurance Program* (NCIAP) [109]. The Canadian government is working on this program together with the provinces, territories, and the private sector.

The overall aim is to promote a more resilient and viable national critical infrastructure through partnership between governments and the private sector. Such partnership will enable two-way information exchange and more directed research and development. It will also develop the means to better assess risks, vulnerabilities, threats, and interdependencies that can affect the continuity of the NCI.

The NCIAP is currently a framework for cooperative action. The short-term goal is to bring together organizations with a stake in better assuring CI/CII, so that an approach can be jointly developed and the exact nature of the partnership and methods of information exchange can be designed. The NCIAP will evolve with the emergence of new needs and the changing risk environment. Through consultation and planning, the NCIAP will evolve from its current framework status to a fully operational program with a powerful yet flexible charter.

109 http://www.ocipep.gc.ca/info_pro/fact_sheets/general/CIP_NCIAP_e.asp.

All stakeholders can participate in and benefit from an array of products, multi-jurisdictional partnerships for information and sharing best practices, R&D efforts, training and awareness programs, and sectoral, regional, and national-international exercises.[110]

Readiness and Response Review

The *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) is coordinating the development of frameworks to help improve the readiness and response capability associated with emergency management (physical and virtual) both for the government of Canada as well as on a national basis, the latter to be a collaborative effort with major stakeholders and partners. This initiative is intended, when implemented, to provide more effective governance arrangements, to increase the coordination between the variety of initiatives and programs which constitute the substance of readiness and response, and to provide more effective management tools to maintain and adapt a readiness and response capability. Proposals to implement new arrangements are anticipated at the end of 2003.[111]

Information-Sharing

Information-sharing is arguably one of the most significant issues in CIIP. Canada has been working intensely to identify better ways to achieve this goal. Information-sharing can be viewed as a means to manage actions that can help deter, prevent, mitigate, and respond to the impact of a threat, as well as a tool to manage risk.

Canada is looking at the possibility of creating an information-sharing framework. This structure would provide a clear structure for the process of establishing information-sharing relationships, bridging silo-style structures, and encouraging consistent approaches among participants, while ensuring that such processes are workable for and relevant to all key stakeholders.

There is value in having centers for sharing and analysis of sensitive information about vulnerabilities, threats, intrusions, and anomalies within specific CI sectors. Government action alone cannot assure the protection

110 http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp.
111 http://www.ocipep.gc.ca/home/index_e.asp.

of vital services provided by CI in the current threat environment. The concept of information-sharing centers is important and Canada is considering with its partners whether and how such information-sharing mechanisms could be developed.

Organizational Overview

Public Agencies

In Canada, the lead agency dealing with CIP/CIIP is the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP).

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

Recognizing Canada's increased interdependencies and vulnerabilities in Critical Infrastructure, the prime minister of Canada announced in February 2001 the creation of the *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP)[112]. The decision to combine critical infrastructure protection and emergency preparedness responsibilities in one organization reflected the new risk environment, in which physical and cyber dimensions of infrastructures are increasingly interconnected. Combining critical infrastructure protection and emergency management resources and policy tools with acquired knowledge and experience in emergency preparedness should ensure a stronger, more integrated, and effective national security posture. Critical infrastructure protection and emergency management are not seen as separate endeavors, but as part of the assurance and protection continuum.

In December 2003, the Prime Minister has announced that OCIPEP (so far in the Department of National Defense) will be integrated into a new portfolio, *Public Safety and Emergency Preparedness*, in order to maximize emergency preparedness and response to natural disaster and security emergencies.[113] OCIPEP collaborates closely with federal actors in the areas of law enforcement (the *Royal Canadian Mounted Police* (RCMP)), the national security and intelligence service (the *Canadian Security Intelligence Service* (CSIS)), and sector departments (e.g., *Industry Canada* as the lead for relations with the telecommunications sector), as well as other

112 http://www.ocipep.gc.ca/home/index_e.asp.
113 http://www.ocipep.gc.ca/home/index_e.asp.

departments and agencies (e.g., the *Treasury Board Secretariat* and the *Communications Security Establishment* (CSE)). Through partnership-building, the government of Canada also works together with the private sector and provincial/territorial governments focusing on developing a seamless, well-coordinated approach to CIIP.

Interdepartmental Committee

The government of Canada has also instituted an interdepartmental committee of senior officials to discuss strategic policies and issues related to its cybersecurity posture. This committee provides guidance on dealing with incidents that could have a serious widespread impact, where the potential impact is unknown, where it may impact on several critical infrastructure sectors, when response and mitigation steps are not obvious, or when the incident has potential national or international consequences.

Public Private Partnerships

The Canadian private sector, which owns and operates most of the nation's infrastructure, plays a key role in securing cyberspace. National sector associations such as the *Canadian Electricity Association* (CEA), the *Canadian Bankers Association* (CBA), the *Canadian Telecommunications Emergency Preparedness Association* (CTEPA), and others have been active in promoting enhanced CIP efforts. Currently, Canada's CI sectors are working to enhance information-sharing among their members, with government, and between sectors.

It is increasingly recognized that information on threats, vulnerabilities, corrective measures, and best practices should be shared widely, across sectors and with governments. Canadian industry and governments at all levels are working together to improve information-sharing and analysis efforts. Industry sectors have identified a variety of challenges, including such issues as timeliness and relevancy of threat information. As industry efforts to increase mutual cooperation and information-sharing mature, so too will the national ability to respond to and manage cyber incidents and attacks.

Early Warning Approaches

Integrated Government of Canada Response System

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), in partnership with law-enforcement and national security agencies, is developing a new response and co-ordination structure for cyber-incidents, which includes the monitoring of cyber-threats 24 hours a day and 7 days per week, serving as one of several points of contact for threat and incident information.

If a cyber-incident is suspected of constituting a criminal offence or involves threats to national security, the federal police (*Royal Canadian Mounted Police* (RCMP)) or federal intelligence service (*Canadian Security Intelligence Service*, CSIS) are contacted directly. Recognizing that it may be difficult for a reporting party to determine whether an incident has criminal or national-security implications, such cases could be reported to the *Government Emergency Operations Co-ordination Center*, where the *Cyber Incident Coordination System* (CICS) *Cyber Triage Unit* would examine it. This unit is composed of officials from OCIPEP, the RCMP, and CSIS who will assess the incident to determine appropriate lead and follow-on action.

The *Cyber Incident Coordination System* provides a comprehensive, coordinated, and integrated system of response to cyber-incidents and vulnerabilities. It has several advantages, including:

- The ability to draw on specific and specialized information technology expertise and resources in several departments and agencies;
- the ability to respond rapidly to an incident and quickly disseminate critical information to stakeholders to reduce the risk of incidents being replicated elsewhere in the government, provinces/territories, the private sector, and other countries;
- the ability to assist provinces, territories, municipalities, the private sector, and international partners in protecting their information systems; and
- the ability to build upon the strong partnerships and expertise that departments and agencies have developed over the years in their respective fields with Canadian and international partners.

Internationally, Canada participates in global watch and warning activities. Discussions are underway between Canada and its international partners to share information in real-time and to detect and prevent cyber-incidents as they emerge.

Timely Alerts and Advisories

Responsible agencies within the government of Canada disseminate alerts, advisories, and other reports pertaining to relevant information technology threats, vulnerabilities, and remedies. There are several channels through which the government of Canada issues alerts and advisories in relation to its information infrastructure. One of the public channels is through the OCIPEP website.[114]

114 http://www.ocipep.gc.ca/opsprods/index_e.asp.

CIIP Country Surveys

Finland

The Country Survey of Finland 2004 was written with the help of Mika Purhonen, Ilkka Kananen and Veli-Pekka Kuparinen, National Emergency Supply Agency (NESA) as well as Markku Haranne, Ministry of the Interior, Rescue Services Unit.

Finland

Critical Sectors

In Finland, critical information infrastructure protection (CIIP) is perceived as vital to the national interest. Therefore, at the national level, Finland aims at ensuring the ability of society to function in all circumstances by securing the functioning of both official infrastructures and those administered by individual citizens and businesses.[115] As an information society, Finland can only function smoothly if its critical infrastructure is fully operational, because any disruptions to them may result in dramatic consequences. Accordingly, the *Security and Defense Committee* has proposed a strategy for securing the vital functions of society. A new government whitepaper on security and defense policy will be issued in 2004.

Protective actions are based on both the *Security of Supply Act* and the order of the *National Emergency Supply Agency* (NESA) of 1992.[116] The Finnish government set the official goals for the development of security of supply in 2002. According to that act, the most critical sectors in Finland are:

- Banking and Finance,
- Energy Supply,
- Food Supply,
- ICT-Sector,
- Industry Related to Defense,
- Media,
- Public Health,
- Public Services,
- Rescue Services,
- Social Welfare,
- Transportation and Logistics,
- Water Supply.

Because modern society is now more complex, technical, and networked, the main goal is to secure the national critical infrastructure on which the functioning of society depends.

115 Ministry of Defense. *Finnish Security and Defense Policy 2001.* Government report to parliament on 13 June 2001. http://www.defmin.fi/index.phtml/page_id/13/topmenu_id/7/menu_id/13/this_topmenu/7/lang/3/fs/12.

Finland's communication systems have traditionally been at a good level of preparedness. This is because the communications operators and providers have had a legal obligation to ensure the functioning of their services, regardless of whether the disturbances occur during normal times, exceptional situations, or in times of crises.

The Communications Market Act (2003) assures the operators that any extra expenses incurred through such preparatory measures will be reimbursed to the operators by the National Emergency Supply Agency (NESA).

Initiatives and Policy

Governmental Support for Information Society

Over the last couple of years, the Finnish government has worked continuously on new programs aimed at promoting the information society, its infrastructure, and the protection of the infrastructure. Several studies about the development of the information society were published in the 1990s. The Ministry of Transport and Communications published a report called *National Outline Policy for the Development of Information Networks 1995–1998*, which evaluated measures to upgrade the infrastructure for data exchange.[117] On the basis of such reports, various ministries produced action plans and provided funding for information society projects. The Ministry of Finance established a *National Information Society Committee* and an *Information Society Forum*. The Ministry of Transport and Communications concentrated on the creation of the technical prerequisites of the information society and on safeguarding network services.[118]

In 2000, the Ministry of Finance published the first report of the *Information Society Advisory Council* titled *Finland as an Information Society*. This report aimed at outlining the present stage of Information

116 The Security of Supply Act (enacted in 1992) is the legal basis for ensuring supplies of various basic materials in the case of emergency situations. Based on the Act, the National Emergency Supply Agency (NESA), a subordinate agency to the Ministry of Trade and Industry, was formally founded in 1993 for the development and maintenance of security of supply. The NESA is the national stock holding agency of Finland (see below for more details). http://www.iea.org/pubs/reviews/files/finland/05-fin.htm.

117 Ministry of Transport and Communications. http://213.138.148.10/finfo/english/ahoneng.html.

Society development and at evaluating the social and economic effects of the Information Society. The report also dealt with the domestic regulatory framework and with measures and programs in the public sector for the promotion and development of the information society.[119] The same ministry on 26 March 2001 published a report on *Finland in eEurope*[120], where the following areas were identified as important for Finland: facilitating the participation of all in the information society, the acceleration of e-Commerce, and e-Government and secure networks.

Finnish Security and Defense Policy 2001

The Ministry of Defense on 13 June 2001 submitted the *Finnish Security and Defense Policy 2001* report to parliament. The document states that the broader concept of national defense includes military, economic, and civil defense as well as social welfare and healthcare, the functioning of technical systems in society, public order and security, and defense information activities. This report also dealt with precautionary measures and the combating of threats confronting modern society: "The precautionary measures cover both military and civilian measures […] and are based on extensive cooperation as the activities in different sectors of society become more interdependent."[121] The *Security and Defense Committee* is responsible for defining the areas vital to the functioning of society and is in charge of drafting a national strategy for precautionary measures. The aim is to prevent situations that could undermine the functioning of society and to create mechanisms for managing such situations and their consequences.

The report states that telecommunications and information system security is becoming increasingly important for the uninterrupted operation of various sectors in society. Networking has increased and logistical systems have changed. The vulnerability of the technical infrastructure of society has increased, and disruptions can cause considerable harm to the functioning

118 http://213.138.148.10/finfo/english/ahoneng.html.

119 Information Society Advisory Board. *Finland as an Information Society. Report of the Information Society Advisory Board to the Government* (Helsinki 2000). http://www.vn.fi/vm/english/public_management/information_society.pdf.

120 Ministry of Transport and Communications. *Finland in eEurope. Summary* (March 2001). http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2001/16en_tiivistelma.pdf.

121 Ministry of Defense. *Finnish Security and Defense Policy 2001. Government report to parliament on 13 June 2001*, p. 5. http://www.defmin.fi/index.phtml/page_id/13/topmenu_id/7/menu_id/13/this_topmenu/7/lang/3/fs/12.

of society. Therefore, those vital systems must be secured through national measures (CIIP). In precautionary measures to safeguard the operation of technical systems in society, the focus has been on telecommunications, public broadcasting, and major information and payment systems as well as energy supply, transmission, and distribution systems. A bill has been submitted to parliament on the subject of CIIP.[122]

Advisory Committee for Information Security (ACIS): Information Security Review and Strategy

The government has set up the *Advisory Committee for Information Security* (ACIS) as a point of contact for citizens, companies, organizations, and authorities on information security issues. ACIS belongs to the *Finnish Communications Regulatory Authority* (FICORA) (see below) and advances the general awareness of information security. It formulates proposals for information security strategy, makes suggestions on how to update the strategy, and oversees the implementation of objectives and measures within the framework of the development agenda. ACIS reports to the Council of State and provides a forum for handling information security issues that brings together various parts of society.[123]

The first stage of ACIS' work was the publication of the *Information Security Review*[124] in June 2002, which deals with the most important information security threats affecting Finland and recommends steps to be taken by all parties to promote information security. The committee expressed its vision – focusing on trust and to be attained by the year 2010 – as follows: "Finland will be an information-secure society that everyone can trust and that enables all parties to manage and communicate information safely." In November 2002, ACIS released its *National Information Security Strategy Proposal*,[125] which was approved by the government on the 4 September

122 Ibid. Section IV: precautionary measures and combating threats to society.

123 Rauni Hagman, Director-General, Finnish Communications Regulatory Authority (FICORA). *ICT Security – Finland's Strategy and Action Plan*. International Northern eDimension Forum in Pori, 11–12 November 2002. http://www.pori.fi/ned2002/esitykset/hagman_p.pdf.

124 Finnish Communications Regulatory Authority (FICORA). *Information Security Review related to the National Information Security Strategy* (May 2002). http://www.ficora.fi/englanti/document/review.pdf.

125 Proposal of the Advisory Committee for Information Security. *National Information Security Strategy Proposal* (25 November 2002). http://www.ficora.fi/englanti/document/infos.pdf.

2003. The paper states that information security risk management will be developed by improving society's ability to cope with disruptions as well as by advanced recognition of information security risks and by protecting critical infrastructure. The paper lists detailed policy objectives and measures to be implemented as well as the responsibilities of the various stakeholders.

E.finland

E.finland provides information on Finnish IT know-how and the Finnish information society, in particular e-Business, e-Government, e-Health, e-Environment and R&D in this field. E.finland is built and maintained in co-operation with the Ministry for Foreign Affairs, the Ministry of Finance, the Ministry of Transport and Communications, the Ministry of Education, the National Technology Agency (Tekes), the Finnish National Fund for Research and Development (Sitra), and the TIEKE Finnish Information Society Development Center.

Organizational Overview

Public Agencies

In Finland, the key authorities responsible for CIIP are located within the Ministry of Transport and Communications (FICORA) and the Ministry of Trade and Industry (NESA; NBED) on the one hand, and within the Ministry of Finance (VAHTI) on the other hand, as well as in the private sector (TIEKE).

Finnish Communications Regulatory Authority (FICORA)

The *Finnish Communications Regulatory Authority* (FICORA) belongs to the Ministry of Transport and Communications and continues the operation of the *Telecommunication Administration Centre*, which was established in 1988. FICORA's mission is to promote the development of the information society in Finland, which includes issuing technical regulations and the co-ordination of standardization work at the national level. FICORA also has duties concerning the protection of privacy and data security in electronic communications, and encourages national and international co-operation. An important objective of FICORA is to enhance knowledge of information security so that citizens, companies, communities, and the state administration are aware of how critical information security is.

Another task of FICORA is to ensure that the telecommunications operators are prepared for emergencies. The operators must report to FICORA significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services.[126] FICORA checks operators for compliance with the *Communications Market Act* (393/2003) and the *Act on the Protection of Privacy and Data Security in Telecommunications* (565/1999) as well as for compliance with the relevant technical regulations and standards. In pursuing this task, FICORA collects information about the operators and carries out inspections.[127]

Two working groups focusing on information security had been set up by FICORA by the end of 2001:

- The COMSEC (communications security) group, whose main task is to ensure reliable telecommunications security and standardization, and
- the national CERT group as a joint group representing information technology organizations, especially in the field of computer emergencies (see below).

National Emergency Supply Agency (NESA)

The *National Emergency Supply Agency* (NESA) is the cross-administrative operative authority for the security of supply in Finland. NESA[128] serves to develop co-operation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply. NESA has a growing role in assuring the critical national infrastructure by developing and financing the technical backup systems.

Finland's most essential communication and IT systems are located in the capital region; this is a very risky concentration. Therefore, the *National EDP Backup Center* was established to secure society's vital IT systems in various exceptional conditions. The center's actions have been evaluated, and there seems to be a growing need for its services. The *National FixedLine Telephone Backup Network* (built in the 1990s), is a digital and nation-wide separate network that was built to secure the vital public organizations' essential contacts, as well as those of other key subscribers in exceptional situations and crises. Both the Ministry of Transport and Communications

126 FICORA. *Annual Report 2001*, p. 74: http://www.ficora.fi/2001/VV_vsk2001.pdf.

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

128 http://www.nesa.fi.

and NESA are developing the network further so that it can also secure other telecommunication services in the future (e.g., e-mail and data).

In addition, NESA has financed several projects to secure the communication and broadcast systems. These projects and activities are related to emergency messaging, domestic and foreign broadcasting, protection against electromagnetic pulse (EMP), and the construction of circuitous routes for critical nodes of networks.[129]

National Board of Economic Defense (NBED)

Founded in 1955, the *National Board of Economic Defense* (NBED), under the auspices of the Ministry of Trade and Industry, supports and assists NESA activities. NBED also plans and co-ordinates economic preparations for implementation in the case of exceptional circumstances in Finland. It is the coordinating and expert organization that serves as a link between the authorities and various industrial branches, and includes many planning bodies in the area of information infrastructure, such as the Information Systems Section. The NBED produces reliable and necessary information for NESA activities.

Private sector enterprises and governmental organizations can develop the security of supply efficiently through preparedness and planning efforts. The NBED conducts these activities. Instructions and basic plans have been prepared for the ICT sector as well as for other vital branches of the infrastructure. In addition, the organization studies and follows up on risks and threats to the security of supply. Databases and methods have been developed to support and improve the level of readiness to act in exceptional situations.

Steering Committee for Data Security in State Administration (VAHTI)

The central government's data security and information management is steered and further developed by the Ministry of Finance. Guidelines are developed by the *Steering Committee for Data Security in State Administration* (VAHTI), a broad group of experts appointed by the Ministry of Finance ten years ago. For the central government, the issue of data security includes a number of sub-areas such as administrative data security, personnel security, physical security, data communication security, database security, and so on. The Ministry of Finance works in close cooperation with other ministries

129 Information provided by a representative of the Finnish National Emergency Supply Agency (NESA).

and agencies and supports and facilitates co-operation in the development of e-Government and electronic services in the state sector.[130]

Public Private Partnerships

Finnish Information Society Development Centre (TIEKE)

The *Finnish Information Society Development Centre* (TIEKE) is a key player in the development of the public and private information society in Finland. TIEKE was launched in 1998 when the functions and the personnel of the *Finnish Data Communication Association* (FDCA) and the *Finnish Association for Interactive Network Services* (TELMO) were combined. It provides basic security information to small and medium-sized companies and has a key networking role as a neutral and non-profit organization in promoting the efforts of its members in the public and private sectors alike. TIEKE's goal is to contribute to the sustainable development of the knowledge-based information society by supporting networking, interoperability, and the distribution of information to all interested parties. TIEKE's membership includes more than one hundred organizations and companies involved in the information society that operate at the crossroads of trade and industry, public administrations, and individual citizens.

Information Society Advisory Board

The members of the *Information Society Advisory Board* are drawn from both the public and the private sectors. The Board is part of the Ministry of Finance, which also appoints the Secretary-General of the Board. The Board is responsible for developing the information society, and takes related opportunities and threats into consideration. Furthermore, it makes legislative proposals relating to the information society and follows international developments. Finally, the Information Society Advisory Board promotes dialog between government and the business sector in information society development projects.[131]

130 http://www.financeministry.fi/vm/liston/page.lsp?r=2685&l=en.
131 http://www.financeministry.fi/vm/liston/page.lsp?r=3724&l=en.

Early Warning Approaches

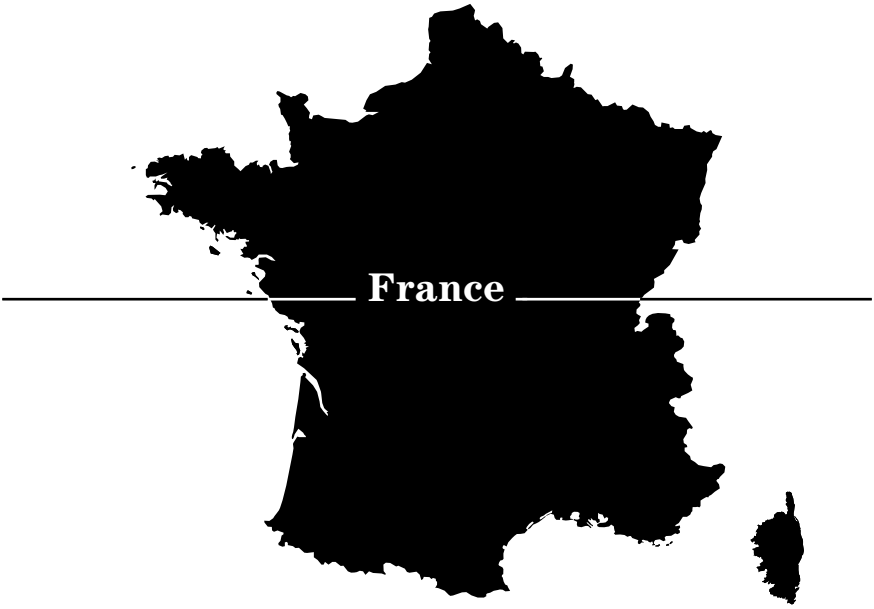
Computer Emergency Response Team Finland (CERT-FI)

Finland is devising a strong early warning and information-sharing network.[132] FICORA's CERT group (CERT-FI) began operations at the beginning of 2002, providing information and assistance to both organizations and individuals. CERT-FI works in co-operation with national and international organizations and receives reports from telecommunications operators on information security incidents and threats. CERT-FI functions include prevention and detection of these incidents, and providing information on them. The aim is to prevent and solve information security problems; supervising the communication networks through which viruses are spread is CERT-FI's responsibility. In the future, the duties of CERT-FI will include a 24-hour information security helpline. By the end of 2002, more than 800 individuals and companies had subscribed to the CERT-FI-ALERT mail service.[133]

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

133 http://www.ficora.fi.

CIIP Country Surveys



France

France

Critical Sectors

All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France. These critical sectors are the following:[134]

- Banking and Finance,
- Chemical and Biotechnological Industries,
- Energy and Electricity,
- Nuclear Power Stations,
- Public Health,
- Public Safety and Order,
- Telecommunication,
- Transport Systems,
- Water Supply.

Initiatives and Policy

Government Action Program for an Information Society (PAGSI)

In August 1997, the prime minister of France designated the information and communication society as a priority for government action. The objective was to build an information society for all, to prevent a digital divide, and to help France catch up with other countries in terms of Internet usage. Making government services available online has been the main goal of the formation of the *Government Action Program for an Information Society* (PAGSI)[135] in January 1998 (adopted at the meeting of the *Inter-ministerial Committee for Information Society* (CISSI)). In addition to the improvement of general public services, standardization, and training for civil servants, PAGSI supports projects in the fields of education, culture, electronic com-

134 Haut Comité Francais pour la Défense Civile. *Livre Blanc HCFDC: 20 ans, 20 constats et propositions*. 2003, p. 18. See also: Preparation for Y2K in France, sensitive sectors: http://www.urgence2000.gouv.fr/y2k/1.htm.

135 http://www.internet.gouv.fr/francais/textesref/essentiel-archives.htm.

merce, and research and innovation, and establishes appropriate regulations for the safer use of information technologies and networks. Two of the main priorities of the PAGSI action plan are managing the *Security of Information Systems* (SSI) (see below) and combating cyber-threats.[136]

Expression of the Needs and Identification of Security Objects (EBIOS)

In 1997, the *Directorate for the Security of Information Systems* (DCSSI) developed and published the first version of the guide *Expression of the Needs and Identification of Security Objects* (EBIOS).[137] It outlines a method for risk analysis concerning the security of information systems (for more details, see Part II).

Preparation for Y2K in France

The *Y2K French National Agency* was set up in 1998. Y2K Senior Officers were appointed in each ministry. The Agency, commissioned by the minister for economy, finance, and industry and by the secretary of state for industry, stimulated awareness of the Y2K issue in France, especially within the government services and small and medium enterprises (SMEs). The website "urgence2000" was established as an important information source for actors interested in the topic. The government's task was to make sure that the main infrastructures would be still functioning at the transition to the year 2000.[138] However, it does not seem that the Y2K experience was subsequently taken into consideration when dealing with information security policies.[139]

136 Service d'Information du Gouvernement. *Four years of Government measures to promote the information society* (August 2001). http://archives.internet.gouv.fr/francais/textesref/agsi4years.pdf.

137 Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical Guide – English Version, Version 1.02. February 1997.

138 http://www.urgence2000.gouv.fr/y2k/1.htm.

139 Dependability Development Support Initiative (DDSI) – Dependability Overview: *National Dependability Policy Environments*, p. 106, (September 2002).

Organizational Overview

In France, the *Secretary-General of National Defense (SGDN)*, a service attached to the Prime Minister's Office, bears complete responsibility for organizing CIP.

Furthermore, within the Ministry of Defense, the *Direction for Security of Information Systems*, (DCSSI), the *Inter-Ministerial Commission for the Security of Information Systems* (CISSI), and the *Advisory Office* are the key organizations responsible for CIP/CIIP, whereas in the Ministry of Interior, the *Central Office for the Fight Against Hi-Tech Crime* plays a comparative lead role.

Public Agencies

Secretary-General for National Defense (SGDN)

The *Secretary-General for National Defense* (SGDN) deals with national and international security affairs. The SGDN is directly subordinated to the French prime minister. The organization was first called into action for Y2K, when a specific network of contacts among different bodies from the public and private sectors became involved under the coordination of the SGDN.

The SGDN promotes and co-ordinates the activities between ministries involved in CIIP. This includes responsibility for the security of information systems (since 1996) and chairing the *Inter-Ministerial Commission for the Security of Information Systems* (CISSI),[140] as well as responsibility for the protection of classified and sensitive military information. The SGDN deals with the impact of the scientific and technical revolution on defense and security policy, focusing on securitization of information and communication technology relating to military as well as civil matters. In this area, the SGDN works closely together with DCSSI.[141]

Since its establishment, SGDN has been refined. One visible aspect is *Piranet*, an equivalent to *VigiPirate*, which involves all security forces (police and army) when the situation requires it, and decisions are taken at the prime minister's level; it deals directly with cyber crime, especially (but not exclusively) with attacks targeted at Critical Infrastructure.[142]

140 Commission interministérielle pour la Sécurité des Systèmes d'Information (CISSI).
141 http://www.premier-ministre.gouv.fr/fr/p.cfm?ref=6467&txt=1#contenu.
142 http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

Central Directorate for Security of Information Systems (DCSSI)[143]

The *Central Directorate for the Security of Information Systems* (DCSSI), which is linked to the *Secretary-General for National Defense* (SGDN), was created in 2000. The DCSSI administers the *Security of Information Systems* (SSI) website and co-ordinates its activities. The SSI website comprises information on the *Computer Emergency Response Team* (CERTA),[144] information on regulation, certification, authorization, electronic signature, and cryptography, and provides technical advice.[145] The DCSSI advises the French government, and it supports the national regulation authority and public services in the field of security of information systems. It builds up scientific and technical expertise in this field, evaluates threats, and issues alerts. It also has a training center for administration staff. Furthermore, it is responsible for the co-ordination of activities between the different government administrations.[146]

Advisory Office

A core operational part of the *Central Directorate for the Security of Information Systems* (DCSSI) is the *Advisory Office* (le bureau conseil), which assists the administration in CIIP matters. If it is in the overall interest of France's security, the *Advisory Office* also advises and collaborates with the private sector. In addition, the *Advisory Office* publishes methodological and technical guides to clarify concepts presented in the *Information Technology Security Evaluation Criteria* (ITSEC)[147] (see Part II for more details).

Central Office for the Fight Against Hi-Tech Crime

In May 2000, the *Central Office for the Fight against Cyber-Crime*[148] was launched by the Ministry of Interior and co-operates with Interpol. It deals with unauthorized intrusions and crime in the field of information and communication technologies and supports the legal investigations in this

143 Direction Centrale de la Sécurité des Systèmes d'Information. (DCSSI): http://www.ssi.gouv.fr/fr/dcssi/index.html.
144 Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques: http://www.ssi.gouv.fr/fr/index.html.
145 http://www.ssi.gouv.fr/fr/index.html.
146 http://www.ssi.gouv.fr/fr/dcssi/index.html.
147 http://www.ssi.gouv.fr/fr/dcssi/conseil.html.
148 http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/missions.

field. The Central Office has been granted nation-wide jurisdiction in this matter and works closely together with the national police as well as the private sector. It provides assistance to all agencies responsible for fighting computer crime such as the police, gendarmerie, and sensitizes the actors at stake.[149]

Public Private Partnerships

The Strategic Advisory Board on Information Technologies (CSTI)

The *Strategic Advisory Board on Information Technologies* (CSTI)[150] was created in July 2000 by a government committee meeting on information society. It is chaired by the French prime minister. The CSTI is composed of leading entrepreneurs from industry and research and development. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the *6th European Framework Research and Development Program*. The CSTI, in particular, has the duty

- to communicate opinions and recommendations to the government on the studies and documents commissioned,
- to maintain a permanent dialog with representatives of industry and to improve co-ordination between private and public researchers (and the industry),
- to define national priorities and to select areas where more action is required,
- to provide general monitoring and warning services in the area of CIIP.

French Dependability Institute (ISDF)

The *French Dependability Institute* (ISDF) provides a forum for the private sector to discuss CIIP issues across a variety of industries. It is strongly supported by the *Department of Industry* as well as representatives from the automotive, military, and space industries and from professional organizations. ISDF fosters connections on information exchange with the industry and aims at becoming the official representative of France in international organizations in the field of CIIP.[151]

149 http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/missions.
150 Conseil Stratégique des Technologies de l'Information: http://www.csti.pm.gouv.fr.
151 DDSI – Dependability Overview: *National Dependability Policy Environments*, p. 108.

Every year since 1990, ISDF has launched a set of projects in connection with the activities of its members. These projects reflect current issues in the field of securing information systems such as reliability, availability, maintainability, safety, and security. As there are about twenty-five technical working groups at ISDF, gathered into seven colleges (management; methods and tools; maintainability; human factor; safety; education and standards; software and systems dependability), the propositions embrace the whole spectrum of safety and dependability topics.[152]

Early Warning Approaches

Computer Emergency Response Teams (CERTs) in France

In France, there are three different Computer Emergency Response Teams (CERTs) addressing three different constituencies: CERT-RENATER, CERTA, and CERT-IST.

CERT-RENATER has existed since 1993 and especially addresses research centers and academic institutions. CERT-RENATER gathers and provides information about information security and is dedicated to the membership of GIP RENATER, the *National Network of Telecommunications for Technology, Education, and Research*.[153]

The *Central Direction for the Security of Information Systems* (DCSSI) has hosted a Computer Emergency Response Team called CERTA[154] since 2000. CERTA deals in particular with the French administration services. As a center of expertise, it evaluates CIIP threats and gives advice, issues warnings, and provides information on how to prevent, respond to, and handle an attack against information systems.

CERT-IST (*CERT-Industry, Services, and Tertiary*) was launched in 1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group. It serves France's private sector as a contact point for security incident response. CERT-IST provides alerts and means of protection against computer attacks aimed at French enterprises. It also helps the association members with incident handling.[155]

152 http://www.bull.com/fr/isdf/pgena.htm.
153 http://www.renater.fr/.
154 http://www.certa.ssi.gouv.fr/.
155 http://www.cert-ist.com.

CERT-IST interacts with the French national security organizations SGDN and DCSSI, in conjunction with CERT- RENATER and CERTA.[156]

CLUSIF (Club de la Sécurité des Systèmes d'Information Français)

The *Club de la Sécurité des Systèmes d'Information Français* (CLUSIF) was created in 1984 and is a non-profit organization of over 600 members representing 300 corporations or administrative organizations. CLUSIF fosters the sharing of information and experiences between its members, keeps users informed about new IT security material, and provides IT security information and whitepapers. Furthermore, it is involved in CIIP activities related to education, raising awareness, and security threat analysis.[157]

The *Secretary-General of National Defense* (SGDN) is also an early warning actor, to the extent that the office coordinates the ministerial officials called High Functionaries of Defense (Hautes fonctionnaires de Défense).[158]

156 DDSI – Dependability Overview: *National Dependability Policy Environments*, p. 107.

157 https://www.clusif.asso.fr/en/clusif/present/.

158 Présentation des nouvelles orientations de l'Etat en sécurité des systèmes d'information. Séminaire DCSSI-AFNOR, 27 March 2003. http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

CIIP Country Surveys

Germany

The Country Survey of Germany 2004 was written with the help of Willi Stein, Dirk Reinermann, and Stefan Ritter, Federal Office for Information Security (BSI) as well as Thomas Beer, IABG.

Germany

Critical Sectors

The main assumption underlying CIIP in Germany is that both the government and society as a whole depend heavily on a secure infrastructure. Any elements of the infrastructure whose failure would result in supply shortages or other dramatic consequences for large parts of the population are defined as critical.[159] The following are the principal infrastructure sections defined as critical in Germany:

- Banking, Finance and Assurance,
- Emergency Services,
- Energy Supply (Electricity, Oil, Gas),
- Government and Public Administration (including Law Enforcement, Custom, and the Federal Armed Forces),
- Health Care (including Food and Water Supply),
- Telecommunications (Information and Communication Technologies),
- Transport.[160]

Generally, the awareness of the necessity to improve the safety and security of IT-dependent critical infrastructures, and the willingness to implement necessary measures, have slowly but steadily improved in Germany. The events of 11 September 2001 have added a certain sense of urgency, and international dialog has intensified.[161]

159 Federal Office for Information Security (BSI). *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit "Kritische Infrastrukturen in Staat und Gesellschaft"* (January 2002), http://www.bsi.de/literat/faltbl/kritis.pdf and Federal Ministry of the Interior: http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

160 http://www.bsi.bund.de/fachthem/kritis/kritis.htm.

161 http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

Initiatives and Policy

In the past five to ten years, many activities directly or indirectly related to the issue of critical infrastructure protection have been undertaken. They emerged from inter-ministerial activities begun in 1997 at the initiative of the federal minister of the interior, motivated in part by the study produced by the *US President's Commission on Critical Infrastructure Protection*. Since then, co-ordination and reporting have taken place at the ministerial level on a regular basis.

The strategy to protect IT-dependent critical infrastructures became more distinct during 2002 and was materializing in 2003. Responsibility for overall coordination remains with the federal Ministry of the Interior, which will call in the *Federal Office for Information Security* (BSI), the *Federal Law Enforcement Agency* (BKA),[162] the *Federal Office for Civil Protection and Disaster Response* (BBK), and the governmental disaster relief organization *Technisches Hilfswerk* (THW).[163] Besides those agencies, the *Office of the Chancellor of the Federal Republic of Germany*,[164], the *Federal Ministry of Justice*, the *Federal Ministry of Economics and Labour*, and the *Ministry of Defense* are involved.

CIIP strategy and methodology will be developed in close cooperation with private infrastructure providers. Public private partnerships will be supported in response to the need for joint efforts to enable adequate protection at the governmental and private-sector levels. A national protection plan will be developed by the government; international cooperation (within the G8, the EU, etc., as well as on a bilateral basis) will be expanded.

AG KRITIS

Initiated by the report of the *President's Commission on 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.[165] It consisted of the ministerial representatives, a steering committee, and a permanent office at the *Federal Office for Information Security* (BSI).

162 "Bundeskriminalamt": www.bka.de.
163 http://www.thw.de/english/.
164 Bundeskanzleramt.
165 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html, 6.

The mandate of AG KRITIS was:[166]

- To describe possible threat scenarios for Germany,
- to conduct a vulnerability analysis of Germany's crucial sectors,
- 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.[167] 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 risks.[168]

Here is an overview of the main results:[169]

- 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 considered to be hacking and unauthorized access to data.

The creation of the *AG KRITIS* was an important basis for all further activities of public agencies in Germany. Its work is carried on, e.g., by the *Federal Office for Information Security* (BSI).[170]

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"[171] issued its fourth progress report, *Security and Protection in the Internet* ("Sicherheit und Schutz im Netz").[172] The commission contributed

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

167 AG KRITIS. *Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS.* (Entwurfsversion 7.95, December 1999). 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. The report itself was never published.

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

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

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

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

172 http://www.bundestag.de.

to the collection and assessment of major risks linked to the new information technologies.[173]

Campaign for "Security in the Internet"

The campaign for "*Security in the Internet*"[174] is a combined initiative undertaken by the Ministry of the Interior, the Ministry of Economics and Labor, and of the Federal Office for Information Security.[175] 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.[176]

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 were to identify possible threats and to study countermeasures. By June 2002, the task force's publications included recommendations on protection against DDoS-attacks and information on 0190-dialers.[177] In 2003, a bill was introduced in both chambers of the parliament that will restrict the distribution of dialers.[178] This law will only permit dialers certified through the Regulatory Agency for Telecommunications and Posts[179] to operate.

Comprehensive Threat Analysis

In the fall of 2001, a comprehensive threat analysis for Germany was published by the *Ministry of the Interior*.[180] The IT section in this report is an

173 http://userpage-fu-berlin.de/~bendrath/Kritis-12-1999.html.
174 http://www.sicherheit-im-internet.de.
175 Bundesamt für Sicherheit in der Informationstechnik, BSI since 2000.
176 http://www.sicherheit-im-internet.de/home/home.phtml, and 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/sld005.htm
177 http://www.bsi.de/taskforce/index.htm.
178 http://www.bundestag.de/presse/hib/2003/2003_117/03.html.
179 http://www.regtp.de/en/index.html.
180 Bundesministerium des Innern. *Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bev-*

attempt to answer the questions identified by the *AG KRITIS* study. Besides other threats, information security is defined as crucial for security of the German society and the success of its economy. It states that all measures, techniques, and instruments necessary for the protection of the vital infrastructure systems that rely on information technology are available. Rigorous application of those measures would eliminate a vast proportion of the threat, and it now remains only to implement those instruments. The risk management approach to information security proposed in this paper delegates the responsibility to the individual company providing information infrastructure services.

Infrastructure Analysis Studies

In mid-2002, the *Ministry of Interior* and the *Federal Office for Information Security* (BSI) commissioned a series of systematic studies of the CI/CII sectors. These studies have been completed and are currently used to support the establishment of a database for instant information access in case of an emergency related to information infrastructures, and for continuous situation evaluation. The database is currently in the making and may become the foundation for interdependency research in and between different CI/CII sectors. This database contains basic information on the infrastructure sector gained through interviews, workshops, and standardized questionnaire. The *Federal Office for Information Security* (BSI) has established its own department for the protection of critical infrastructures.[181]

International Outreach

An initiative between the *German Ministry of the Interior*[182] and the *US Department of Homeland Security*[183] at the ministerial level established the basis for future cooperation to enhance the protection of computer systems and networks. As a mid-term measure, a joint early-warning system should be created.[184] This bilateral initiative is a complement to the already ongoing counter-terrorism efforts. Additionally, a joint exercise will simulate an international IT-security violation event. Furthermore, both parties agreed

ölkerung bei Grosskatastrophen und im Verteidigungsfall. (Berlin, October 2001). http://www.bzs.bund.de/bzsinfo/broschur/zsforschung/gefahrenbericht_2.pdf.

181 http://www.bsi.de/fachthem/kritis/index.htm.

182 http://www.bmi.bund.de.

183 http://www.dhs.gov.

184 http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_92348.htm.

to foster regular consultations in international organizations in order to enhance multilateral cooperation.

Federal Office for Civil Protection and Disaster Response (BBK)

In order to facilitate cooperation between the different levels of public authority, a *Federal Office for Civil Protection and Disaster Response* (BBK)[185] will be established.[186] One of the main functions of this agency will be information-sharing and resource allocation in case of an emergency. A public relations and information website has already been established.[187] This *German Emergency Preparedness Information System* (deNIS) provides general information about organizations, emergency potentials, and web links on emergency precaution and preparedness.[188]

Moreover, decision-makers at the federal and state levels will be enabled to pool, process, and distribute resources in cases of wide-ranging catastrophes. This is an attempt to overcome the problems of the federal structure, where responsibility for civil protection lies with the federal authorities in cases of armed attack, and with the state-level authorities in cases of catastrophes. In particular, securing the energy and food supply and a smooth functioning of the information infrastructure are regarded as elementary.[189] In a further stage of development, a secure and classified system called *deNIS II* will be established.[190] Every international request for emergency support from Germany will be handled through *deNIS*.[191]

Kirchbach Report

The *Kirchbach Commission*, established after the devastating flood of 2002 in the Free State of Saxony, analyzed the overall structure of the *German Emergency Protection System*. Besides the focus on the flood disaster, it

185 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
186 http://www.bmi.bund.de/dokumente/Rede/ix_92444.htm.
187 http://www.denis.bund.de.
188 Zentralstelle für Zivilschutz. *Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem.* (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.
189 http://www.bmi.bund.de/dokumente/Rede/ix_92444.htm.
190 Zentralstelle für Zivilschutz. *Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem.* (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.
191 http://www.bzs.bund.de/index2.html; Zentralstelle für Zivilschutz.

included a comprehensive analysis of existing facilities, and recommendations for future capacities to secure information and communications technology in cases of emergency.[192] This disaster and the conclusions of the Kirchbach report triggered a broad range of measures in a variety of ministries and agencies.

Guideline "Critical Infrastructure"

The *Federal Office for Information Security* (BSI) has published a security guideline on "Critical Infrastructure" that includes options going beyond basic IT security measures. Though the importance of such measures 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:[193]

- Define a business strategy for treatment of enterprise critical infrastructure,
- Assemble a stock of IT techniques and components in consideration of mutual dependencies,
- Define the criticality of processes and components,
- Verify and facilitate decision-making,
- Define appropriate measures and concepts.

Secure E-Government and BundOnline 2005

The *Federal Office for Information Security* (BSI) is supporting the e-Government initiative and the *BundOnline 2005*[194] program. The e-Government initiative aims at a consistent use of modern information and communications technology in order to make administrative processes more efficient and to facilitate an exchange between the business community, the public, and the administration.

The objective of the BundOnline 2005 initiative is to make about 400 federal administration services available online by 2005. Under this plan, the BSI was charged with developing the basic IT security component and

192 *Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002.* (2nd ed. 2003). http://www.sachsen.de/de/bf/hochwasser/programme/download/Kirchbach_Bericht.pdf.

193 Bundesamt für Sicherheit in der Informationstechnik (BSI). *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit* "*Kritische Infrastrukturen in Staat und Gesellschaft*". (January 2002). http://www.bsi.de/literat/faltbl/kritis.pdf.

194 http://www.bund.de/Service/english-.6118.htm.

with setting up the data security competence center. The BSI also published the e-Government manual covering all aspects of the subject of secure e-Government and presenting pragmatic approaches to their solution.[195]

Further Activities

Besides the above-mentioned activities, the *German Armed Forces* (Bundeswehr)[196] have initiated various steps within the field of CIIP. Most of these measures have concentrated on the vulnerabilities and response to potential information attacks, and on the active exploitation of information operations by the armed forces.

Currently, there are no comprehensive studies available to the public in Germany that analyze complex interdependencies between critical infrastructures. A survey for representatives of CI/CII business sectors was taken at an early stage of *AKSIS* (→ for more details see Part II) to systematically collect threats and expected damages to CII. The collected data was summarized in a matrix.[197] Some sector-specific studies have been published in the meantime, e.g., for the financial sector.[198]

Organizational Overview

An organizational analysis reveals that the professional lead for CIIP lies at the *Federal Ministry of the Interior* (BMI). The reason for the BMI's responsibility for CIIP is mainly historical. Out of the *Central Cipher Agency*,[199] which was tasked with computer security in 1986, an inter-ministerial board for security evolved with the acronym ISIT. The board was chaired by the Federal Ministry of the Interior. In 1989, the *Central Cipher Agency* was transformed into the *Central Authority for Security in Information Technology*, reflecting the increased significance of information systems for the functioning of the state and the economy. The development of a framework that would guarantee the safe and secure application of information

195 http://www.bsi.de/fachthem/egov/index.htm and http://www.bund.de/Service/English/BundOnline-2005-Model-Projects-.6131.htm.

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

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

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

technology was seen for the first time as a matter requiring urgent action. The main requirements of the framework were outlined as follows:

- Action to improve safety and security was urgently needed,
- Threat reduction is a task that lies within the responsibility of public authorities, and
- A federal agency should be in charge of risk analysis and the derivation of security concepts.

Therefore, a law was passed in 1990 establishing the *Federal Office for Information Security* (17.12. 1990, BGBl. I S. 2834 ff).[200] Germany's Minister of the Interior Otto Schily reorganized the agency in 2001, making it the central IT security service agency for all federal authorities.

The events of 11 September 2001 caused the government to make additional resources available under the heading of the "campaign against terrorism". Some of these additional funds were used to combat cyber-terrorism. Those funds were partly used for additional personnel in the *Federal Office for Information Security* (BSI).[201]

Public Agencies[202]

Federal Ministry of the Interior (BMI)

As the government agency responsible for ensuring Germany's internal security, the *Federal Ministry of the Interior* (BMI) is closely involved with CIP/CIIP.[203] This is where the relevant topics are dealt with and coordinated, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. The authority in charge of IT-related issues with regard to CIP is Department IT 3 (Security of Information Systems) under the *Federal Ministry of the Interior's Chief Information Officer*.

The Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI), one of the agencies under the *Federal Ministry of the Interior*, plays an especially important role in CIP. The BSI deals with all areas related to security in cyberspace

199 Zentralstelle für Chiffrierwesen.
200 http://www.jura.uni-sb.de/BGBl/TEIL1/1990/19902834.1.HTML.
201 Information provided by a representative of IABG.
202 Information provided by a representative of BSI.
203 http://www.bmi.bund.de/dokumente/Artikel/ix_93830.htm.

and takes preventive action in the form of analyzing IT weaknesses and developing protective measures, including the following:

- Internet security: analyses, concepts, advising;
- Management of the computer emergency response team (CERT) and virus center;
- Network security and cryptology, public key infrastructure (PKI) and biometrics;
- Critical infrastructure.

Federal Office for Civil Protection and Disaster Response (BBK)

In the area of physical security, the *Federal Office for Civil Protection and Disaster Response* (BBK) will be responsible for developing measures to improve physical protection.[204] Currently, this responsibility is discharged in cooperation with the *Federal Office of Administration* (BVA) under the heading of civil protection and disaster preparedness.

The Federal Bureau of Criminal Investigation (BKA)

The *Federal Bureau of Criminal Investigation* (BKA)[205] is responsible in the first instance for prosecuting crimes against the internal or external security of the Federal Republic of Germany and crimes involving damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society. Further, the BKA is the central agency for investigating crimes involving information and communications technology.

Federal Ministry of Economics and Labor (BMWA)

Since more than 90 per cent of Germany's critical infrastructure is in private hands, the *Federal Ministry of Economics and Labor* (BMWA)[206] also plays a role as its brief includes economic policy. With regard to the energy sector, one of the BMWA's tasks is developing the framework for securing the energy supply. According to Article 87f of the German constitution, the BMWA is also responsible for ensuring the availability of adequate telecommunications infrastructure and services.

204 http://www.bmi.bund.de/Annex/de_25112/Gesetzentwurf_fuer_die_Einrichtung_des_Bundesamtes_fuer_Bevoelkerungsschutz_und_Katastrophenhilfe.pdf.
205 http://www.bka.de.
206 http://www.bmwa.bund.de.

Regulatory Authority for Telecommunications and Posts (RegTP)

As part of this effort, the *Regulatory Authority for Telecommunications and Posts* (RegTP), within the remit of the BMWA, is responsible for enforcing the relevant regulations to ensure the reliability and security of telecommunications networks. According to the amended *Telecommunications Act*, telecommunications companies are obliged to take appropriate technical and other measures to protect software-driven telecommunications and data processing systems against unauthorized access and disturbances that can cause significant disruptions of telecommunications networks.

Other ministries involved

The *Federal Ministry of Justice* (BMJ) [207] is responsible for relevant legislation, in particular ensuring that national laws comply with the cybercrime agreement of 23 November 2001.

The *Federal Ministry of Defense* (BMVg) [208] is involved in the context of its responsibility for national defense and for maintaining troop readiness and performance.

The *Federal Chancellery* plays a coordinating role at the ministerial level. Additional ministries are also involved in CIP in connection with particular areas of responsibility.

Responsibilities are also distributed among the agencies within the remit of the various ministries. The *Federal Intelligence Service* (BND) and the *Federal Office for the Protection of the Constitution* (BfV) provide important information regarding the threat situation and possible domestic targets.

Public Private Partnerships

The prevalent assumption in Germany is that cooperation between the public and the private sectors is the best strategy.[209] There are several cooperation initiatives in Germany between public and private actors related to CIIP.

207 http://www.bmj.bund.de.

208 http://www.bmvg.de.

209 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.

Initiative D21

The *Initiative D21*[210] is the largest public private partnership in Germany. This economic initiative also deals with information security. The *Initiative D21* is a neutral platform, independent of party allegiance and of individual industrial sectors. Its work is based on the assumption 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" with 226 participants; all sectors of industry (not only ICT providers), institutions, and politics are represented.[211] The Initiative D21 has formed 5 task forces and 17 subtask forces. In the task forces, important topics are discussed and agreements are implemented. Some of the main activities of the task force on *e-Government/Security and Trust on the Internet* include:

- Composition of a networked D21-CERT;
- The *Federal Ministry of the Interior* and D21 support middle class enterprises in the application of IT security criteria. The taskforce has developed a code of practice for IT security criteria and their application;
- Composition and completion of an administrative public key infrastructure according to the signature law;
- Promotion, standardization, and distribution of chip cards.[212]

Partnership for Secure Internet Business

The *Partnership for Secure Internet Business*[213] is supported by the *Ministry of Economics and Labor* and was founded in May 2000. The partnership was initiated by the ministry together with ten prominent trade associations and companies.[214] The main actors in the *Partnership for Secure Internet Business* are the *Ministry of Economics and Labor*, from the public sector, and up to 40 trade associations and companies from the private sector.

210 http://www.initiatived21.de.
211 Including 94 member companies, 33 sponsors, 59 supporters, and 43 advisory council members.
212 http://www.initiatived21.de/english/index.php.
213 Partnerschaft Sichere Internet-Wirtschaft.
214 See http://www.sicherheit-im-internet.de.

Working Group on Infrastructure Protection (AKSIS)

Based on the assumption that the increasing dependability of society on CII means the associated risks must be studied in a comprehensive approach, the *Working Group on Infrastructure Protection* (AKSIS) [215] was established in 1999 on the initiative of the Center for Strategic Studies (ZES),[216] which belongs to the company IABG (*Industrieanlagen-Betriebsgesellschaft*).[217] The main purpose of AKSIS is to provide a forum for information exchange to analyze and 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 bringing together representatives of the public and private sectors (ministries, armed forces, police, telecommunication, energy, transport, banks, academia, etc.). Models for close cooperation between the government's CII protection initiative and AKSIS are currently being discussed.

Early Warning Approaches

CERT-Bund

The *Referat CERT-Bund* (CERT-Bund Unit) was established on 1 September 2001 at the *Federal Office for Information Security* (BSI). CERT-Bund is a central contact point charged with the security of data processors and networks of the federal public administration. CERT-Bund also offers some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[218] CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decisionmakers, and cooperation with existing CERTs.[219]

215 Arbeitskreis zum Schutz von Infrastrukturen, AKSIS.

216 Zentrum für Strategische Studien (ZES).

217 See http://www.aksis.de, and http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld010.htm.

218 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.

219 Ennen, CERT-Bund, 35.

Mcert

The study *CERT Infrastructure Germany*[220] was published in January 2002. It determined that a CERT addressing the needs of small and middle enterprises (SMEs) was required in addition to the existing CERTs (such as dCERT,[221] DFN-CERT,[222] S-CERT,[223] secu-CERT,[224] Telekom-CERT,[225] and CERT-Bund[226]). This gap was closed with the collaborative establishment of Mcert between the *Federal Ministry of Economics and Labour*, the *Ministry of the Interior*, and the non-profit organization BITKOM.[227] Some major IT players in Germany are already members and sponsors of this new body. Mcert addresses SMEs without in-house IT departments or security resources and provides them with a suitable warning service. Mcert was founded in May 2003, and services will be available beginning in December 2003 at www.mcert.de.

220 See http://www.initiatived21.de.
221 http://www.dcert.de/index_e.html.
222 http://www.cert.dfn.de.
223 http://www.s-cert.de.
224 http://www.secunet.de.
225 http://www.telekom.de/dtag/home/portal.
226 http://www.bsi.de/certbund/index.htm.
227 http://www.bitkom.org.

CIIP Country Surveys

Italy

The Country Survey of Italy 2004 was written with the help of Roberto Setola, Working Group for Critical Information Infrastructure Protection; Giovanna Dondossola, CESI, and Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment (ENEA).

Italy

Critical Sectors

The main premise underlying Italy's CIIP policy is that the welfare of most countries depends increasingly on information and communication technology (ICT) systems.[228] ICT plays an important role in a number of critical sectors of Italian society.[229] There is no official definition of critical sectors in Italy, but the following sectors are taken into consideration:[230]

- Banking and Finance,
- Civil Defense,
- (Tele-) Communication,
- E-Governance,
- Energy,
- Gas,
- Public Administration,
- Public Health,
- Transport Systems on Air and on Land,
- Water.

Initiatives and Policy

The subject of CIIP was officially discussed for the first time in a meeting held at the *Ministry of Foreign Affairs*, organized by the *Directorate-General for Economical Cooperation* of the same ministry in March 2000. It was a preparatory meeting to identify potential areas of scientific and technological cooperation between Italy and the US. A second important occasion to foster awareness of the problem was a *Workshop on Critical Information Infrastructure Protection* jointly organized between the *Italian Prime Minister's Office* and the US embassy in Rome in May 2002.

228 Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. *Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana* (ottobre 2003).

229 Ministero per l'innovazione e le tecnologie. *Le politiche governative in tema sicurezza*. http://securit.cineca.it/eventi/atti_290503/cilli.pdf.

230 Information provided by the Italian experts involved.

A follow-up *Working Group on Critical Information Infrastructure Protection* was set up at the *Ministry for Innovation and Technologies* in March 2003. All ministries involved in the management of critical infrastructures are represented inside the group, together with many Italian infrastructure operators and owners as well as some research institutes. The main goal of this Working Group was to help the Italian government to come to a better understanding of the problems associated with CIIP, particularly accidental and deliberate faults, and to provide a basis for the identification of organizational requirements and initiatives that could increase the robustness of critical infrastructures.

Critical Information Infrastructure Protection

The *Working Group on Critical Information Infrastructure Protection* in October 2003 released the document *Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana* (Critical Information Infrastructures Protection: The Case of Italy) offering a synthesis of its efforts. The document describes many elements of the Italian infrastructures, emphasizes their interdependencies and suggests CIIP policy strategies. In particular, the Working Group suggests that full responsibility for the correct implementation of a survivability policy should remain with the individual owners and operators of critical infrastructure, while the government should be responsible for the definition of an overall policy to minimize interdependencies and cascading failures. The document also suggests:

- The establishment of a *National Interest Group on Critical Infrastructure* (GdIN – Gruppo di Interesse Nazionale) that would survey the requirements of different owners and operators.
- The definition of a national research and development agenda in the area of Critical Infrastructure Protection.
- The realization of an Interdependencies Simulation and Analysis Center (SAI – Centro Virtuale di Simulazione e Analisi delle Interdipendenze).[231]

Action Plan for E-Government

The Italian government intends to reform the public administration to meet user needs, to provide modern services, and create public value. The necessary steps are outlined in detail in the e-Government Action Plan of June

231 Information provided by expert.

2000 .[232] One crucial step is the establishment of a model for e-Government. It must be based on a modern infrastructure that will ensure the efficient and secure provision of a number of basic functions. To achieve this goal, the *Ministry for Innovation and Technologies* has developed the following strategic reference points for e-Government:

- Service Provision,
- Digital Identification,
- Access Channels,
- Service Provision Agencies,
- Interoperability and Cooperation,
- Communication and Infrastructure.

The Government's Guidelines for the Development of the Information Society

On 28 May 2002, the *Committee of Ministers for the Information Society* welcomed the *Government Guidelines for the Development of the Information Society* published by the Ministry of Innovation and Technologies.[233] It is stated the Italian government's commitment to making Italy a leader in the digital age, stressed its dedication to modernizing the country through widespread use of new ICT in both the public and private sectors, and vowed to boost the country's competitiveness by accelerating e-Business and e-Government.[234] The *Government Guidelines* also deal with network security and introduce a national plan for ICT security and privacy. The aim of this security model is to increase network security; in particular, it aims to create trust and to convince consumers and businesses to use the Internet, especially in their dealings with government. The national plan is based on the following principal actions:

- The introduction of an *ICT Security Directive* (to define the basic minimum of security that all government departments must achieve);
- The establishment of a *National Technical Committee for ICT Security* (to co-ordinate all activities);

232 http://www.innovazione.gov.it/eng/egovernment/index.shtml.

233 Minister for Innovation and Technologies. *The Government's Guidelines for the Development of the Information Society.* (June 2002). http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

234 Ibid., p. 19f. http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

- The establishment of an organizational model for ICT security (to include guidelines, recommendations, standards, and certification procedures);
- The introduction of a *National Plan for ICT Security* (to specify the activities, areas of responsibility, and deadlines for the introduction of necessary standards and methods for security certification in government);
- The final certification of ICT security for the public administration within five years.[235]

Organizational Overview

Besides the *Working Group on Critical Information Infrastructures Protection*, the main Italian government bodies dealing with CIIP are the *Ministry of Innovation and Technologies*, the *Ministry of Communication*, and the *Ministry of the Interior* –(*Postal and Communications Police*).

Public Agencies

Ministry for Innovation and Technologies

The *Ministry for Innovation and Technologies*[236] is charged with promoting specific action plans and programs for the deployment of information technologies in order to improve governmental online services for citizens and business. A *Committee of Ministers for the Information Society* was set up in 2001 to support the development and use of information and communication technologies in public administration, as well in Italian society as a whole. The first meeting of this committee was on 19 September 2001. The following areas were chosen for priority action:

- Communications (it was decided to set up a joint Ministry of Communications and Ministry for Innovation and Technologies Task Force on Broadband Communication);
- Education and training;
- Small and medium-sized enterprises and legislative change.[237]

235 Ibid., pp. 65–66. http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.
236 http://www.innovazione.gov.it/eng/index.shtml.
237 http://www.innovazione.gov.it/eng/intervento/pol_soc_eng.shtml.

National Technical Committee on Computer and Telecommunications Security within the Public Administration

On 16 October 2002, the *Ministry for Innovation and Technologies* and the *Ministry of Communication* created the *National Technical Committee for ICT Security in the Public Administration*. The establishment of this new committee followed from the Directive on ICT Security for the Public Administration, which enacts EU recommendations with the important initial aim of achieving compliance with a set of minimum-security standards. The Technical Committee can therefore be seen as the operative arm of the new national IT security policy.[238]

The *National Technical Committee for ICT Security in the Public Administration* was constituted in July 2002 with support from the *Ministry for Innovation and Technologies* and the *Ministry for Communications*[239].

The committee aims to attain a satisfactory security level in information systems and digital communications, in compliance with international standards, in order to guarantee the integrity and reliability of the information. It prepares strategy proposals concerning computer and telecommunications security for the public administration; in particular, it develops:

- The Emergency National Plan for the security of information and communication technologies in the public administration. The committee annually verifies its state of advance, and proposes corrective measures if required;
- The ICT security national organizational model for the public administration. The committee monitors its level of activation and application.

Furthermore, the committee formulates proposals for regulating the certification and security assessment, as well as certification criteria and guidelines for ICT security certification in the public administration, on the basis of national, sectoral, and international norms of reference.

Finally, the committee elaborates guidelines for agreements with the Department of Public Administration for training public employees in ICT security. Among the other proposals, the group is to set up the Computer Emergency Response Team (CERT) for the Public Central Administration (CERT-PA). It will have a central "Early-Warning System" operating around the clock.

238 http://www.innovazione.gov.it/eng/comunicati/2002_10_11.shtml.

239 Minister for Innovation and Technologies. *The Government's guidelines for the development of the Information Society.* http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.

National Center for Informatics in the Public Administration (CNIPA)

The *Authority for IT in the Public Administration* (AIPA), founded in 1993, was transformed into the *National Center for Informatics in the Public Administration* (CNIPA) in 2003.[240] CNIPA belongs to the *Ministry of Innovation and Technologies*, and its head is nominated by the *Council of Ministries*. It addresses central and local administration, especially the elements responsible for IT systems in the public administration.[241] CNIPA's main task is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration.[242] CNIPA published a comprehensive guide on the protection of personal data in 2001.[243]

Ministry of Communication

The *Ministry of Communication* supervises postal and telecommunications services, acting personally as a regulator, as well as practicing a policy of coordination, supervision, and control – tasks that were previously in the purview of the *Ministry of Post and Telecommunications*.[244] It is involved in the definition of the security polices for communication and the Internet.

Permanent Working Group on Network Security and Communications Protection

The *Permanent Working Group on Network Security and Communications Protection* was constituted in 1998. It was composed of representatives of the Ministries of Communication, Internal Affairs, and Justice. Within the group, the "Subgroup Internet" deals with investigative and judicial matters related to the Internet. This subgroup is preparing a list of data that Internet Service Providers will have to supply to the police if so ordered by a judge. A similar list already exists for telephone companies. A coordination center was recently constituted to coordinate crime-fighting with other governmental institutions.[245]

240 http://www.cnipa.gov.it.
241 http://www.cnipa.gov.it.
242 http://www.cnipa.gov.it.
243 http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dl_030630.pdf.
244 http://www.comunicazioni.it/en/index.php?Mn1=5.
245 Information provided by the Italian experts involved.

The Postal and Communications Police

In 1992, the *Ministry of the Interior* issued a directive assigning to the state police specific responsibilities for IT and telecommunications security that are in fact carried out by the *Postal and Communications Police*. The *Postal and Communications Police* is a flexible organization with a staff of around 2000 highly trained officers, subdivided in a central service and placed at the peak of a structure involving 19 regional departments and 76 territorial sections. The *Postal and Communications Police* reviews communications regulations, studies new technical investigative strategies to fight computer crime, and coordinates operations and investigations for other offices. This police force also collaborates with other institutions – in particular with the Ministry of Communication and the Privacy Authority – and with private operators who deal with communications. As the Italian contact point for G8 country computer crime offices, it is available at all times. This particular organizational aspect guarantees a quick, qualified, and efficient response[246] in the event of a threat or computer attack originating nationally or internationally.

From a technical and operational point of view, the *Postal and Communication Police Service* will host and manage an emergency center at both the national and regional levels, in order to better deal with computer crimes against critical infrastructure and conduct preventive monitoring activities. The center will be a focal point for the evaluation of threats, thus providing adequate countermeasures to face such situations.

Establishment of a National Certification Body for the Information Technologies

The Ministry for Innovation and Technologies and the Ministry of Communication plan to establish the *Istituto superiore delle comunicazioni e delle tecnologie dell'informazione* (ISCTI) as the national body for security certification in IT. It will be responsible for certifying IT systems' compliance with ITSEC, SO/IEC IS-15408 (Common Criteria) or ISO standards.

246 http://www.poliziadistato.it/pds/english/specialist.htm.

Public Private Partnerships

Italian Association for Security in Informatics: CLUSIT

The *Italian Association for Security in Informatics* (CLUSIT) [247] is a non-profit organization founded in 2000. It is based at the *Department of Informatics and Communications* (DICO) at the University of Milan.[248] CLUSIT addresses individuals and organizations involved or interested in information security in order to promote awareness, continuous education, and information-sharing. The specific duties of CLUSIT are:

- To raise awareness concerning computer security among companies, the public administration, and citizens;
- To participate in and contribute to the development of laws, practical codes, and computer security at national and international level;
- To help define certifications for computer security professionals;
- To promote the adoption of methodologies and technologies to contribute to the improvement of the security level of the information infrastructure at all levels.[249]

National Interest Group on Critical Infrastructure: GdIN – Gruppo di Interesse Nazionale

The *Working Group on Critical Information Infrastructure Protection* has strongly encouraged the constitution of a forum, to be formed on a voluntary basis, of the owners and operators of critical infrastructure. This forum will serve as a meeting-point to exchange best practices, and report to the government institutions on needs and problems.

247 Associazione Italiana per la Sicurezza Informatica: http://www.clusit.it/homee.htm.
248 http://www.dico.unimi.it.
249 http://www.clusit.it/indexe.htm.

Early Warning Approaches

CERT-IT

The *Italian Computer Emergency Response Team* (CERT-IT) is the main body in charge of early warning at the technical level in Italy.[250] CERT-IT was founded in 1994 as a non-profit organization. It is mainly supported by the *Department of Informatics and Communications* (DICO) at the University of Milan.[251] CERT-IT is a member of the Forum of Incident Response and Security Teams (FIRST). Its main goal is to contribute to the development of security in the computer world. It promotes research and development activities in security systems, provides information about computer security, and has an expertise team for handling computer incidents.[252] CERT-IT has also developed an electronic forum in order to disseminate all information related to vulnerabilities in a timely and widespread fashion.[253]

Other CERT-IT activities in Italy include the GARR-CERT and the MoD CERT (Ministry of Defense). A CERT-PA is planned by the *National Technical Committee on Computer and Telecommunications Security* within the public administration. Its task will be to support the public central administrations.

Incident Response Italy: IRItaly

Incident Response Italy (IRItaly)[254] is a project of the Department of Information Technologies at the University of Milan-Crema that was presented on 10 June 2003 at the *First Italian Forum on Incident Response in the Information Security.* Its main aim is to inform the Italian scientific community, small and medium-size private organizations, and private and public actors on incident response issues.

250 http://securit.cineca.it/eventi/atti_290503/cilli.pdf.

251 http://www.dico.unimi.it/.

252 http://idea.sec.dsi.unimi.it/index.html.

253 Dependability Development Support Initiative (DDSI) – *Dependability Overview: National Dependability Policy Environments* (2002), p. 159.

254 www.iritaly.org.

CIIP Country Surveys

The Netherlands

The Country Survey of the Netherlands 2004 was written with the help of Eric Luiijf, TNO Physics and Electronics Laboratory, and Roland de Bruin, KWINT, ECP.nl.

The Netherlands

Critical Sectors

With the *Quick Scan* method (see Part II for more details) and in consultation with the industry and government, it was determined that the Netherlands' critical infrastructure comprises 11 sectors and 31 products and services. Infrastructures are deemed critical if they constitute an essential, indispensable facility for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term. In the Netherlands, critical sectors and (products and services) include the following:[255]

- Drinking Water (Drinking Water Supply),
- Energy (Electricity, Natural Gas, and Oil),
- Financial (Financial Services and Financial Infrastructure both Public and Private),
- Food (Food Supply and Food Safety),
- Health (Health Care),
- Legal Order (Administration of Justice and Detention, Law Enforcement),
- Public Order and Safety (Maintaining Public Order, Maintaining Public Safety),
- Retaining and Managing Surface Water (Management of Water Quality, Retaining and Managing Water Quantity),
- Telecommunications (Fixed Telecommunication Network Services, Mobile Telecommunication Services, Radio Communication and Navigation, Satellite Communication, Broadcast Services, Internet Access, Postal and Courier Services),
- Public Administration (Diplomacy, Information Provision by the Government, Armed Forces and Defense, Public Administration),
- Transport (Road Transport, Rail Transport, Air Transport, Inland Navigation, Ocean Shipping, Pipelines).

The Critical Information Infrastructure (CII) of the Netherlands consists mainly of the internal supporting infrastructure of critical sectors like the energy, transport, and financial sectors, and is supported by a set of

255 Ministry of the Interior and Kingdom Relations. The Netherlands, April 2003: Critical Infrastructure Protection in The Netherlands, p. 13–14.

services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, Internet access, electricity). It is explicitly not considered as an infrastructure in its own right. However, the KWINT program (see below) is targeted at the protection and safe use of the Internet.

Initiatives and Policy

In the Netherlands, CIP/CIIP is perceived increasingly as a crucial issue of national security. Since the end of the 1990s, several efforts have been made to better manage CIP/CIIP.

"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.[256] This memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructure and of mastering the growing complexities of advanced IT applications.[257]

Defense Whitepaper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the *Dutch Defense Whitepaper 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."[258]

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*

256 http://www.gbde.org/egovernment/database/netherlands.html.

257 Luijjf, 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), p. 5.

258 Ministerie van Defensie, *Defensienota 2000*, (1999), p. 59.

to stimulate the discussion on the need to protect CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in co-operation with the appropriate national public and commercial organizations.[259] 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 KWINT-manifest document is available only in Dutch.[260]

KWINT Report and Memorandum

The report entitled *Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid* (KWINT), written by Stratix/TNO[261] 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. 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.[262]

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*, *the Interior*, *Justice*, and *Transport* (Telecom and Post Directorate) [263]. As a result, the KWINT government memorandum (*Vulnerability of the Internet*) was endorsed by the cabinet on 6 July 2001. It includes a set of recommendations for action. A government-wide computer emergency response team (GOVCERT.NL) was established and a malware alerting service for SMEs and the public was set

259 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 "BITBREUK, de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij") (Amsterdam, March 2000).

260 http://www.infodrome.nl.

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

262 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).

263 The Telecom and Post Directorate (DGTP) became part of the Ministry of Economic Affairs as of 1 January 2003.

up. Other actions were tasked to ECP.NL, the public private platform for e-Commerce in the Netherlands.

The Dutch CIIP policy as laid out by KWINT 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.[264] The government policy is aimed at fostering wider application of ICT and an understanding of the consequences. In its report, entitled "Government losing ground", the WRR,[265] a government advisory body, analyzed some of the political aspects of the further advance of ICT across society.[266]

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.[267] The *National Co-ordination Center* (NCC), which is part of the *Ministry of the Interior and Kingdom Relations*, has been tasked with developing an integrated set of measures to protect the critical infrastructure within a multi-step project, called "Bescherming Vitale Infrastuctuur" (*Protection of the Dutch Critical Infrastructure*). This project will run until 2004 and comprises the following steps:[268]

- Quick Scan (see below),
- Public private partnership kick-off workshop,
- Investigation of vital nodes,
- Risk analysis generating a list of measures, which is compared to the list of measures already taken generating a balanced set of actions by government and industry.

In June 2002, 11 working groups were formed, one for each vital sector. In April 2003, the findings of the Quick Scan, performed in close collaboration with the *Netherlands Organization for Applied Scientific Research* (TNO) were published by the *Ministry of the Interior.*[269] The objective of Quick Scan was to give an overall view of the essential products and services that comprise the Netherlands' CI, to determine their interdependencies and to

264 De Bruin, From Research to Practice.
265 Wetenschappelijke Raad voor het Regeringsbeleid.
266 http://www.infodrome.nl/english/missie-eng.html.
267 House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.
268 Ministry of the Interior and Kingdom Relations. The Netherlands, April 2003: Critical Infrastructure Protection in The Netherlands, p. 9.
269 Ibid, p. 7.

consider the consequences of their possible breakdowns. (→ for details, see Part II, chapter 1 on Sector Analysis, Example 2).

In December 2002, the following main conclusions could be drawn from the Quick Scan results:

- The Dutch government and industry now have a clear understanding of the critical products and services that comprise the Netherlands' critical infrastructure, and of their (inter-) dependencies,
- The direct and indirect vitality of critical products and services have been elaborated,
- It became clear that actors responsible for critical products and services have merely a limited understanding of other critical products and services depending on them, and of the extent of this dependence.[270]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP will include risk and vulnerability analyses by sector, scenarios to test the effectiveness of CIP/CIIP measures, and international interdepartmental exchange of information and coordination.[271]

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 were 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 co-operation in this area, bringing in experts from other organizations in order to analyze and mitigate the problem. HERT will be fully operational in a few years.

Organizational Overview

Public Agencies

As stated above, responsibility for the Dutch CII lies with various actors and involves both public and private sectors as well as multiple ministries. In particular, the *Ministry of Economic Affairs/Telecom and Post Directorate* is responsible for the protection policy for telecommunications and the

270 Ibid, p. 23.
271 Ibid., p. 25.

Internet. Other parts of the same ministry are responsible for CIP/CIIP policies regarding the energy sector and private industry, including SMEs. The *Ministry of the Interior* is responsible (in terms of policy) for the protection of government information infrastructures and coordinates CIP policy across all sectors and responsible ministries.

Ministry of the Interior (BZK)

The duties of the *Ministry of the Interior* include the promotion of public order and safety and the administration of the national police forces. It includes the *National Co-ordination Center* (NCC), which is in charge of coordination activities at policy level in case of emergencies with nation-wide impact.

Ministry of Economic Affairs

The *Directorate-General for Telecommunications and Post* was subordinate to the *Ministry of Transport, Public Works, and Water Management* (V&W) until mid-2002. The directorate is now subordinate to the *Ministry of Economic Affairs*. The two most important goals are the strengthening of the Netherlands' competitive position in the field of telecommunications, telematics, and postal services, and to ensure that these facilities remain available to citizens and companies.[272]

Furthermore, this ministry is responsible for C(I)IP policy in the energy sector and within the private industry, including SMEs.

Ministry of Transport, Public Works, and Water Management (V&W)

The *Ministry of Transport, Public Works, and Water Management* (V&W)[273] is responsible for CI in transport and water management (quantity). The biochemical quality of the surface water lies within the responsibility of the *Ministry of Health* (VWS).

General Intelligence and Security Service (AIVD)

The *General Intelligence and Security Service* (Algemene Inlichtingen- en Veiligheidsdienst, AIVD, formerly called BVD[274]) is a division of the *Ministry of the Interior* and is tasked with information security and the protection of vital sectors of Dutch society.[275] The AIVD´s focus shifts in accordance

272 http://www.minez.nl/default_bel.asp?pagina=english.
273 http://www.minvenw.nl/cend/dco/home/data/international/gb/index.htm.
274 In December 2000, a total of 594 personnel were employed by the BVD.
275 http://www.fas.org/irp/world/netherlands/bvd.htm.

with social and political changes. One of its tasks is to uncover forms of improper competition such as economic espionage that could harm Dutch economic interests.[276] Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere.[277] The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

Public Private Partnerships

In general, public private partnerships in the Netherlands are organized by agreement between the actors.[278] The government is usually a facilitator bringing together the actors concerned.[279]

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

Public private co-operation within the project 'Bescherming Vitale Infrastuctuur' (Protection of the Dutch Critical Infrastructure) also involves the *Confederation of Netherlands Industry and Employers* (VNO-NCW) in a coordinating private-sector role.

Platform Electronic Commerce in the Netherlands (ECP.NL)

ECP.NL[280], the platform for *e*Netherlands, has been tasked by the *Ministry of Economic Affairs* with setting up a public private partnership program to implement the action guidelines of the KWINT Memorandum

The objective of the KWINT program[281] is to define concrete protective measures against the risks of Internet usage for businesses, consumers, the government, and citizens. A second objective is to provide a platform for public private partnership, and in this way provide a sounding board for government policy-making. The steering board and the various working groups consist of representatives of the government and the private sector.

276 http://www.minbzk.nl.
277 http://www.minbzk.nl.
278 This has been common practice in the Netherlands since the 13th century in the continuous struggle against flooding by rivers and the sea.
279 Interview with a representative of Netherlands' Organization for Applied Scientific Research (TNO), April 2002.
280 http://www.ecp.nl/ENGLISH/index.html.
281 http://www.kwint.org.

Acting on the recommendations of a risk analysis, the program is currently focused on the following aspects: continuity of the Internet infrastructure in the Netherlands, viruses, denial of service attacks, hacking, transparency of Internet services, integrity and confidentiality of information, and misuse by personnel.

Within the program, a best practice has been developed for defining solutions, creating commitment, and communicating solutions to end-users who will be implementing them. The program has delivered many different results, varying from complex risk analyses to practical tools. Commitment has been created not only among participants, but also among many stakeholders. To this end, public stakeholder debates are organized involving politicians, researchers, business executives, and users. KWINT Marketplaces are organized to present solutions to intermediary organizations that play a key-role in disseminating them to their members. These intermediaries also provide feedback to the KWINT program on the actual implementation of the solutions by their members. Finally, the program also actively anticipates and works in close co-operation with government on international developments, for example within the OECD and the European Union.

As stated above, the KWINT program also focuses on the continuity of the Internet infrastructure in the Netherlands. Since the Internet is regarded as one of the critical infrastructures, any results within this area of activities are also delivered to the CIIP initiative of the Dutch government. Apart from that cooperation, a liaison with the steering board and the government CIP initiative has been established.

Infodrome

Infodrome[282] is a think-tank founded in 1999 and sponsored by the Dutch government. 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 data on IT-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the 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* reflected the program's ambitious targets. The program was conducted under the direction of a steering

282 http://www.infodrome.nl/english/missie_eng.html.

group and presided over by a member of cabinet. In addition, participants included members of important policy think-tanks. All ministries were represented in the supervisory committee. The structure ensured that politicians, (political) scientists, and representatives of the administrative system were actively engaged in the development of government strategy vis-à-vis the information age.

Early Warning Approaches

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 involving SURFnet customers, either as victims or as suspects. 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 disasters).[283] CERT-NL disseminates information coming from CERT-CC/FIRST.

NLIP Security Coordination Group

Some 55 ISPs are organized within the NLIP (Brancheverenigingen van Nederlandse Internet Providers), the Netherlands Internet Providers' trade association. This independent association has existed since 1997.[284]

GOVCERT.NL

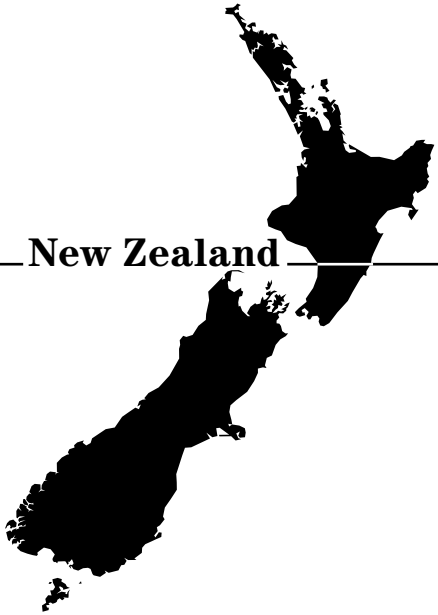
A computer emergency response team for government departments (CERT-RO) was established in June 2002. In February 2003, it was renamed GOVCERT.NL.[285] It is operated under the responsibility of the *Ministry of the Interior*'[286] under its ICT agency ICTU. GOVCERT.NL is co-located and co-operates with "Waarschuwingsdienst.nl",[287] a group that is responsible for issuing alerts and advice memoranda to the public and SMEs about

283 http://cert-nl.surfnet.nl/home-eng.html.
284 http://www.nlip.nl.
285 http://www.govcert.nl.
286 http://www.minbzk.nl.
287 http://www.waarschuwingsdienst.nl.

viruses, Trojan Horse codes, and other malicious software, or "malware". Warnings are disseminated via e-mail, web services, and SMS, will soon be issued via public radio and TV channels as well. The Waarschuwingsdienst was founded in early 2003 and is funded by the *Ministry of Economic Affairs/Telecom and Post Directorate.*

At the tactical level, the KWINT program focuses on improving general awareness of ICT security through best-practice procedures. This includes, for example, the free provision of the Dutch version of ISO/IEC 17799:2000 (or BS 7799), the "Code voor Informatiebeveiliging". Currently, no early-warning or incident-analysis capability is planned at the strategic national level. This is because CII is mainly considered to be a subsidiary of the individual CI sectors.

CIIP Country Surveys



New Zealand

The Country Survey of New Zealand 2004 was written with the help of Mike Harmon, Centre for Critical Infrastructure Protection (CCIP).

New Zealand

Critical Sectors

CIIP in New Zealand is about the protection of infrastructure necessary to provide critical services. "Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement."[288] New Zealand's critical sectors comprise the assets and systems required for the maintenance of:[289]

- Emergency Services,
- Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),
- Finance and Banking,
- Governance (including Law and Order and National and Economic Security),
- Telecommunications and the Internet,
- Transport (including Air, Land, and Sea).

Various critical sectors depend on each other. Most systems assume the continuity of power and telecommunications infrastructures and make extensive use of networked information technology in their management and control systems.

Initiatives and Policy

The New Zealand government's *Defence Policy Framework* is a crucial document that illustrates that CIIP is a key objective of the country's overall security policy. The *Centre for Critical Infrastructure Protection* (CCIP) addresses the cyber-threat aspects of that objective.

288 http://www.ccip.govt.nz/about-ccip/niip-report-final.htm#_Toc501363182.

289 E-Government Unit, State Services Commission. *Protecting New Zealand's Infrastructure from Cyber-Threats* (8 December 2000). http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

CIIP within the Defence Policy Framework

New Zealand's government promotes a comprehensive approach to security and aims to protect and maintain the country's physical, economic, social, and cultural security. In the government's *Defence Policy Framework* of June 2000, critical infrastructure protection is identified as one of the key objectives: "[…] to defend New Zealand and to protect its people, land, territorial waters, Exclusive Economic Zone, natural resources and critical infrastructure."[290]

Protecting New Zealand's Infrastructure from Cyber-Threats

On 8 December 2000 the report *Protecting New Zealand's Infrastructure from Cyber-Threats* was released by New Zealand's *State Services Commission's E-Government Unit*. The report deals with the protection of New Zealand's critical infrastructure from cyber-crime and other IT-based threats. The report assessed levels of risk due to IT-based threats in finance and banking, transport, electric power, telecommunications and the Internet, oil and gas, water, and critical State services that support national safety, security, and income.[291] The report made several recommendations such as:

- the establishment of a New-Zealand-based security-monitoring and incident-handling organization,
- the harmonization of computer-crime legislation with that of other nations (e.g., Australia, the United States, United Kingdom and Canada),
- the adoption of specific IT security standards,
- the establishment of an ongoing cooperation program between owners of critical infrastructure and the government.[292]

290 Minister of Defence. *The Government's Defence Policy Framework* (June 2000), p. 4: http://www.executive.govt.nz/minister/burton/defence/index.html. Or: http://www.defence.govt.nz/public_docs/defencepolicyframework-June2000.pdf.

291 Minister of State Services, 11 February 2001. Media Release on Cyber Crime. http://www.ccip.govt.nz/about-ccip/media-release-cyber-crime.htm.

292 E-Government Unit, State Services Commission, 8 December 2000. *Protecting New Zealand's Infrastructure from Cyber-Threats.* http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

Centre for Critical Infrastructure Protection (CCIP)

On 11 June 2001, the report *Towards a Centre for Critical Infrastructure Protection* (CCIP) was issued by the *E-Government Unit.*[293] It recommended the establishment of a Centre for Critical Infrastructure Protection by the government. The argument was that the dependence of citizens and businesses on various infrastructure services, the vulnerability of IT systems, and the increasing risks and possible damages caused in case of failure were increasing. Therefore, measures must be taken to ensure that infrastructure operators and government agencies are kept up to date on vulnerability and threat information: "The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss."[294]

In the early stages of CCIP planning, the location of the new centre was constrained by a) the need to give private-sector companies the confidence that their sensitive commercial and security information would be adequately safeguarded, and by b) the need to provide a secure environment to adequately protect intelligence information to which the CCIP must have access. It was stated that "Overseas experience shows that the Centre should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders to the detriment of rectifying damage and of confidentiality."[295] The *Government Communications Security Bureau* (see below) was finally appointed on the basis of cost, effectiveness and because of its significant IT security skills and its culture of security.[296]

Furthermore, the E-Government Unit acknowledged that timely access to classified intelligence, among other sources, would be necessary for the CCIP to provide the best chance of a successful threat warning.[297]

293 E-Government Unit, State Services Commission. *Towards a Centre for Critical Infrastructure Protection* (11 June 2001). http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

294 Ibid., p. 5.

295 Cabinet Paper. *Centre for Critical Infrastructure Protection* (13 August 2001), pp. 5, 9–11: http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.

296 Ibid., and: Towards a Centre for Critical Infrastructure Protection, 11 June 2001, p. 2. http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

297 Towards a Centre for Critical Infrastructure Protection, 11 June 2001, p. 9. http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

Security in the Government Sector

The *Interdepartmental Committee on Security* in 2002 issued a comprehensive and detailed manual called '*Security in the Government Sector*', which took into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 "Information Technology – Code of Practice for Information Security Management" dealing with possible sources of threats to information and how to counter them. The manual's security guidelines were made mandatory for government departments, ministerial offices, the *New Zealand Police*, the *New Zealand Defence Force*, the *New Zealand Security Intelligence Service*, and the *Government Communications Security Bureau*. In the manual, the government requires information important to its functions, its official resources, and its classified equipment to be adequately safeguarded to protect the public and national interests and to preserve personal privacy.[298]

Furthermore, the manual proposes that overall responsibility for security rest with a manager, designated as *Departmental Security Officer* (DSO). That person's duties should include the formulation and implementation of the general security policy and common minimum standards within the organization, to issue instructions on security, and to serve as liaison with the *Secretary of the Interdepartmental Committee on Security* (ICS), the *New Zealand Security Intelligence Service* (NZSIS), and the *Government Communications Security Bureau* (GCSB) for any special advice.[299]

Security Policy and Guidance Website

The security policy and guidance website (*www.security.govt.nz*) provides information on the governments action concerning information security. This website acts as a focal point for the publication of government information about security standards, procedures and resources.[300]

298 Department of the Prime Minister and Cabinet. *Security in the Government Sector* (2002). http://www.security.govt.nz/sigs/index.html.

299 Ibid., Chapter 2.

300 http://www.gcsb.govt.nz/infos/infos02.htm.

Standards New Zealand (SNZ)

Standards New Zealand (SNZ) [301] promotes several New Zealand specific standards as well as a host of joint Australian/New Zealand and international standards. AS/NZS ISO/IEC 17799 Information Security Management provides an overview of factors to be considered and included in the protection of information and information systems.

Organizational Overview

Public Agencies

The Domestic and External Security Secretariat (DESS)

The main actor in charge of formulating New Zealand's security policy, including CIIP, is the *Domestic and External Secretariat* (DESS), which co-ordinates central government activities aimed at protecting New Zealand's internal and external security, including intelligence, counter-terrorism preparedness, emergency and crisis management, and defense operations. The DESS director provides timely advice to the prime minister on issues affecting the security of New Zealand, including policy, legislative, operational, and budgetary aspects. DESS is the support secretariat for the *Officials Committee for Domestic and External Security Co-ordination*.[302]

Officials Committee for Domestic and External Security Co-ordination (ODESC)

The *Officials Committee for Domestic and External Security Co-ordination* (ODESC) is chaired by the prime minister and makes high-level policy decisions on security and intelligence matters, including policy oversight in the areas of intelligence and security, terrorism, maritime security, and emergency preparedness. ODESC comprises chief executives from the *Ministry of Foreign Affairs and Trade*, the *Ministry of Defence* and the *Defence Force*, the *New Zealand Security Intelligence Service*, the *Government Communications Security Bureau*, the *Police*, the *Ministry of Civil Defence and Emergency Management*, *Treasury*, and others when necessary.[303]

301 http://www.standards.co.nz.
302 http://www.dpmc.govt.nz/dess/index.htm.
303 http://www.dpmc.govt.nz/dess/index.htm.

Interdepartmental Committee on Security (ICS)

The *Interdepartmental Committee on Security* (ICS)[304] is a sub-committee of the *Officials Committee for Domestic and External Security Co-ordination* (ODESC). It formulates and coordinates the application of all aspects of security policy and sets common minimum standards of security and protection, which all government organizations must follow. In addition, the ICS provides detailed advice on information security matters to government and other organizations or bodies that receive or hold classified information.[305]

Centre for Critical Infrastructure Protection (CCIP)

The *Centre for Critical Infrastructure Protection* (CCIP) was established in 2001 to provide advice and support to public and private owners of CI, in order to protect New Zealand's critical infrastructure from cyber-threats. The CCIP is located within the *Government Communications Security Bureau* and has three main tasks:

- To provide a round-the-clock vigilance and advice service to owners of critical infrastructure and to government departments,
- To analyze and investigate cyber-attacks, and
- To collaborate with national and international critical infrastructure organizations to improve awareness and communications regarding information technology security.[306]

Whereas the CCIP provides coordination, support, and advice on the ways in which information security can be maintained and improved, owners of critical infrastructures in the public and private sectors will remain responsible for the security of their own systems.[307]

Government Communications Security Bureau (GCSB)

The CCIP is part of the *Government Communications Security Bureau* (GCSB). In 1977, the *Combined Signals Organization* was replaced by the current signals intelligence agency – the GCSB, which is a civilian organization. Its chief executive reports directly to the prime minister. The GCSB

304 http://www.security.govt.nz.

305 Department of the Prime Minister and Cabinet. *Security in the Government Sector* (2002). http://www.security.govt.nz/sigs/chapter-1-security-policy.doc. http://www.security.govt.nz/sigd/sigd2a.html.

306 http://www.ccip.govt.nz/about-ccip/about-ccip.htm.

307 Cabinet Paper. Centre for Critical Infrastructure Protection, 13 August 2001: http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.

gives advice and assistance to New Zealand government departments and agencies concerning the security of information-processing systems.[308]

One of the GCSB's tasks is to ensure the integrity, availability and confidentiality of official information through the provision of *Information Systems Security* (INFOSEC) services to departments and agencies of the New Zealand government, and to contribute to the protection of the critical infrastructure from IT threats.[309] The *New Zealand Security of Information Technology* (NZSIT) publications are therefore produced as guidelines for New Zealand government organizations in support of securing and protecting IT systems and associated information and services.[310]

E-Government Unit

The E-Government Unit was established in July 2000 in the *State Services Commission* (a department of the New Zealand Public Service[311]). The following projects are under the umbrella of this unit:

- A *Secure Electronic Environment* (S.E.E.) for the protection of sensitive information within and among government agencies. A sub-project of the S.E.E. project is the development of a framework for authentication in accessing sensitive systems within public key infrastructures. The intention is to develop minimum requirements and a framework for the accreditation of certification authorities;
- The study "*Protecting New Zealand's Infrastructure From Cyber-Threats*" on national critical infrastructures and their level of vulnerability to cyber-threats.

Public Private Partnerships

New Zealand Security Association (NZSA)

The *New Zealand Security Association* (NZSA) was formed in 1972 and represents licensed and certificated persons providing services to government departments, state-owned enterprises, businesses, and private users. The NZSA has two member groups: Corporate members, who are individu-

308 Domestic and External Security Secretariat. *Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies* (December 2000). http://www.dpmc.govt.nz/dess/securingoursafety/index.html.

309 http://www.gcsb.govt.nz/function.htm.

310 http://www.gcsb.govt.nz/nzsit/index.htm.

311 http://www.ssc.govt.nz/display/home.asp.

als or companies engaged in the security industry, and associate members, who are individuals or companies involved or interested in security without offering the services to the public. Members of the latter category include government departments, insurance companies, airlines, banks, food distributors, area health boards, oil companies, etc.[312] Among the NZSA's main objectives are:

- To set minimum operating standards for members and developing and approving codes of practice,
- To co-operate with the police, government departments, and agencies and other organizations concerned with the safekeeping of people, property, and information in New Zealand,
- To provide information and advisory services, education, and training.[313]

Computer Society Special Interest Group on Security (NZCS SigSec)

The *New Zealand Computer Society's Special Interest Group on Security* (NZCS SigSec) is a forum for networking with others with an interest in IT security from within and outside government. It meets quarterly for a presentation and networking.[314]

Early Warning Approaches

AusCERT

AusCERT[315] is the national *Computer Emergency Response Team for Australia* and also provides significant support to New Zealand organizations. It is one of the leading CERTs in the Asia/Pacific region; it provides prevention, response, and mitigation strategies for members.[316]

AusCERT was founded as a commercial CERT for Australia before the New Zealand *Centre for Critical Infrastructure Protection* (CCIP) was formed. The CCIP has a working relationship with AusCERT, but also

312 http://www.yellow.co.nz/site/newzealandsecurityassociation/.
313 http://www.security.org.nz/nzsa/aboutus.htm.
314 http://www.nzcs.org.nz.
315 See also the Country Survey on Australia in this book.
316 http://www.auscert.org.au.

provides an early-warning service and a moderated mailing list through its website.

Several commercial organizations – including the New Zealand company Co-logic – also provide vulnerability alerts filtered and tailored for their customers.[317]

317 http://www.cologic.co.nz .

CIIP Country Surveys

Norway

The Country Survey of Norway 2004 was written with the help of Stein Henriksen, Roger Steen, and Kjetil Sørli, Directorate for Civil Protection and Emergency Planning (DSB) as well as Cort Archer Dreyer, Ministry of Trade and Industry.

Norway

Critical Sectors

A central premise underlying the Norwegian CIIP policy concept is that the production of most goods and services depends in some way or other on information and communication technology (ICT) systems. This dependency may occur as part of the production process itself, or as part of the logistics of making 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:[318]

- Banking and Finance,
- Central Government Administration,
- (Tele-)Communications,
- Defense,
- Energy and Utilities,
- Oil and Gas Supply,
- Police,
- Public Health,
- Rescue Services,
- Social Security,
- Transport,
- Water Supply and Drainage.

The main challenges for society concerning information infrastructure are seen in the areas of rapid technological development, deregulation, globalization, interdependencies, the lack of expertise, and outsourcing of manpower and systems.[319]

Norway's CIIP policy is based on the following goals:[320] 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 society and the challenges to many

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

319 Ministry of Trade and Industry. *Information and Infrastructure Protection – a Norwegian View* (no date). http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.

320 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

CII sectors, the government has initiated several relevant measures such as the security part of eNorway, the *ITSEC* (IT Security) national strategy, the Intelligence Services Initiative, and the *Center for Information Security* (SIS).[321]

Initiatives and Policy

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. Since the end of the 1990s, CIIP has been regarded as a security 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.[322] Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[323]

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*.[324] In the aftermath of 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector.[325]

321 Report no. 17 to the Storting (2000–2001).
322 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
323 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
324 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
325 Report no. 17 to the Storting (2000–2001).

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.[326] The commission's task 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.[327]

The government commission identified several focus areas. One of these was CI.[328] 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.[329] Furthermore, a strategy based on the following pillars was proposed:[330]

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

ICT-Vulnerability Project

The *ICT Vulnerability Project*[331] was commissioned by the *Ministry of Trade and Industry* in 1999 and consisted of an interdepartmental group. The project collaborated with the government commission on the '*Vulnerable Society*', and the two groups coordinated their findings on ICT vulnerabili-

326 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.

327 http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm.

328 Jan Hovden. *Public policy and administration in a vulnerable society.* Norwegian University of Science and Technology and the Norwegian Academy of Science and Letters, Center for Advanced Study (June 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1074.doc.

329 Ibid.

330 Ibid.

331 Ministry of Trade and Industry, *Society's vulnerability*, p. 10.

ties.[332] In the ICT Vulnerability Project, each sector authority evaluated the risks linked to specific functions in that sector.[333] This project resulted in the *National Strategy for ICT Security.*

National Strategy for ICT Security

The *Ministry of Trade and Industry* published a national strategy for securing ICT systems in Norway in June 2003,[334] which proposed several initiatives for improving security based on the *OECD Guidelines for the Security of Information Systems and Networks* (→ for more details see Part III). The strategy involves all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure.

The Norwegian national authorities started implementing the suggested measures in the autumn of 2003. The establishment of the *Center for Information Security* (*SIS*, see below), is one of them already carried out. Other initiatives include the establishment of a coordination committee for ICT security and campaigns to raise awareness of challenges and problems related to the use of ICT systems.[335]

eNorway 2005 Action Plan

The government presented in May 2002 the *eNorway (eNorge) 2005 Action Plan*, which describes the needs, responsibilities, and action required for the development of an information society.[336] With *eNorge*, the government ensures that the country has equally ambitious objectives as those formulated by the EU in the *eEurope Plan*.[337] eNorway is an evolving plan and deals predominantly with the furtherance of e-Government and e-Business.

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

333 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.

334 http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf.

335 http://www.norsis.no/detailse.php?type=news&id=176.

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

337 http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf.

"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 of 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."[338] The recommendations laid the basis for new government measures, including most importantly the formation of the new *Directorate for Civil Protection and Emergency Planning* (DSB).[339]

Organizational Overview

Public Agencies

In Norway, the ministry or authority that has the responsibility for an area during peace or non-crisis times also has the responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the *Ministry of Justice and Police*. The overall authority for ICT security is the *Ministry of Trade and Industry*, while the *Ministry of Defense* is responsible on the military side. The *Ministry of Transport and Communications* has responsibility for the communication sector in Norway, including all related security issues. Directorates and authorities that are responsible for handling the different sides of CIIP on behalf of the ministries are subject to the respective ministries.[340]

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.[341]

338 Report no. 17 to the Storting (2000–2001). *Statement on Safety and Security of Society (Summary)* (April 2002).

339 http://www.dsb.no.

340 Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

341 Information provided by a Norwegian expert from the Norwegian Ministry of Trade and Industry, June 2002.

Directorate for Civil Protection and Emergency Planning (DSB)

The *Directorate for Civil Protection and Emergency Planning* (DSB)[342] was established on 1 September 2003, replacing the former *Directorate for Civil Defense and Emergency Planning* and the *Directorate for Fire and Electrical Safety.*

The new DSB is subordinate to the *Ministry of Justice and Police*, and its 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 during disasters in peacetime.

To ensure adequate preparedness measures in the community, the DSB 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.

In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in co-operation with other actors.

National Authority for Investigation and Prosecution of Economic and Environmental Crime (OKROKRIM)

The *National Authority for Investigation and Prosecution of Economic and Environmental Crime* (OKOKRIM) is responsible for issues concerning cyber-crime.[343] OKOKRIM has a unit called IKT-*teamet* that focuses on ICT-related crimes.

The Directorate of National Protection

The *Directorate for National Protection* (Nasjonal sikkerhetsmyndighet)[344] was established in January 2003. Its main CIIP task is to produce secure solutions and technology, together with enforcing laws and regulations on handling classified information and securing critical objects. It also handles certification systems (SERTIT) according to Common Criteria standards.[345]

342 http://www.dsb.no.
343 http://www.okokrim.no.
344 http://www.nsm.stat.no.
345 Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

Public Private Partnerships

The most important public private initiatives in Norway are the *Center for Information Security* (SIS) and the *Warning System for Digital Infrastructure* (VDI) project.

Center for Information Security (SIS)

The Norwegian government decided some years ago to establish a *Center for Information Security* (SIS). In 2001, a pilot study was commissioned to investigate options for the establishment of this center.[346]

SIS is now responsible for coordinating activities related to information and communication technology security in Norway. This includes the exchange of information, competence, and knowledge about threats and countermeasures, and a holistic threat image generation.[347] The clients of the SIS are government agencies, security services, politicians, and private enterprises, offering a broad basis for assessing the status of national security. SIS is closely linked to UNINETT CERT (see below).

Warning System for Digital Infrastructure (VDI)

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 *Warning System for Digital Infrastructure* (VDI)[348] is an initiative by the intelligence services intended to enable intelligence and security professionals to chart the extent of the threat to vulnerable information infrastructure through the use of Intrusion Detection Systems (Sniffers). The project was a cabinet reaction to the commission on '*A Vulnerable Society*' and the *Ministry of Trade and Industry* report in summer/autumn of 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

346 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), p. 10.

347 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.

348 Ibid.

privacy and other issues. VDI co-ordination has now moved to the *National Security Agency*.

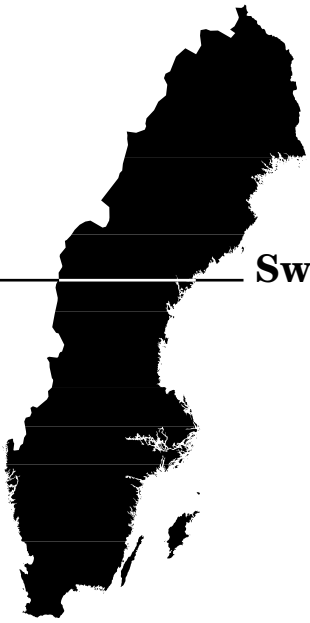
Early Warning Approaches

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.[349] The team was created to contribute to better Internet security for UNINETT member institutions, and to serve as a focal point for security issues regarding UNINETT member institutions.[350] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more members of the constituency. Examples of incidents are spamming, suspicious port-scanning, and denials of service.[351]

349 Dependability Development Support Initiative, country report Norway (version April 2002).
350 http://cert.uninett.no/policy.html.
351 http://cert.uninett.no/policy.html.

CIIP Country Surveys



Sweden

The Country Survey of Sweden 2004 was written with the help of Jan Lundberg and Sara Siri, Swedish Emergency Management Agency (SEMA) as well as Georg Fischer and Henrik Christiansson, Swedish Defence Research Agency (FOI).

Sweden

Critical Sectors

There is no official definition of CII or CIIP in Sweden. However, CIIP can be understood as the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services.[352] In a preparatory work to the *Commission on Vulnerability and Security*[353] (see below), the following critical information infrastructure sectors were suggested:

- Air control systems,
- Electric power systems,
- Financial systems,
- National command systems,
- Telecommunication systems.

Disruption of any of these systems would have immediate serious consequences for society.

Initiatives and Policy

CIIP-issues have been on the political agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures have been implemented since World War II. The vulnerability problems associated with society's increasing dependence on IT and information infrastructures were identified early on as a matter of national security. In addition, management of IT-related vulnerabilities has been discussed since the early 1970s. The present Swedish CIIP policy is derived from these historical developments and from some more recent initiatives described below.

352 Information provided by a Swedish expert of SEMA, 2003.

353 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 Cabinet Office Working Group on Defensive Information Operations (AG-IO/IW)

On 12 December 1996, the government appointed within the cabinet a *Working Group on Defensive Information Operations*. In addition to the members from the cabinet office and ministries, the group also included representatives of relevant private companies and organizations. The working group's task was to monitor developing threats and risks in the area of information warfare and to spread information about these matters. In addition, the working group prepared a proposal on how to assign responsibilities and to formulate strategy guidelines for protection against information operations. The working group presented two main reports before it was disbanded. Some of its tasks have been transferred to the *Swedish Emergency Management Agency* (see below).

Commission on Vulnerability and Security

Following a decision on 23 June 1999, the Swedish government authorized the *Minister for Civil Defense* to appoint a *Special Investigator* to head a commission of inquiry, with a mandate to analyze and submit proposals for a more integrated approach to civil defense and emergency preparedness planning.[354] The findings and proposals of the *Commission on Vulnerability and Security*, as presented in May 2001, have been a most important step in the implementation of a new structure for a defense and emergency preparedness planning in Sweden.

The commission suggested several strategic measures for improving the general stability of critical technical infrastructure.[355] In its final report, the commission also proposed measures designed to specifically enhance information assurance and improve protection against information operations. The commission's view was that the central government must assume responsibility in these areas. At the same time, the commission emphasized that all managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and to

354 Ibid.

355 Such as cross-sector activity, security standards, Computer Emergency Response Teams, a coordinating body for IT security, an information security technical support team, an intelligence and analysis unit, R&D, international cooperation, a system for the certification of IT products, and more. Ibid., pp. 41–60.

provide functions and facilities that exceed the financial capabilities of other sectors in society.

Committee on Information Assurance in the Swedish Society

The Swedish government on 11 July 2002 instituted the *Committee on Information Assurance in the Swedish Society*. The committee's brief was to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organizational matters of the Swedish signals protection service. In addition, the committee was asked to submit proposals regarding:

- The development of a national strategy for information assurance,
- The form and focus of future Swedish engagements in international cooperation on information assurance,
- The implementation of the *OECD Guidelines for the Security of Information Systems and Networks*.

The committee is also expected to monitor the implementation of information assurance measures within state agencies in accordance with the *Government Bill on Society's Security and Preparedness* (see below).[356] The committee will finish its work during 2005.

Committee on Joint Radio Communication for Public Safety and Security

At present, Sweden has no single radio communication infrastructure for public safety and security (PSS), i.e. emergency services. There are about two hundred different systems for radio communication within the domain of PSS in Sweden. In the light of this and other issues, the government instituted the *Committee on Joint Radio Communication for Public Safety and Security* on 10 June 2002. In September 2003, the government decided to allocate the necessary funding to finance a new radio system for PSS.

The aim of government policy on telecommunications is to give citizens and the Swedish authorities access to reliable and effective electronic communications. Everyone should have access to telecom services on equal terms. The communications systems should also be robust and accessible

356 Government bills 2001/02:158.

during situations of crisis and war.[357] Robust telecommunications are to be achieved through long-term and systematic preparatory efforts.

Government Bill on Society's Security and Preparedness

In March 2002, the government presented its bill on Swedish security and preparedness policy. The bill was, to a large extent, based on the findings and proposals of the *Commission on Vulnerability and Security* (see above).

The bill presented the government's framework for a new planning system to prepare for major societal crises and for activities related to a potential threat of war. Further, the bill gave an account on how the crisis management structure will be strengthened. All of this has implications for the assurance of critical infrastructures in general, and for critical information infrastructures in particular.

Based on the findings and proposals of the *Commission on Vulnerability and Security*, the government presented a new organizational structure for Swedish information assurance:

- Overall responsibility for information assurance and for policy intelligence and analysis in the public sector rests with the *Swedish Emergency Management Agency* (SEMA) (see below);
- A *Computer Emergency Response Team* operates at the *Swedish National Post and Telecom Agency*. The team monitors IT incidents, gathers statistics, and provides warnings to IT-system owners when necessary (see below);
- An *Information Security Technical Support Team* of experts and support staff with a high level of technological expertise operates at the *Swedish National Defense Radio Establishment* (see below);
- A system for security-oriented evaluation and certification of IT products and systems has been established at the *Swedish Defense Materiel Administration* (see below).

357 Government bills 2001/02:158 and 2002/03:110.

Organizational Overview

Public Agencies

The government agencies report to their respective ministries, but are formally subordinated only to collective cabinet decisions. The various agencies and organizations in charge of critical information infrastructure protection are presented below under the heading of the ministry they are affiliated with.

Ministry of Defense

The Swedish Emergency Management Agency (SEMA)

The *Swedish Emergency Management Agency* (SEMA) [358] was established on 1 July 2002 to coordinate work on the preparedness of society for major crises and war. When it was formed, SEMA took over some of the tasks of the *Swedish Agency for Civil Emergency Planning* and the *National Board of Psychological Defense*. SEMA presents proposals to the government on the allocation of resources, and then distributes funds to the authorities active in the emergency management area. This includes directing, coordinating, and evaluating measures taken.

SEMA analyzes the development of society, and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors. The agency also coordinates and initiates research and development in the emergency management area and has overall governmental responsibility for information assurance in Sweden. The *Information Assurance Department* mainly manages the latter task, while the *Research and Analysis Department* handles the former task.

SEMA/The Information Assurance Department

The main activities of the Information Assurance Department include:

- The preparation of an annual overall assessment of information assurance in Sweden;
- Fostering and contributing to cooperation between governmental organizations, corporations, and other important actors within this area;

358 http://www.krisberedskapsmyndigheten.se/english/index.jsp.

- Gathering, analyzing, and disseminating open-source information related to information assurance;
- The development of preventive IT security recommendations (consistent with ISO/IEC 17799) to support the IT security activities of other organizations;
- Initiating research and development in the area and summarizing risk and vulnerability assessments of different important societal systems;
- Managing the Board of Information Assurance (see below).

SEMA/The Board of Information Assurance

The *Board of Information Assurance* was established to support SEMA's activities in the area of information assurance. This board will create a network of skilled experts from a variety of important organizations in the area. The board replaced the earlier *Cabinet Office Working Group on Information Operations.*[359] The board's primary assignment is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the area of information assurance;
- Suggestions and viewpoints concerning direction, prioritizing, and realization of SEMA's activities in the area of information assurance.

The Swedish Defense Materiel Administration (FMV) and the Certification Body for IT security (FMV CB)

The *Swedish Defense Materiel Administration* (FMV) [360] is the Swedish procurement agency for the armed forces. The FMV has been involved in the area of IT security evaluations since 1989, performing in-house evaluations of equipment intended for use by the armed forces.

In the summer of 2002, the FMV was tasked by the government with establishing a Swedish scheme for the evaluation and certification of IT

359 SEMA document 0160/2003: Account of Measures Taken in Assuming Responsibilities from the Working Group on Information Operations (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

360 http://www.fmv.se.

security products to be used within Swedish governmental organizations. The establishment of the *Certification Body* at the FMV[361] is planned for the period 2003–2004.[362]

FRA/The Information Security Technical Support Team

The *Information Security Technical Support Team* is associated with the *Swedish National Defense Radio Establishment* (FRA),[363] which is the Swedish signals intelligence organization. It is a civil agency directly subordinated to the *Ministry of Defense*. The *Information Security Technical Support Team* consists of twenty experts in the field of IT security. The team is specifically intended to support:

- National crisis management where IT security qualifications are required;
- Identification of individuals and organizations involved in IT-related threats against critical systems.

On request, the team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses etc. The team co-operates on a regular basis with the national and international IT security community.

The Swedish Armed Forces

The *Swedish Armed Forces*[364] must be able to quickly respond to different types of threats and risks. The Swedish parliament has therefore decided to develop the armed forces according to the concept of *Network-Based Defense*. This places a great demand on the information infrastructure in terms of availability and security. The armed forces are therefore heavily involved in research and development in areas such as IT security and information infrastructures.

361 http://www.fmv.se/cb/index.asp?K=016&L=UK.

362 Evaluations will be performed according to the international standard ISO/IEC 15408 Evaluation Criteria for IT Security, also known as Common Criteria (CC).

363 http://www.fra.se/english.shtml.

364 http://www.mil.se.

The *Swedish Military Intelligence and Security Service* handles operational IT security in the armed forces during peacetime. In addition, the *National Communications Security Group* (TSA) offers Swedish defense organizations and industries advice and inspections of cryptographic systems.

The National Center for IO/CIP Studies (CIOS)

The *National Center for IO/CIP Studies* (CIOS) is located at the *Swedish National Defense College.*[365] CIOS conducts research and policy development in the fields of IO and CIP. Research at CIOS is funded by the *Ministry of Defense* and the *Swedish Emergency Management Agency* (SEMA).

The Swedish Defense Research Agency (FOI)

The *Swedish Defense Research Agency* (FOI) [366] focuses on R&D in the field of applied natural sciences and political sciences, such as security policy analysis. At the Division of Defense Analysis, the *Critical Infrastructure Studies Unit* (CISU) research group is carrying out a long-term research program on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security – another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

Ministry of Industry, Employment, and Communications

The Swedish National Post and Telecom Agency (PTS)

The *Swedish National Post and Telecom Agency* (PTS) is a government authority that monitors all issues relating to Information Communication Technology (ICT) and postal services. One of its key tasks is to ensure the development of functioning postal and telecom markets. Within the PTS, the *Department of Network Security* is responsible for security issues concerning ICT.

The *Department of Network Security* is tasked with monitoring developments concerning security issues and implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for running the *.se*-domain

365 http://www.fhs.se.
366 http://www.foi.se.

autonomously have been installed within Sweden's borders. The *Swedish IT Incident Center* (see Early Warning) is associated with this department.

Department of Justice

The Swedish National Police Board (NPB)

The *Swedish National Police Board* (NPB) [367] is the central administrative and supervising authority of the police service. The NPB administers the National Criminal Investigation Department and the Swedish Security Service. Within the NPB, the *IT Crime Squad* has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The *Internet Reconnaissance Unit* is linked to this squad.

Additionally, there is the *Swedish Security Service* (SÄPO). Its fundamental duty is to prevent and detect crimes against the security of the realm. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the constitution. Whenever IT criminal activity touches upon these fields, the *Swedish Security Service* is involved.

The Government Office

The Swedish Agency for Public Management

The *Swedish Agency for Public Management*[368] conducts studies and evaluations at the request of the government and modernizes the public administration with the use of ICT. The agency helps to develop Swedish administrative policy and also ensures that electronic infrastructure in the public sector is open and secure.

The report "*The 24/7 Agency – Criteria for 24/7 Agencies in the Networked Public Administration*"[369] proposes a four-stage agency development plan towards enhancing accessibility and providing service round

367 http://www.polisen.se.
368 http://www.statskontoret.se.
369 http://www.statskontoret.se/pdf/200041.pdf.

the clock, seven days a week. The criteria recommended by the agency focus primarily on government agencies' capacity to provide interactive services for the public and businesses. In the area of IT security specifically, the agency has compiled a strategy for information assurance in society[370] and produced a publication on secure authentication.[371] At the time of writing, the agency was carrying out the project "*Information Security at Authorities*". It aims at supporting other authorities with methods and tools for implementing threat and risk analyses according to ISO 17799.

Public Private Partnerships

The Swedish Emergency Management Agency (SEMA)

The *Swedish Emergency Management Agency* (SEMA) promotes interaction between the public sector and the business sector, and works to ensure that the expertise of non-governmental organizations (NGOs) is taken into account in emergency management.

There are two advisory councils connected to SEMA: the *Private Sector Partnership Advisory Council* and the *Board of Information Assurance*. However, it has not yet been established how the CIIP public private partnership will be institutionalized.

The Industry Security Delegation (NSD)

The *Industry Security Delegation* (NSD)[372] is a delegation within the *Confederation of Swedish Enterprise* (Svenskt Näringsliv) whose objective is to increase cooperation between enterprises, organizations, and authorities, and to promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness among the general public and the business sector. The NSD arranges courses in information assurance as well as crisis and risk management to help its members improve security.

370 *Coherent strategy for information assurance in society* (Sammanhållen strategi för samhällets IT-säkerhet, rapport Statskontoret rapportserie, 1998, p. 18).

371 *Security related to electronic identification* (Säkerhet med elektronisk identifiering, rapport i Statskontorets rapportserie 1999, p. 30).

372 http://www.svensktnaringsliv.se/index.asp?pn=155246.

The Swedish Information Processing Society (DFS)

The *Swedish Information Processing Society* (DFS) [373] is an independent organization for IT professionals with 32'000 members. The DFS owns SBA brand of security products (the abbreviation stands for SårBarhetsAnalys, or "vulnerability assessment" in Swedish), which focus on risk analysis and information security. SBA is said to be a Swedish de facto standard.

Early Warning Approaches

PTS/The Swedish IT Incident Center (SITIC)

In May 2002 the Swedish government tasked the PTS with establishing the *Swedish IT Incident Center* (SITIC) [374]. The center was officially opened on 1 January 2003. SITIC supports national activities for the protection against IT-incidents by:

- Operating a system for information exchange on IT incidents between both public and private organizations and SITIC;
- Rapidly communicating information on new problems that can disrupt IT systems to the public;
- Providing information and advice on preventive measures;
- Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

373 http://www.dfs.se.
374 http://www.sitic.se.

CIIP Country Surveys

Switzerland

The Country Survey of Switzerland 2004 was written with the help of Ruedi Rytz, Federal Strategy Unit for Information Technology (ISB); André Schmid, Managing Director InfoSurance Foundation; Anton Lagger, Federal Office for National Economic Supply; Marc Henauer, Federal Police/DAP, and Michel Dufour, Dufour Consulting.

Switzerland

Critical Sectors

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in the Swiss debate on security policy. The high density of information and communication technology (ICT) in Switzerland's public and private sectors offers a high potential for vulnerabilities. There is no official list of critical information infrastructure sectors. The definition of critical sectors is at the stage of planning and roughly includes the following:[375]

- (Public)Administration,
- Civil Defense and Emergency Services,
- (Tele-)Communication,
- Energy,
- Finance,
- Industry/Manufacturing,
- Media,
- Public Health,
- Transport (and Logistics),
- Water.

375 InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen – Methodischer Leitfade*n (2002). More research (still unpublished) is being carried out in Switzerland in the field of defining critical sectors. Some of this work addresses CIP generally rather than CIIP in particular, or deals with emergency scenarios.

Initiatives and Policy

Since the end of the 1990s, several important steps have been taken in Switzerland to improve the management of CIIP.[376]

Strategic Leadership Exercise 1997

A key experience, and in fact the impetus for many later steps in Switzerland, was the *Strategic Leadership Exercise* in 1997 (SFU 97).[377] The exercise dealt with the revolution in information technologies and the related challenges to modern society, politics, economics, and finance as well as to other critical sectors.[378] 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.[379]

"Strategy for the Information Society Switzerland"

In 1998, the *Federal Council* defined its "*Strategy for the Information Society Switzerland*". The strategy paper outlined the basis for promoting an information society and identified the areas where action was most urgently needed.[380] The Federal Council also defined the four governing principles: (1) access to information for everyone, (2) empowerment for everyone to use information technologies, (3) freedom of development for the information society, and (4) acceptance of new technologies. Developments triggered by

376 See also Sibilia, Riccardo: "Informationskriegführung. Eine schweizerische Sicht", in: *Institut für militärische Sicherheitstechnik (IMS)* no. 97–6 (Zurich, 1997); Generalsekretariat VBS (ed.), *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz* (draft version, Berne, 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*, no. 11. *Schweizerischer Nationalfonds* (Berne, 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.

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

378 Schweizerische Bundeskanzlei. *Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97.* (Berne, 1997), p. 2.

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

the information and communication technology were perceived as a high priority issue for Switzerland.[381]

Security Policy Report 2000

In the *Security Policy Report 2000*[382], the *Swiss Federal Council* recognizes CIP/CIIP as a goal of its security policy: "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'".[383]

Exercise "INFORMO 2001"

After a two-year planning process, the Strategic Leadership Training conducted in 2001 the three-day exercise *INFORMO 2001*. The goals were to review the information assurance process established after 1997 and to train a newly-established *Special Task Force on Information Assurance* (Sonderstab Information Assurance, SONIA).[384]

InfoSurance Foundation, Risk Analysis

The *InfoSurance Foundation* started its work in 2002 with a nation-wide risk analysis covering various sectors and branches such as telecommunications, finance, government, energy (electricity) and water, industry, emergency and rescue services, transportation and logistics, media, and health care. The risk analysis focuses on interdependencies of information infrastructures both within and between the various sectors. The same methodological guidelines are employed for all sectors (for more details, see Part II).

380 ISB: Vulnerable Information Society – Challenge Information Assurance, p. 18 (available at http://www.isb.admin.ch).

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

382 http://www.vbs-ddps.ch/internet/vbs/en/home/theddps/publikationen/berichte.Par.0001.DownloadFile.tmp/SIPOLEv2.pdf.

383 Ibid. p. 56.

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

Annual Events

The three most important annual events in Switzerland concerning information security are the *Bernese Conference on Information Security*,[385] the *Symposium on Privacy and Security*, and the *Lucerne Information Assurance Days* (LUTIS).[386]

The *Bernese Conference on Information Security* is organized by the *Special Interest Group on Information Security of the Swiss Informaticians Society* and the *Swiss Federal Strategy Unit for Information Technology* (ISB). Every year, the event covers a specific topic.[387] The *Symposium on Privacy and Security*[388] offers 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.[389] *LUTIS*, the annual two-day meeting organized by the *InfoSurance Foundation*, assembles the actors in the field of information security both from the private sector and from government in order to further the Swiss cooperation model for information assurance.

Coordination Group for Information Society (KIG)

The *Coordination Group for Information Society* (KIG) defined the security and availability of information infrastructures as one of the high-priority operative essentials. The key policy document, '*Concept Information Assurance*', was published in 2000. It recommended the establishment of a crisis management system of a special task force on '*Information Assurance*'.[390] This strategy of the *Swiss Federal Council* was accompanied by a large number of parliamentary initiatives. In the reporting year 2002/2003, 24 initiatives dealing with the information society were proposed by members of parliament. About half the parliamentary initiatives were

385 Berner Tage für Informationssicherheit.
386 Luzerner Tage für Informationssicherung.
387 Past topics have included 'Information assurance' (2002), 'Public key infrastructures' (2001), and 'Humans as an important security factor' (2000).
388 Symposium on Privacy and Security 2002, available at http://www.privacy-security.ch.
389 The 2003 event topics were 'Identity and anonymity in an increasingly interconnected world'.
390 See Koordinationsgruppe Informationsgesellschaft (KIG): Konzept "Information Assurance", May 2000.

concerned with crime and the Internet, while a quarter of the initiatives dealt with mobile telephony and the Law on Telecommunications.[391]

Information Assurance Policy

The overall information assurance policy as defined in Switzerland over the past few years is based on *four pillars*:[392]

- *Prevention:* Suitable preventive measures have to be implemented to limit the number of incidents;
- *Early recognition:* Dangers and threatening situations have to be recognized as early as possible to provide the necessary defensive measures or to avoid particularly vulnerable technology;
- *Damage limitation:* The effects of disruptions on society and the state have to be kept to a minimum;
- *Combating causes of crisis:* The technical causes of the disruption have to be identified and corrected.

It is a tenet of Swiss information assurance policy that all four of the above pillars, or principles, must be taken into account to achieve a complete and strong system of CIP/CIIP.

Organizational Overview

Public Agencies

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

Federal Strategy Unit for Information Technology (ISB)

One of the main bodies is the *Federal Strategy Unit for Information Technology* (Informatikstrategieorgan Bund, ISB).[393] It is subordinated to the *Swiss Federal Department of Finance* (EFD). The ISB reports to the EFD and is charged with producing instructions, methods, and procedures

391 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council, p. 24.

392 ISB: Vulnerable Information Society – Challenge Information Assurance, pp. 23–28 (available at http://www.isb.admin.ch).

393 http://www.isb.admin.ch/internet.

for the federal administration's information security. It collects data on incidents within the Swiss federal government, and it is responsible for the *Special Task Force on Information Assurance* and for the *Reporting and Analysis Center* (MELANI; see also Early Warning).[394]

Federal Office for Communication (BAKOM)

The *Federal Office for Communication* (Bundesamt für Kommunikation, BAKOM) is the main regulatory body in the field of telecommunications and ICT in Switzerland. The BAKOM studies various 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 BAKOM deals with risks in the information society, 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.[395]

Federal Office for National Economic Supply (BWL)

The *Federal Office for National Economic Supply* (Bundesamt für Wirtschaftliche Landesversorgung, BWL), which includes the *ICT Infrastructure Unit*, reports to the *Swiss Federal Department of Economic Affairs* (EVD). Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The BWL provides governmental support when the private sector is unable to resolve supply problems on its own. However, measures to ensure national economic supply would only be undertaken if the free market system were seriously disrupted.[396]

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

The *Swiss Federal Office of Information Technology, Systems, and Telecommunication* (Bundesamt für Informatik und Telekommunikation, BIT) reports to the *Swiss Federal Department of Finance* (EFD). Its responsibilities include security and emergency preparedness for information systems on an operational level for the federal administration.[397]

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

395 http://www.vbs-ddps.ch/internet/groupgst/en/home/integral/sicherheit/informatiksicherheit0.html.

396 Federal Office for National Economic Supply (BWL), available at http://www.bwl.admin.ch.

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

Coordination Unit for Cybercrime Control (CYCO)

Citizens can report suspected Internet crimes, including unlawful entry into IT systems, spreading of computer viruses, destruction of data, and similar offences to the *Swiss Coordination Unit for Cybercrime Control* (CYCO),[398] which is part of the *Federal Office of Police* (Fedpol). The offences reported are then forwarded to the respective national or foreign prosecution authorities. CYCO also looks out for criminal subject matter on the Internet and is responsible for in-depth analysis of cybercrime.[399]

Department of Defense, Civil Protection, and Sports (VBS)

The *Department of Defense, Civil Protection, and Sports* (VBS)[400] is developing a doctrine for information operations. As ICT plays an increasingly important role in modern warfare, the Swiss army is preparing for these new challenges of the information revolution. Protection against information operations and information warfare is seen as crucial to the functioning of the Swiss army. As information operations not only influence the military defense, but also the economy and the society as a whole, co-operation between the Swiss army and the private sector, academic institutions, and other countries is seen as crucial for an exhaustive investigation of the topic.[401]

Public Private Partnerships

Switzerland has a long-standing tradition of public private partnerships. Historically, this is due to the tradition of part-time service in a strong "militia" system, both in the military and in politics, in particular in the *Federal Office for National Economic Supply* (BWL).

InfoSurance Foundation

The most prominent example of a body promoting cooperation between industry and public administration is the *InfoSurance Foundation*.[402] It is supported by both leading companies and the Swiss government. The core tasks of *InfoSurance* are to increase awareness of the information assur-

398 Ibid.
399 http://www.cybercrime.admin.ch/e/koord.htm.
400 http://www.vbs-ddps.ch/internet/vbs/en/home.html.
401 http://www.vbs-ddps.ch/internet/groupgst/de/home/generalstab/truppeninformationsdienst/information/tid_pressespiegel/resume/schweiz.html.
402 The Foundation for the Security of Information Infrastructure in Switzerland. See http://www.infosurance.ch.

ance issue, to develop measures of prevention, and to establish networks of cooperation among the various players. The foundation aims at creating a closely-linked network that promotes the organizational and structural conditions for recognizing and analyzing Switzerland's growing dependency on information technologies and the associated risks.

ICT Infrastructure Unit (ICT-I)

Another important public private partnership is the *Federal Office for National Economic Supply* (BWL). Its main task is to ensure the provision of vital goods and services to the Swiss population at all times. The BWL works in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested the BWL 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 Approaches

A central office for early warning in CIIP at the federal level is currently being developed. For this office, Switzerland has chosen a cooperation model, which means that various partners already fulfilling similar tasks will work together. In terms of view of functionality and efficiency, this was seen as the most suitable model for CIIP early warning in Switzerland.[403]

The Reporting and Analysis Center for Information Assurance (MELANI)

On 29 October 2003, the government decided to create an authority that would collect information on the security of IT-infrastructure, especially of the Internet.[404] This new authority, called *Reporting and Analysis Center for Information Assurance* (Melde- und Analysestelle Informationssicherung,

403 Rytz, Ruedi and Jürg Römer. MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age, paper for the *Workshop on Critical Infrastructure Protection (CIP)* in Frankfurt a. M., 29–30 September 2003 (available at http://www.isb.admin.ch), p. 4, and OFCOM: 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council (June 2003), p. 49.

404 http://www.isb.admin.ch/internet.

MELANI), will be the core of the Swiss CIIP early warning system. MELANI will be set up by the *Federal Strategy Unit for Information Technology* (ISB) and is structured as a permanent body. It will play a role in all four pillars of the Swiss information assurance policy (as defined above). In addition to its own investigations, it depends on close cooperation with the public and private sectors, particularly on voluntary reporting of incidents in information and communication infrastructures. The three partners of MELANI have the following main tasks:[405]

- *Federal Strategy Unit for Information Technology* (ISB): is responsible for strategic issues and the management of MELANI;
- *Federal Office of Police* (fedpol): operates the MELANI analysis center and is responsible for collecting, condensing, and presenting operational information from different sources in the public and private sectors;
- *Swiss Education and Research Network* (SWITCH): operates the Computer Emergency Response Team (SWITCH-CH) and is responsible for dealing with technical incidents, in particular concerning the Internet and computer operating systems.

From 1 January onwards 2004 MELANI will be operational.

Special Task Force on Information Assurance (SONIA)

The *Special Task Force on Information Assurance* (Sonderstab Information Assurance, SONIA) is a crisis management organization and constitutes the core element of the third pillar of the Swiss information assurance policy (damage limitation). SONIA's main task is to advise the *Swiss Federal Council* and senior management representatives from the private sector in crisis situations and to act as a link between the public and private sectors.[406] SONIA would take charge after a breakdown in the information and communication infrastructure that resulted in (massive) disruptions in CI. Unlike MELANI, it is not a permanent body, but would only be convened for damage limitation in genuine crisis situations.

SONIA is mainly supported by the following organizations:

- *InfoSurance* and the *Federal Office for National Economic Supply* (BWL), to raise awareness and to give guidance in threat and risk analysis, as well as for protective measures during peacetime.

405 Rytz, Ruedi and Jürg Römer, op. cit., pp. 4–5, and OFCOM: 5th ISCG Report, p. 49.
406 Ibid., p. 48.

- MELANI, as a provider of reliable information about a possible imminent threat and its consequences, and as an information base in case of a crisis.[407]

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 information security problems. SWITCH represents the interests of Switzerland as a research center in numerous bodies, and therefore makes an important contribution to the development and operation of the Internet in Switzerland.[408]

407 Haefelfinger, Rolph L. The Swiss Perspective on Critical Infrastructure. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century, Stockholm*, 17–18 November 2003.

408 http://www.switch.ch/about.

CIIP Country Surveys

United Kingdom

The Country Survey of the United Kingdom 2004 was written with the help of Stephen Cummings, Ted Barry, and John Park, National Infrastructure Security Coordination Centre (NISCC).

United Kingdom

Critical Sectors

In the United Kingdom, the *Critical National Infrastructure* (CNI) comprises those parts of the infrastructure for which "the continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic or other grave social consequences for the community or would be of immediate concern to the Government."[409] Many of the critical services that are essential to the well being of the UK depend on IT and are provided by both the public and private sectors. The term 'national' has been adopted to indicate infrastructures that are critical to the UK's national interest.[410]

The ten sectors and 39 sub-sectors that comprise the CNI reflect the government's current classification of what is critical to UK interests considering vulnerabilities to physical and electronic attack and from the perspective of civil contingency planning. This comprehensive list is therefore jointly used by all UK agencies involved in CIP, CIIP, or emergency management:[411]

- Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
- Emergency Services (Ambulance, Fire and Rescue, Marine, Police),
- Energy (Electricity, Natural Gas, Petroleum),
- Finance (Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
- Food (Produce, Import, Process, Distribute, Retail),
- Government and Public Services (Central Government, Regional Government, Local Government, Parliaments and Legislatures, Justice, National Security),
- Hazards and Public Safety (Chemical, Biological, Radiological and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
- Health (Health Care, Public Health),
- Transport (Air, Marine, Rail, Road),
- Water (Mains Water, Sewage).

409 http://www.niscc.gov.uk/cni/index.htm.
410 Information provided by an NISCC expert in 2003.
411 Ibid.

A *UK Government Strategy for Information Assurance* has been developed. The *Central Sponsor for Information Assurance* (CSIA), a unit within the *UK Cabinet Office*, is implementing this strategy in partnership with other organizations across the public sector. A public document relating to the main points of the strategy is to be launched early in 2004.

Initiatives and Policy

CIIP Policy Guidelines

The British government aims at protecting the CNI from two kinds of threat: terrorist attacks against installations and equipment on the one hand and electronic attacks against computer or communications systems on the other hand.[412]

The government has produced a *Government Information Assurance Strategy*, which complements counter-terrorism strategies, national security considerations, and measures against high-tech crime. The aim of the strategy is to provide ongoing assurance to the government that the risks to information systems underpinning key public interests are appropriately managed. Most importantly, the strategy recognizes that within an increasingly interdependent and interconnected information infrastructure, the government must concern itself with the confidentiality, availability, and integrity of *all* information systems. The *Central Sponsor for Information Assurance* (CSIA) is the coordinating body for the strategy, working alongside other key government bodies.

e-commerce@its.best.uk

The UK approach to the information society was laid out in 1998 by the *Department of Trade and Industry's Competitiveness White Paper* that noted the major role played by ICT in facilitating growth.[413] In September 1999, the *Performance and Innovation Unit* (now the *Cabinet Office's Strategy Unit*[414]) issued "*e-commerce@its.best.uk*", a report outlining the

412 http://www.mi5.gov.uk/major_areas_work/major_areas_work_5_4.htm.

413 Department of Trade and Industry. *UK Digital Content: An Action Plan for Growth* (1998). http://www.dti.gov.uk/comp/competitive/wh_int1.htm.

414 http://www.strategy.gov.uk/about/about.shtml.

organizational and policy framework for achieving these goals.[415] The report's recommendations have been implemented under a national strategy known as *UK Online*, which gives access to government information and services online. UK Online aims to give every citizen Internet access by 2005.[416]

UK Online Strategy

The *UK Online Strategy* is overseen by the e-Minister and the e-Envoy, who report directly to the prime minister. The e-Envoy is responsible for ensuring that all government services are available electronically by 2005 and supports government plans to develop the UK as a world leader for electronic business.[417] The *UK Online Action Plan* includes 113 detailed recommendations covering 26 commitments to ensure that the UK is at the forefront of the knowledge economy revolution.[418]

Progress Report on Electronic Security

The e-Minister and the e-Envoy delivered their progress report on electronic security to the prime minister on 3 March 2003.[419] The key developments highlighted in the report were:

- A new information security element of the *UK Online for Business Website* was launched, with a view to offering basic security advice;[420]
- The *National Hi-Tech Crime Unit* (NHTCU) has developed a confidentiality charter to address the concerns of business, which has traditionally been reluctant to report IT incidents;
- The Office of the e-Envoy/CSIA has published a complete set of security frameworks describing measures that organizations should take to secure their electronic service delivery systems against assessed risks;
- The *Office of the e-Envoy/CSIA* has also published advice on the selection of biometrics products, which are of increasing interest;

415 Performance and Innovation Unit Report: "*e-commerce@its.best.uk*" (September 1999). http://www.cabinet-office.gov.uk/innovation/1999/ecomm.shtml.

416 http://www.ukonline.gov.uk/Home/Homepage/fs/en.

417 http://www.e-envoy.gov.uk/oee/oee.nsf/sections/about-oee/$file/aboutus.htm.

418 http://www.e-envoy.gov.uk/oee/oee.nsf/sections/ukonline-top/$file/ukstrategy.htm.

419 *Monthly Report from the e-Minister and e-Envoy* (3 March 2003). http://www.e-envoy.gov.uk/oee/OeE.nsf/sections/reports-pmreports-2003/$file/3march03.htm.

420 http://www.ukonlineforbusiness.gov.uk/informationsecurity.

- The *Office of the e-Envoy* has published guidelines for the registration of individuals and organizations with governmental electronic services, and a skeleton *Information Security Policy Document* that public-sector organizations can use to develop their own security policies;
- The *Central Sponsor for Information Assurance* (CSIA) is supporting the *National Infrastructure Security Co-ordination Centre* (NISCC) in establishing the first *Warning, Advice and Reporting Point* (WARP) in partnership with *London Connects*, the agency responsible for delivering electronic government (e-Government) in London.

Standard for Information Security Management

The *Cabinet Office's Security Division* promotes good practice in information security within government departments and across governmental systems. This includes the development of ISO/IEC 17799, which began as the British Standard BS 7799, one of the most popular codes of practice relating to information technology and information security management.[421] It deals with external, internal, accidental, and malicious threat sources, and aims at ensuring the confidentiality, integrity, and availability of information. The code deals with:

- Security policy and organization;
- Information security infrastructure;
- Information classification;
- Secure areas;
- Responding to security incidents and malfunctions;
- Network management and access control.[422]

421 http://www.cabinet-office.gov.uk/cabsec/Previous%20years/1998/sd/index.htm.
422 http://www.bsi-global.com/Portfolio+of+Products+and+Services/IT+Information/Info+Security/Overview/Topics.xalter.

Organizational Overview

In the UK, the main responsibility for CIIP lies with the home secretary.[423] However, a number of other departments play a role in the protection of the various CNI sectors and contribute resource and expertise to the British CIIP effort. These contributions are coordinated by an interdepartmental center that reports to the Home Office – the *National Infrastructure Security Co-ordination Centre* (NISCC). Policy is formulated and developed at a working level through a dialog between several government departments and bodies: the NISCC; the *Central Sponsor for Information Assurance* (CSIA); the *Civil Contingencies Secretariat* (CCS); the *Cabinet Office Security Policy Division*; and the *Home Office* itself. The various roles and responsibilities of these governmental bodies are described below.

While the NISCC has the lead in coordinating CIIP efforts within government and with the private sector, other responsibility is placed with a number of bodies:

- CIIP is a subset of CIP: the provision of physical protective security advice to the CNI is the responsibility of the *Security Service* and the *Police*;
- CIIP (focusing on just the CNI) is also a subset of the wider information assurance strategy dealing with all aspects of the information society. Responsibility for this lies with the *Central Sponsor for Information Assurance*;
- The coordination of the government's contingency and emergency response effort (regardless of the cause of the disruption) is the responsibility of the *Civil Contingencies Secretariat* (CCS) within the Cabinet Office.

Public Agencies

National Infrastructure Security Co-ordination Centre (NISCC)

The protection of the CNI from electronic attack has been the responsibility of the *National Infrastructure Security Co-ordination Centre* (NISCC) since 20 December 1999. The latter is an interdepartmental center that coordinates and develops existing work within government departments and agencies as well as CNI organizations in the private sector. The NISCC operates under a director, who is a member of a management board chaired

423 http://www.homeoffice.gov.uk/terrorism/govprotect/infrastructure/index.html.

by the Home Office. The other members of the board are from the *Cabinet Office*, the *Communications-Electronics Security Group* (CESG – the government's technical authority on information security), the *Security Service*, the *Ministry of Defence*, the *Police*, and the *Department of Trade and Industry* (DTI).

The NISCC aims to establish partnerships with CI providers. It has various duties towards its CNI partners across the UK:

- Promoting dialog with owners of CI systems to identify the most critical systems;
- Issuing alerts or warnings of attack;
- Providing assistance in response to serious attacks;
- Collecting, analyzing, and disseminating information about the threat;
- Undertaking research into vulnerabilities;
- Offering specialist protective security advice and expertise.[424]

The NISCC provides a range of government and other organizations with access to resources, expertise, and knowledge. The NISCC either carries out research itself or sponsors work in a variety of fields connected with electronic attack and information security. It bases its threat assessments on a variety of sources, including sensitive intelligence, overseas security and intelligence partners, open-source material, and the reports of those who have experienced electronic attack.

The NISCC passes information, such as warnings of specific threats and vulnerabilities, to CI partners so that operators can install suitable defenses, and offers periodic assessments of the nature of the threat from electronic attack. NISCC information on vulnerabilities and alerts are disseminated through UNIRAS, the UK government CERT, a component of the NISCC.[425]

Other government departments and the NISCC

The following government departments contribute to the CIIP effort through the NISCC, in addition to their own wider departmental roles and responsibilities:

- The *Cabinet Office* contributes policy and coordination; its own units– the *Civil Contingencies Secretariat* (CCS) and the *Central Sponsor for Information Assurance* (CSIA) – work closely with the NISCC.

424 http://www.gov.uk/cni/cniinfo.htm.
425 http://www.niscc.gov.uk/cni/cniinfo.htm.

- The *Communications-Electronics Security Group* (CESG) is the information assurance arm of the *Government Communications Headquarters* (GCHQ), and is the national technical authority on information security. The CESG aims to protect the communications and information of central government departments, agencies, and other parts of the national information infrastructure by developing technical means of countering assessed threats. The CESG delivers information assurance policy and gives technical recommendations and authoritative advice on assessing current and foreseeable risks.[426]
- The *Department of Trade and Industry* (DTI) has several CIIP-related responsibilities, and assists the NISCC by promoting ISO-17799; having departmental responsibility for the energy and telecommunications sectors; and by encouraging information assurance for SMEs.
- The *Home Office* is the reporting line for the NISCC; chairs the NISCC Management Board; and its press office responds to press enquiries on the NISCC- or CIIP.
- The *Ministry of Defence* (MoD) contributes technical and research efforts; as part of the CNI, the MoD's own hierarchical set of CERTS work closely with UNIRAS. The *Defence Research Centre* (DSTL) carries out research into CIIP for both the MoD and the NISCC.
- *Police*: the crime prevention and attack investigation roles of police high tech crime units complement the CIIP effort of the NISCC. In particular, the *National High Tech Crime Unit* (NHTCU) is a close partner of the NISCC. The NISCC itself is not a criminal investigation or police authority; and where a CII incident requires a police response, the NHTCU would lead.
- The *Security Service* contributes expertise on threat investigation, intelligence, and protective security to the NISCC. Its CIIP contribution to the NISCC complements its physical counter-terrorist protective security role, as described above.

Central Sponsor for Information Assurance (CSIA)

The *Central Sponsor for Information Assurance* (CSIA) was officially formed as a unit within the UK Cabinet Office on 1 April 2003. CSIA promotes information assurance and information risk management across government as well as for industry and the public. The unit's responsibilities are:

426 http://www.gchq.gov.uk/about/cesg.html.

- To provide a nationwide strategic direction for Information Assurance (IA);
- To co-ordinate and complement the activities of parties contributing to IA;
- To sponsor activities that benefit IA;
- To accredit pan-government systems and, in some cases such as the *Government Secure Intranet* (GSI), own the risk to shared information;
- To identify and address vulnerabilities in national telecommunications systems, and to resolve them in conjunction with other organizations such as the NISCC.

The Civil Contingencies Secretariat (CCS)

The *Civil Contingencies Secretariat* (CCS) is part of the Cabinet Office. It was established in July 2001, and reports to the prime minister through the S*ecurity and Intelligence Co-ordinator* and permanent secretary to the Cabinet Office. It was set up to improve the resilience of central government and the UK. Resilience is defined as the ability to handle disruptive challenges that can lead to or result in crisis. Disruptive challenges may arise from many causes – including, but not limited to, individual crises.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. Specifically, it services the *Civil Contingencies Committee*, which is chaired by the home secretary and deals with managing and exercising arrangements to handle individual crises as they arise. The CCS is organized around three divisions: An assessments division, which evaluates potential and evolving threats; an operations division, which develops and reviews departmental continuity and contingency plans; and a policy division, which gives the Cabinet Secretariat support in consequence management.

The aim of the CCS is to improve the UK's resilience to disruptive challenge through working with others inside and outside government on the anticipation, preparation, prevention, and resolution of threats. Its current objectives are:

- To identify and assess potential and imminent disruptive domestic challenges and assist in the development of an integrated response;
- To build partnerships with other organizations to develop and share best practices in horizon-scanning, and to develop the knowledge of the UK's critical networks and infrastructures;
- To ensure that the government can continue to function and deliver public services during crises, working with departments and other

secretariats in the Cabinet Office to ensure that plans and systems to cover the full range of potential disruption are in place and exercised;
- To improve resilience to disruption across government and the public sector, including supporting ministers in developing policy, agreeing priorities and planning assumptions, and ensuring that core response capabilities are developed accordingly;
- To improve the capability at all levels of government, the wider public sector, and the private and voluntary sectors to prepare for, respond to, and manage potential challenges through development of key skills and awareness.

The *Emergency Planning College* is an integral part of the CCS. It has a key role to play in the development and promulgation of the UK's resilience doctrine, and in the development of the cross-organizational communities to deliver it.

Public Private Partnerships

The NISCC's Public Private Partnerships

In addition to its assurance advice to specific CNI companies, the *National Infrastructure Security Co-ordination Centre* (NISCC) actively promotes two types of information-sharing initiatives.

The first type of initiative consists of *Information Exchanges*, where the NISCC facilitates and attends periodic confidential industry forums. Currently, representatives from over 50 private sector companies share information with each other and with the government under the initiative. There are currently three exchanges: telecommunications industry; finance, and those sectors that use process control or SCADA technologies. Sensitive information is shared in person at Exchange meetings, but is anonymized when passed to other Exchanges, or to a wider CIIP audience.[427]

Warning, Advice, and Reporting Points (WARPs) are an NISCC initiative designed to create and foster small, community-based, inter-linked information-sharing cells. They offer a cost-effective alternative to CERTs and ISACs. The first pilot WARP has been established for local authorities in London. A WARP 'toolbox' is being developed to make it easier to establish further WARPs. This will contain procedures, guidance, documentation,

427 http://www.niscc.gov.uk/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.do, at p. 62.

and possibly software to operate the three core WARP services. The model is widely promoted beyond the CNI and has been adopted into other initiatives.[428]

Other Private-Public Partnerships

There is a wide range of private-sector bodies that work with the public sector to promote information assurance. Among these are:

The Information Assurance Advisory Council (IAAC), founded in 2000, is not part of the UK government, but has government representation. It fosters public private partnerships between corporate leaders, public policy makers, law enforcement, and the research community to address the challenges of information infrastructure protection. The IAAC makes policy recommendations to government and corporate leaders at the highest levels.[429] The IAAC facilitates cross-sectoral dialog, information exchange, and the emergence of new trusted long-term partnerships. The IAAC has active links with the NISCC, the Department of Trade and Industry (DTI), the Office of Science and Technology (OST), and the Office of the e-Envoy, as well as with the private sector and military communities. The IAAC has five working groups dealing with threat assessment, risk assessment, standards, research and development, and education and outreach.[430]

Other Public Private Partnerships include the *British Computer Society* (BCS),[431] the *Internet Security Forum*, the *National Computing Centre*[432], the *Internet Watch Foundation*,[433] and the *Confederation of British Industry*.[434] There is also an annual conference on 'Protecting Critical Information Infrastructures' that brings together private- and public-sector partners.[435]

428 http://www.niscc.gov.uk/IAAC%20NISCC%20Sharing%20is%20Protecting%20v21.doc and http://www.niscc.gov.uk/warp_publications/WARPs.pdf, at p. 69.

429 http://www.iaac.org.uk/start.htm.

430 Parsons, T. J., Protecting Critical Information Infrastructures. The co-ordination and development of Cross-sectoral research in the UK. *Plenary Address at 'The Future of European Crisis Management*, Uppsala, Sweden (March 2001). http://www.krisestyring.dk/krisestyring/uppsala/uppsala.pdf.

431 http://www1.bcs.org.uk.

432 http://www.ncc.co.uk/index.cfm.

433 http://www.iwf.org.uk/index.html.

434 http://www.cbi.org.uk/home.html.

435 http://www.hsaconferences.co.uk/pcii2001_info.htm.

Early Warning Approaches

Unified Incident Reporting and Alert Scheme (UNIRAS)

UNIRAS is the *UK Government Computer Emergency Response Team* (CERT) and is run by the *National Infrastructure Security Co-ordination Centre* (NISCC). It draws on technical support from the *Communications-Electronics Security Group* (CESG), the UK's national technical security authority. Its original customers were government departments and agencies, but in the last few years, this has been expanded to include companies holding sensitive government contracts, and most recently CNI organizations. UNIRAS has three main tasks:

- Response to electronic attack and other significant IT security incidents;
- Warning about IT security incidents and vulnerabilities; and
- Gathering information about IT security incidents.

UNIRAS provides ad-hoc advice on specific problems to individual members and warnings of IT security vulnerabilities by issuing 'Alerts' and 'Briefings'. These Alerts and Briefings are sent to the UNIRAS community by e-mail, but also posted on its website so that any company can make use of them.[436]

Ministry of Defence Computer Emergency Response Team (MODCERT)

The *UK Ministry of Defence* (MOD) is a member organization of both the international *Federation of Incident Response Security Teams* (FIRST)[437] and the *Trusted Introducer* (TI)[438] scheme, both of which provide a mechanism for sharing information on computer security incidents amongst communities of interest. MODCERT consists of a central co-ordination center and a number of monitoring and reporting centers, Warning, Advice, and Reporting Points (WARPs), and incident response teams. It also works closely with the government CERT, UNIRAS.[439]

436 http://www.uniras.gov.uk.
437 http://www.first.org.
438 http://www.ti.terena.nl.
439 http://www.mod.uk/cert.

CIIP Country Surveys

United States

The Country Survey of the United States 2004 was written with the help of John A. McCarthy and Emily Frye, Critical Infrastructure Protection Project, George Mason University School of Law, Arlington, and Scott C. Algeier, US Chamber of Commerce, Washington.

United States

Critical Sectors

Critical Infrastructure Protection (CIP) in the United States 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.[440]

In the US, critical infrastructures are defined[441] according to the *USA Patriot Act* of 2001, section 1016(e): "[…] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[442]

In the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*[443] and in the *National Strategy to Secure Cyberspace*[444], both from February 2003, the following critical infrastructure sectors are identified:

- Agriculture and Food,
- Banking and Finance,
- Chemicals and Hazardous Materials,
- Defense Industrial Base,
- Emergency Services,
- Energy,

440 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.

441 In the Homeland Security Presidential Directive/HSPD-7, 17 December 2003 (see below). http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

442 http://www.epic.org/privacy/terrorism/hr3162.html ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" is the full title of the USA PATRIOT Act of 26 October 2001).

443 The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

444 The White House. *The National Strategy to Secure Cyberspace* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

- Higher Education,
- Insurance,
- Law Enforcement,
- Oil and Gas,
- Postal and Shipping,
- Public Health,
- Telecommunications and Information Technology,
- Transportation,
- Water.

Moreover, the following key assets are identified for major protection initiatives:

- Commercial Key Assets,
- Dams,
- Government Facilities,
- National Monuments and Icons,
- Nuclear Power Plants.[445]

Varying definitions of the critical infrastructure sectors are in use, and this listing is not a static list. As different sectors become more important, or more crucial to maintaining basic operations, different sectors will be included (or perhaps excluded) from this list.

The protection of all of these infrastructure sectors is related to cyberspace at a fundamental level because of their reliance on interconnected computers, servers, routers, switches, and fiber-optic cables that ensure their functionality.

Initiatives and Policy

There have been several efforts since the 1990s to better manage Critical Infrastructure Protection and Critical Information Infrastructure Protection (CIIP) in the US. CIIP plays an important role in the overall US security strategy. The US government views CIIP as an element of its homeland security strategy. Where traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the

445 The National Strategy for Physical Protection of Critical Infrastructures and Key Assets. http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

intelligence community with respect to defense, homeland security is viewed as a shared responsibility that requires coordinated action across many sectors.[446]

The US government is especially committed to CIIP, as evidenced by President George Bush signing a US$ 37.4 billion Homeland Security appropriations bill for 2004. US$ 839.3 million was allocated specifically to the *Information Analysis and Infrastructure Protection Directorate*, which has responsibility for cybersecurity. Among other things, this money will fund research and development in examining network weaknesses and evaluating threats and vulnerabilities.

The following government efforts are aimed at developing initiatives and creating appropriate policies to address CIIP.

Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the *Critical Infrastructure Working Group* (CWIG), President Bill Clinton set up the *Presidential Commission on Critical Infrastructure Protection* (PCCIP) in 1996, the first national effort to address the vulnerabilities of the information age.

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.[447] The commission's most important decision was to foster cooperation and communication between the private sector and the government.

Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP in May 1998 and issued *Presidential Decision Directives* (PDD) 62 and 63.[448] They established policy-making and oversight bodies making use of existing agency authorities and expertise. 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*.[449]

446 Ibid.

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

448 Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63.*

449 Clinton, Presidential Decision Directive 63.

Homeland Security Presidential Directive/HSPD-7

On 17 December 2003, President Bush released a new *Homeland Security Presidential Directive/HSPD-7*, which supersedes PDD 63 of May 1998, and any Presidential directives issued prior to this HSPD-7.

This new directive establishes a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and protect them from terrorist attack. Basically, it identifies which government agencies are responsible for protecting specific infrastructure sectors. A key element of this directive is the requirement that *Sector-Specific Agencies* will collaborate with appropriate private sector entities.

Also, the HSPD-7 says that by July 2004, the heads of all Federal departments and agencies shall develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate, including identification, prioritization, protection, and contingency planning. On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts.[450]

The *Secretary of Homeland Security* will serve as the "the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."

National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national masterplan for CIP as "*Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0*".[451] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.[452]

450 http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

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

452 http://www.ciao.gov/resource/np1final.pdf.

Homeland Security Executive Decisions

In the aftermath of 11 September 2001, President George Bush signed two *Executive Orders* (EO) affecting CIP. With EO 13228, entitled "*Establishing the Office of Homeland Security and the Homeland Security Council*" and issued on 8 October 2001, the *Office of Homeland Security* was established, headed by the Assistant to the President for Homeland Security.[453] One of its functions is the coordination of efforts to protect the country 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 "*Critical Infrastructure Protection in the Information Age*" 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".[454] Finally, the EO also established the *National Infrastructure Advisory Council* (NIAC).[455]

National Strategies

On 14 February 2003, the White House released two presidential national strategies that are follow-on documents to the *National Strategy for Homeland Security*, which was released in July 2002.

- The main aim of the *National Strategy to Secure Cyberspace* is to engage US citizens in securing the portions of cyberspace they own, operate, control, or with which they interact.
- The main aim of the *National Strategy for Physical Protection of Critical Infrastructure and Key Assets* is to reduce the nation's vulnerability to acts of terrorism by protecting the national critical infrastructure and key assets from physical attack.

The fact that the US government has further defined and elaborated on the *National Strategy for Homeland Security* in two separate documents highlights an important distinction between critical information infrastructure

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

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

455 Bush, Executive Order 13231.

protection and critical infrastructure protection. However, several sectors have been identified as crucial to both types of vulnerable infrastructure.

The National Strategy to Secure Cyberspace

The *National Strategy to Secure Cyberspace* (NSSC) [456] recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from the entire society and government. In order to achieve this goal and to engage the public in securing cyberspace, a draft version of the NSSC has been released for public comment, and ten town hall meetings were held around the US to gather input on the development of a national strategy. This careful vetting process is a clear sign that cyberspace security is viewed as a public private partnership.

The NSSC defines cyberspace as an "interdependent network of information technology infrastructures," and depicts cyberspace as the nervous system or control system of society. The NSSC outlines an initial framework for both organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation states, while highlighting the role of public private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;
- To reduce the national vulnerability to cyber-attack;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that the private sector is best equipped and structured to respond to cyber-threats. Therefore, public private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* states that the CI sectors of the US provide the foundation for national security, governance, economic vitality, and the American way of life. An attack on the nation's critical infrastructures and key assets could not only result in large-scale human casualties and property destruction, but also damage the national prestige, morale, and confidence, as experi-

456 Own shorthand expression.

enced in the 11 September 2001 attacks. As a result, the following strategic objectives are considered:

- To identify and assure the protection of those infrastructures and assets that are deemed most critical in terms of national-level consequences for public health and safety, governance, economic and national security, and public confidence;
- To provide timely warning;
- To assure the protection of other infrastructures and assets that may become terrorist targets over time.

By pursuing these objectives, coordinated action is required on the part of federal, state, and local governments, as well as the private sector and concerned citizens. The *Department of Homeland Security* (DHS) (see below) will provide overall cross-sector coordination in this new organizational scheme, acting as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector. Cross-sector initiatives should be fostered in the areas of planning and resource allocation, in information-sharing, in personnel security (including background checks where appropriate) and awareness, in research and development, and in modeling, simulation, and analysis.[457]

Procedures for Handling Critical Infrastructure Information

In April of 2003, the DHS released regulations for handling critical infrastructure information.[458] These regulations, which were authorized in the Homeland Security Act of 2002, provide rules for the receipt, care, and storage of Critical Infrastructure Information, the maintenance of security and confidentiality, and methods for dealing with proprietary or business-sensitive information. The basic concept of the regulations again underscores the fundamental principles of public private partnership. It stipulates that business-sensitive information that businesses voluntarily submit to the *Department of Homeland Security* may be labeled CII and exempted from *Freedom of Information Act* (FOIA) disclosure. This change in the law has potentially broad effects on normal business operations, as disclosure of information held by government has traditionally been favored in the US.

457 http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

458 Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (2003) (to be codified at 6 C.F.R. §29).

Organizational Overview

Public Agencies

Department of Homeland Security (DHS)

The attacks of 11 September 2001 provided the impetus to restructure the overall organizational framework of CIIP in the US. The most important change was the establishment of the *Department of Homeland Security* (DHS).[459] It is expected that the DHS will become a federal center of excellence for cybersecurity and critical infrastructure protection and will encompass the following roles:

- Developing a comprehensive national plan for securing the key resources and critical infrastructures of the US;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance and emergency recovery plans to the private sector and other government entities;
- Coordinating with other agencies of the government to provide specific warning information and protective measures, and to fund research and development;
- To circulate information regarding cyber-security to the private sector;
- To fund research and development.

The DHS brought together 22 existing federal agencies in the largest federal reorganization since 1947. The Department is divided into five major divisions or 'Directorates': (1) Border and Transportation Security, (2) Emergency Preparedness and Response, (3) Science and Technology, (4) Information Analysis and Infrastructure Protection and (5) Management. In addition to these five directorates, several other critical agencies are amalgamating with the new department or are being newly created, such as the *US Coast Guard*, the *US Secret Service*, the *Bureau of Citizenship*, and the *Immigration Services*.[460] In addition, the DHS maintains a special liaison office for the private sector, again highlighting the essential focus on public private collaboration.

The next section provides an overview of key public actors in CIIP today. Due to the consolidation brought about by the formation of the DHS, many of these entities are now part of the department. It is important to note that

459 http://www.dhs.gov.
460 http://www.dhs.gov/dhspublic/display?theme=9&content=1075.

there are other governmental entities and agencies besides the DHS that are focused on homeland security.

Directorate for Information Analysis and Infrastructure Protection (IAIP)

As one of the five major divisions of the US Department of Homeland Security, the *Directorate for Information Analysis and Infrastructure Protection* (IAIP) [461] is responsible for identifying and assessing current and future threats and vulnerabilities to the homeland, issuing timely warnings, and taking preventive and protective action. The directorate focuses special attention on the protection of critical infrastructure and cyber-security.

The IAIP leads and coordinates the national effort to secure the nation's infrastructure and fosters an active partnership with the private sector. With the creation of the IAIP, the government has established a central contact point for state, local, and private entities to coordinate protection activities with the federal government.

An especially high priority is placed on protecting the infrastructure of cyberspace from terrorist attacks whose possible consequences could cascade across many sectors, causing widespread disruption of essential services, damage to the economy, or risk to public safety. Therefore, the IAIP has unified and focused the key cyber-security activities of the *Critical Infrastructure Assurance Office* (CIAO), formerly part of the *Department of Commerce*; the *National Infrastructure Protection Center* (NIPC), from the FBI; and the *Federal Computer Incident Response Center* (FedCIRC), formerly of the *General Service Administration*. Because CI relies heavily on information and telecommunication services and interconnections, the IAIP also assumed the functions and assets of the *National Communications Systems* of the *Department of Defense*, which coordinates emergency preparedness for the telecommunications sector and some responsibility of the *Energy Security and Assurance Program of the Department of Energy.*[462]

While the IAIP directorate is still reviewing its restructuring and incorporating various entities into its structure, it is expected that its infrastructure protection component will be organized into four divisions. These will likely include the *Infrastructure Coordination Division*, the *National Cyber Security Division*, *the Protective Services Division*, and the *National Communications System*.

461 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.
462 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

National Cyber Security Division (NCSD)

In June 2003, the *National Cyber Security Division* (NCSD) was created under the IAIP to combat Internet-based attacks against government and critical private-sector backbone networks. The NCSD's main tasks are to identify, analyze, and reduce cyber-threats and vulnerabilities, issue threat warnings and coordinate incident response, as well as provide technical assistance in operations continuity and recovery planning.

The NCSD builds upon the existing capabilities transferred to the DHS from the former *Critical Infrastructure Assurance Office* (CIAO), the *National Infrastructure Protection Center* (NIPC), the *Federal Computer Incident Response Center* (FedCIRC), and the *National Communications System* (NCS). The NCSD works together with the *National Institute of Standards and Technology* (NIST) regarding the security of federal systems and with federal law enforcement authorities.[463]

The division is organized around three units designed to:

- Identify risks and help reduce the vulnerabilities to the government's cyber assets and coordinate with the private sector to identify and help protect critical cyber assets;
- Oversee a consolidated *Cyber Security Tracking, Analysis and Response Center* (CSTARC), which will detect and respond to Internet events; track potential threats and vulnerabilities to cyberspace; and coordinate cyber-security and incident response with partners from the private sector and international partners at the federal, state, and local levels;
- Create, in coordination with other appropriate agencies, cybersecurity awareness and education programs and partnerships with consumers, businesses, governments, academia, and international communities.[464]

Critical Infrastructure Assurance Office (CIAO)

The *Critical Infrastructure Assurance Office* (CIAO)[465] was created in May 1998 and is now part of the IAIP. The *Planning and Partnerships Office* (PPO) within the IAIP assumed many of the responsibilities previously held by the CIAO, such as raising issues that cut across industry sectors and

463 http://www.dhs.gov/dhspublic/display?content=916.
464 http://www.dhs.gov.
465 http://www.ciao.gov.

ensuring a cohesive approach to achieving continuity in delivering critical infrastructure services. Its main tasks are:

- To coordinate and implement the national strategy;
- To assess the government's own risk exposure and dependencies on CI;
- To raise awareness and public understanding and participation in CIP efforts;
- To coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

National Infrastructure Protection Center (NIPC)

In 1998, the *Office of Computer Investigations and Infrastructure Protection* (OCIIP) was expanded to become the inter-agency *National Infrastructure Protection Center* (NIPC).[466] The NIPC is located at the FBI headquarters, but is part of the DHS IAIP. It coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and monitoring reconstitution efforts. It coordinates the federal government's response to incidents, mitigating attacks, investigating threats, and monitoring reconstitution efforts.

Office of Homeland Security

The *Office of Homeland Security* was established in October 2001. Its mission is to "develop and coordinate the implementation of a comprehensive national strategy to secure the US from terrorist threats and attacks."[467] Among its functions is the coordination of efforts to ensure rapid restoration of CI after disruption by a terrorist attack.[468] 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.[469]

Homeland Security Council

The *Homeland Security Council* is an executive entity charged with advising the president on homeland security matters. In order to more effectively coordinate the homeland security policies and functions of the government, the council assesses the objectives, commitments, and risks, and oversees

466 http://www.nipc.gov.
467 http://www.dhs.gov/dhspublic/theme_home1.jsp.
468 Bush, Executive Order 13228.
469 Interview with a representative of the US Chamber of Commerce, June 2002.

and reviews the homeland security policies of the government. The council makes recommendations resulting from these activities to the president.

The council comprises a Principals Committee as well as coordination committees. The *Secretary of Homeland Security*, the *Secretary of Treasury*, the *Secretary of Defense*, the *Attorney-General*, the *Secretary of Health and Human Services*, the *Secretary of Transportation*, the *Budget Director for Central Intelligence*, the *FBI Director*, the *FEMA Director*, the *Chief of Staff to the President*, and the *Chief of Staff to the Vice President* compose the Principals Committee.

One of the coordination committees within the council is focused on CI. It is centered on the protection of both physical and virtual infrastructure.[470]

US Department of State

With respect to the formulation of an international CIP program in the US, the *Department of State* has overall statutory authority to conduct foreign affairs and therefore takes the lead in the interagency process of coordinating international CIP matters. The *Department of State* works together with other departments and agencies (including the Departments of Homeland Security, Justice, Defense, Commerce, Energy, Treasury, and Transportation, as well as the intelligence community, and others) to coordinate their objectives in an overarching strategy. Further activities of the Department of State include chairing the interagency *International CIP Policy Working Group*, which has key coordination mechanisms, and monitoring the implementation of agreements.[471]

Congressional Focus

Both Houses of Congress have created bodies to focus on CIIP issues. As part of the House of Representative's Select Committee on Homeland Security, the *House Subcommittee on Cybersecurity, Science, and R&D* examines the following: security of computers, telecommunications, information technology, industrial control, electric infrastructure, and related data systems including science, research, and development; protection of government and private networks and computer systems from domestic

470 http://www.whitehouse.gov.

471 Russell, Erica B. International and Interagency Critical Infrastructure Protection Coordination. *Presentation at the PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century* (Stockholm, 17–18 November 2003). http://www.krisberedskapsmyndigheten.se/english/documents/seminar/programme_pfp-seminar_17-18_nov2003.pdf.

and foreign attack; prevention of injury to civilian populations and physical infrastructure caused by cyber attack; and oversight of relevant sectors. This subcommittee has held a number of hearings on related topics.

Within the Senate Committee on the Judiciary, the *Subcommittee on Terrorism, Technology, and Homeland Security* has oversight of laws related to government information policy, electronic privacy, security of computer information, and the Freedom of Information Act.

Defense Community

In response to the May 1998 *Presidential Decision Directive/NSC-63* (PDD-63), the *Department of Defense* (DOD) assigned the additional duty of *Critical Infrastructure Assurance Officer* (CIAO) to the *DOD Chief Information Officer* (CIO). In addition, each of the armed services (air force, army, and navy) established CIAOs, typically as an additional duty for the respective department's CIO. The armed services' CIAOs were responsible for developing a plan for protecting their department's critical virtual and physical infrastructure, for coordinating remedial efforts and reported to the DOD CIO/CIAO. Further, regional and functional commanders-in-chief and the services began identifying and securing their critical, operationally relevant assets and related infrastructure components.

Initially, the DOD and the individual services vulnerability assessment teams (inside the fence) and the *Joint Program Office for Special Technology Countermeasures* (outside the fence) conducted scheduled vulnerability assessments by installation on a regional basis to identify single points of service that could be vulnerable to loss through natural causes, human error, or deliberate attack.

With the establishment of the *Department of Homeland Security* (DHS), the DOD has established an *Assistant Secretary for Homeland Defense* and implemented a campaign plan for domestic military missions. The DOD's Defense Planning Guidance for the fiscal year 2004 defines the military's role in homeland defense as the military protection of US territory, the domestic population, and critical defense infrastructure against external threats and aggression.

Further, this guidance also calls for DOD to routinely study state activities to deter potential aggressors and to prepare US military forces for action, if needed. The functions of the previous DOD and armed services CIAOs have been integrated into the DHS under the IAIP directorate with the *Planning and Partnerships Office* (PPO) within DHS-IAIP, assuming many of the responsibilities previously held by the military CIAOs.

In addition to the lead in CIIP taken by the various DHS offices, the White House, Congress, and the defense community, each critical sector has a lead agency that can regulate or suggest practices for CIIP. For example, the lead agency for the energy sector is the *Department of Energy*. The *Department of Energy* regulates the nuclear power plants, and has mandated certain computer security rules for the plants. Further, the *Department of the Treasury* has responsibility for the financial services sector.

Public Private Partnerships

The government has actively promoted cooperation between the public and private sectors. It is a critical component of the national strategies and a strategic objective of the administration. Because the private sector owns the majority of critical infrastructure assets in the US (80–90 per cent), public private collaboration is essential to achieving effective CIIP. Further, one of the *Department of Homeland Security*'s main tasks will be to facilitate partnership efforts between the government and the private sector. It will develop relationships with and among state, local, and private entities.

To date, a number of unresolved issues have prevented comprehensive sharing between the public and private sectors. For example, unresolved legal issues – such as the *Freedom of Information Act* (see above), as well as anti-trust and liability issues, have hampered effective information-sharing. According to experts, resolving these issues should enhance information-sharing and spur the growth of ISACs.[472]

Office of Private Sector Liaison, Department of Homeland Security

The *Department of Homeland Security* has demonstrated its commitment to working with the private sector and strengthening public private partnerships by establishing the *Office of Private Sector Liaison*.[473] This office provides businesses with a direct line into the department. It acts both as an advocate for the private sector, by informing the secretary of their concerns, and as a clearinghouse, by directing businesses to the appropriate agency or directorate. The office is coordinated by the *Special Advisor to the Secretary for the Private Sector*.

One of the Liaison Office's main services is coordinating with *Information Sharing and Analysis Centers* (ISACs), trade associations, and businesses whenever there is a change in the threat level. The office provides guidelines

472 Interview with a representative of the US Chamber of Commerce, June 2002.
473 http://www.dhs.gov/dhspublic/display?theme=37.

and suggestions to private sector entities, so they may properly respond to the changes. Additionally, the office clarifies liability and compliance issues for businesses affected by new homeland security laws or regulations.

Although the Liaison Office is a relatively new post, it is growing steadily in significance and responsibility. The department plans to develop regional divisions next year, and the Liaison Office will play an important part in community outreach. With over 25 million businesses to coordinate, the office faces a tremendous task.

Information Sharing and Analysis Centers (ISACs)

Today, most critical infrastructure industry sectors have established their own *Information Sharing and Analysis Center* (ISAC), or are about to do so. 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).[474]
- The telecommunications industry has established 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 NCC, and members decide whether the suspect behavior is serious enough to report to the appropriate federal authorities.[475]
- The electric power sector has created 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.[476] The government and industry work together in the NERC to ensure the resiliency of the electricity infrastructure to potential physical and cyberspace attacks.[477]

474 http://www.fsisac.com.

475 http://www.ncs.gov/ncc.

476 http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.energyisac.com.

477 http://www.nerc.com/cip.html.

- 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 is operated by Internet Security Systems.[478]
- Other ISACs include the Surface Transportation ISAC,[479] the Oil and Gas ISAC,[480] the Water Supply ISAC, the Chemicals Industry ISAC, the Emergency Fire Services ISAC, the Emergency Law Enforcement ISAC, the Food ISAC, the Health ISAC, and the Interstate ISAC.

In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council. This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

InfraGard

InfraGard is a partnership between industry and the US government as represented by the FBI. The *InfraGard* initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share information among their membership. This information is then disseminated through the *InfraGard* network and analyzed by the FBI.[481] There are currently over 75 *InfraGard* chapters.

National Cyber Security Alliance (NCSA)

The *National Cyber Security Alliance* (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. It tries to raise citizens' awareness of the critical role that computer security plays in protecting the nation's Internet infrastructure, and to encourage computer users to protect their home and small business systems.[482] The NCSA is sponsored by a variety of organizations ranging from America Online, Apple, AT&T, CISCO Systems, Microsoft, MITRE, and Symantec to CERT/CC, GSA, and InfraGard.

478 https://www.it-isac.org.
479 http://www.surfacetransportationisac.org.
480 http://www.energyisac.com.
481 http://www.infragard.net.
482 http://www.staysafeonline.info.

Partnership for Critical Infrastructure Security (PCIS)

The *Partnership for Critical Infrastructure Security* (PCIS) grew out of initiatives outlined in *Presidential Decision Directive 63* (PDD 63). It is a private-sector coalition that works to secure CI and examines cross-sector issues.

On 18 September 2002, many private-sector entities released plans and strategies for securing their respective infrastructures. The PCIS has played a unique role in facilitating private-sector contributions to this strategy.[483] The PCIS maintains a CIP calendar of conferences and other events as well as an Awareness Resources Repository, a searchable index of information on critical infrastructure security.[484]

Early Warning Approaches

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on information-sharing are also engaged in early-warning activities.

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.[485] According to some reports, 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 high-quality information on law enforcement and intelligence. Under PDD 63, the NIPC as part of the FBI was given 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.[486] The NIPC, as discussed above,

483 http://www.pcis.org.
484 http://www.pcis.org.
485 President's Commission on Critical Infrastructure Protection, Critical Foundations.
486 Clinton, Presidential Decision Directive 63.

was incorporated into the DHS. The comprehensive early-warning system is now likely to be channeled through the US CERT, discussed below. The FBI still retains its responsibilities for addressing cybercrime.

Directorate for Information Analysis and Infrastructure Protection (IAIP)

The *Department of Homeland Security's Directorate* IAIP[487] was set up with a special focus on systematically analyzing all information and intelligence on potential terrorist threats within the US. This division compiles and analyzes information from multiple sources, including the CIA, the FBI, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA), and issues early warnings of terrorist attacks.[488] In case of an attack, IAIP would aim to:

- Provide warning of threats against the US, including physical and virtual attacks;
- Issue threat advisories through the Homeland Security Advisory Systems;
- Provide information about terrorist threat to the public, private industry, state, and local government.[489]

The new *National Cyber Security Division* (NCSD) within the IAIP will issue alerts and warnings around the clock. Its three units are geared to early detection of cyber threats, especially the Cyber Security Tracking, Analysis & Response Center.

US-CERT

On 15 September 2003, the *Department of Homeland Security*, in conjunction with the *CERT Coordination Center* (CERT/CC) at Carnegie Mellon University, announced the creation of the US-CERT. The US-CERT works with the *National Cyber Security Division* (NCSD) of the IAIP to prevent and mitigate cyber-attacks and to reduce vulnerabilities to cybernetic attacks. The US-CERT is also the central element in the NCSD's *Cyber Security Tracking Analysis and Response Center*, which includes the *Federal Computer Incident Response Center* (FedCIRC).

The US-CERT initiative is designed to utilize the CERT/CC's capabilities to help accelerate the nation's response to cyber-attacks and vulnerabilities.

487 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.
488 http://www.whitehouse.gov/deptofhomeland/sect6.html.
489 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

The initiative also enables the DHS to provide expanded analysis, warning, and response coordination.[490]

Federal Computer Incident Response Center (FedCIRC)

The responsibility for detecting and responding to cyber-attacks on federal agencies 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 FedCIRC was incorporated into the IAIP as part of the DHS in March 2003 and is now part of the *National Cyber Security Division* (NCSD).

The Bush administration is expected to issue a guide for federal agencies to report computer security incidents to the FedCIRC. The guide is expected to outline the type of information required in an incident report that will give FedCIRC the data it needs to track and analyze incident reports.

CERT Coordination Center, Carnegie Mellon University

The CERT/CC is located at the *Software Engineering Institute* (SEI), a federally funded research and development center operated by Carnegie Mellon University. It was established in 1988 after the Morris worm crashed 10 per cent of the world's Internet systems. CERT/CC acts as a coordination hub for experts during security incidents, and works to prevent future incidents.[491]

The CERT/CC acts through several mechanisms. First, they research and assess network vulnerabilities and develop risk assessments. Second, they disseminate information to the public through regular security alerts and presentations to the public. Finally, members of the CERT/CC participate in various security groups to improve Internet security and network survivability. The CERT/CC will also now be a primary contributor to the US-CERT.

Internet Security Alliance

The *Internet Security Alliance* (ISAlliance) is a non-profit collaborative effort between the Carnegie Mellon University's *Software Engineering Institute* (SEI) CERT Coordination Center (CERT/CC) and the *Electronic Industries Alliance* (EIA), a federation of trade associations representing 2'500 companies. It was created to provide a forum for intellectual leadership and information-sharing on information-security issues. ISAlliance allows

490 http://www.uscert.gov.
491 http://www.cert.org.

its participants to access threat reports, learn of best security practices, and discuss risk management strategies.

Information-Sharing and Analysis Centers (ISACs)

The *Information Sharing and Analysis Centers* (ISACs) were planned to help create an early-warning database. The idea is that private-sector owners and operators will survey incidents and pass the information on to central point of contact for information-sharing and then distribute it to ISAC membership (see Chapter on 'Public Private Partnerships' above).

Part II
Analysis of Methods and Models for CII Assessment

by Myriam Dunn

Structure of Part II

Introduction

Part II of the Handbook describes methods, models, and approaches used to analyze and evaluate aspects of critical information infrastructures (CII) in the surveyed countries. This is of particular relevance for CIP/CIIP, because it is important to understand the crucial aspects of CI/CII under consideration, such as their behavior under normal circumstances and under stress, as well as their role and criticality for government and society. Such an understanding is necessary in order to cost-effectively prioritize means of preparing for, mitigating, and responding to possible threats.

However, infrastructure owners, regulators, decision-makers, and researchers currently face difficulties in understanding the complex behaviors of interdependent critical infrastructures, because infrastructure networks present numerous theoretical and practical challenges. In general, networks are inherently difficult to understand and to manage. There are several reasons: the structural and dynamical complexity of the networks, their large-scale and time-dependent behavior, their dynamic evolution, the diversity of possible connections between nodes, and node diversity.[1]

Additionally, many of the challenges and problems posed by the infrastructures are just emerging. The inherent system characteristics of new information infrastructures, especially, differ radically from those of traditional infrastructures in terms of scale, connectivity, and dependencies. Moreover, there are several "drivers" that will likely aggravate the problem of critical information infrastructures in the future. Among these drivers are the interlinked aspects of market forces, technological evolutions, and newly emerging risks. This situation forces analysts to constantly look ahead and to develop new analytical techniques, methodologies, and mindsets to keep up with the rapid developments in the technological sphere.

Whenever possible, Part II focuses on approaches for critical information infrastructures (CII). However, the majority of the discussed methods and models are designed for the assessment of critical infrastructures (CI). This is due to the fact that the CII is usually just perceived as one special part of the overall CI. The following seven major aspects of CI/CII assessment are discussed in individual subchapters of Part II:

1 Strogatz, Steven H. "Exploring Complex Networks". *Nature*, 410 (8 March 2001): pp. 268–276. http://tam.cornell.edu/SS_exploring_complex_networks.pdf.

1) *Sector analysis*: This subchapter introduces approaches aimed at defining critical sectors and approaches used to specify various characteristics of critical sectors, such as the economic environment, core processes, or interdependencies betweens sectors;
2) *Interdependency analysis*: This subchapter addresses the question of how to categorize interdependencies and gives examples of qualitative interdependency analyses;
3) *Risk analysis*: This subchapter broadly introduces the technique of risk analysis, specifies nine steps that can be included in an IT risk analysis, and provides examples of risk analysis processes designed specifically for CI /CII;
4) *Threat assessment*: This subchapter addresses aspects of threat assessment, namely a management methodology, a general description of the current threat environment, and an IT risk analysis approach;
5) *Vulnerability assessment*: This subchapter introduces various vulnerability assessment approaches with different focal points;
6) *Impact assessment*: This subchapter shows examples of how to evaluate the impact and consequences of an adverse event;
7) *System analysis*: This subchapter presents approaches that employ mathematical models and simulation tools to assess aspects of CI/ CII.

In each chapter, a diverse range of country-specific approaches serve as examples. Some more comprehensive approaches that offer illustrations for more than one chapter (such as the Australian PreDict approach, or the Dutch KWINT Report) appear more than once under different subheadings. To facilitate reading, these approaches are marked by a sign (♦) and a cross-reference (see also Table 1 for overview of examples in the seven chapters). Further, important terms are included in the key terms section (Appendix A1); an entry is marked by an arrow (→).

Country Specific Approaches	1) Sector Analysis	2) Interdependency Analysis	3) Risk Analysis	4) Threat Assessment	5) Vulnerability Assessment	6) Impact Assessment	7) System Analysis
PreDict (AU)	233–234	246–247			279–280		
NSW (AU)			257–258	271–272			
NCPG (Can)	229–230						
CIPTF (Can)	235	247–249	259				
OCIPEP (Can)				273–274		289	
M&S* (EU)							295–296
CORAS(EU)			260–261				
EBIOS (Fr)			261–263				
ACIS (Ger)	236–237						
CYTEX (Ger)					280–281		
Quick Scan (NL)	230–231						
Bitbreuk (NL)	237–238						
KWINT (NL)	238–239				281–282		
BAS (No)			263–265				
Roundtables (Swi)	240–241		260				
NISCC (UK)			267–268			289–292	
DoE (US)	242				282–283		
OCTAVE (US)			268–269				
NIST (US)				274–276			
CIAO (US)					284–286		
NISAC (US)							296–297

Table 1: Examples in Chapters 1 to 7 and corresponding pages.

* This category includes four modeling and simulation projects of the European Union: ACIP, COSIN, DepAuDE, and Safeguard.

1 Sector Analysis

A →*Sector* can be defined as a group of industries or infrastructures that perform a similar function. In general, critical sectors are sectors whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social well-being of a nation. However, the definition of critical sectors varies among countries (→see *Part I: CIIP Country Studies*). Each country uses different standards of what is critical. The definitions also vary over time. Furthermore, some of these infrastructures are always critical, some are occasionally critical, while others only become critical in the case of failures in other vital infrastructures.

What is Sector Analysis?

There are many aspects that might be analyzed in connection with individual sectors, such as how and why they are critical, or what parts of it are particularly vulnerable, etc. In general, sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects such as underlying processes, stakeholders, or resources needed for crucial functions. Sector analysis is a basis for better understanding the larger, complex infrastructure systems. However, sector analysis on its own remains insufficient for a holistic understanding of the larger infrastructures system at hand.

Even more, the division of the whole system into sectors is rather artificial and serves a more practical purpose. It is a need stemming from the fact that infrastructures are mainly owned and operated by private actors, so that the only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. It is therefore necessary for a meaningful analysis to evolve beyond the conventional 'sector'-based focus, since, for example in the case of a terrorist attack, key elements within an infrastructure are more likely targets than entire sectors. It makes more sense to categorize targets in terms of their inherent function – e.g., the supply of raw material, distribution nodes, or command and control centers.

How to Determine Which Sectors Are Critical

In sector analysis, the question of "what is critical" is a key problem. The subject of what infrastructures and sectors are to be included in the list of critical assets requires input from private sector experts as well as experts and officials at various levels of government. More often than not, the issue is addressed by expert groups, either in larger or smaller groups, but might also be determined by lead agencies within government. It must be kept in mind that therefore results often depend on the subjective impressions of experts.

Since different people from different communities are involved in the process, a common understanding and definition of the term "critical" is of the essence: Without standardization of the assets to be considered, prior to any attempted assessment, owners and operators of potentially critical assets might not all choose a common level of granularity. For example, a representative of the electric power generation business might identify generating stations or dams as critical, while others might extend that assessment to the level of turbines or bearings.[2]

Usually, a component or a whole infrastructure is defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to the interdependency between the component or the infrastructure and other infrastructures. In a broader view, infrastructures or components of infrastructures have come to be seen as critical due to their inherent symbolic meaning.[3]

2 Cf. Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets* (Draft, 19 December 2002): p. 2.

3 For more details, see Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.). Stockholm International Peace Research Institute (SIPRI), *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford, forthcoming 2004) and *Part I: Country Surveys* , e.g. Country Surveys on Canada and the US.

Examples of How to Determine Which Sectors Are Critical

In the following, two examples are given of how to identify critical sectors:

- Example 1 (Canada) – The National Contingency Planning Group's Approach to Criticality (NCPG)
- Example 2 (the Netherlands) – Quick Scan on Critical Products and Services (Quick Scan)

Example 1 (Canada) – The National Contingency Planning Group's Approach to Criticality (NCPG)

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.[4] Two criteria were used to determine the criticality:

- 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).[5]

In February 1999, the group finished identifying and defining elements of Canada's critical infrastructure. The assessment of criticality was based on information that the NCPG had collected from a broad group of stakeholders, including key industries, and other government departments. It assessed the likelihood of Year 2000 failure on the basis of the state of preparedness for the Year 2000 changeover and progress in developing contingency plans. The

4 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.

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

interdependencies identified in those plans were used to assess the potential impact of failure of critical infrastructure elements.[6]

Example 2 (The Netherlands) – Quick Scan on Critical Products and Services (Quick Scan)

In early 2002, the Dutch government initiated the critical infrastructure protection project *Bescherming Vitale Infrastructuur*, with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT.[7] The project includes four steps: 1) a *quick-scan analysis* of the Dutch critical infrastructure, 2) stimulation of a public-private partnership, 3) threat and vulnerability analysis, and 4) a gap analysis of protection measures. The analysis undertaken under step 1 identifies products and services vital to the nation's critical infrastructure, the (inter-) dependencies of these products and services, and underlying essential processes.

To identify sectors, products, and services comprising the national critical infrastructure, a quick-scan →*Questionnaire* was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were then augmented and refined in seventeen workshops with the vital public and private sectors. In parallel, damage experts evaluated the potential damage impact of loss or disruption of vital products and services on five →*Indicators*: (1) people, (2) animals, (3) the economy, (4) the environment, and (5) immaterial complacency.[8]

To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are 'merely' very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution

6 Office of the Auditor General of Canada. *1999 Report of the Auditor General of Canada, September and November, Chapter 25: Preparedness for Year 2000, Final Preparation.* http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9925ce.html.

7 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services* (April 2003).

8 Luijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). *EICAR Conference Best Paper Proceedings 2003.* http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.

to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale or endangers the minimum quality level." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society.

According to this model, a sector is deemed "critical" if its breakdown or serious disruption could lead to damage on a national scale, or in other words, if the impact of a disruption was severe enough. The definition of vitality was sharpened by making a distinction between direct and indirect vitality: →*Indirect Vitality* is the extent to which other vital products and services contribute to the dependability of the vital service or product, while →*Direct Vitality* is the contribution that a product or service makes to the continuity of the society, which is equivalent to the amount of direct (first-order) damage caused by a loss or serious disruption of the product or service.

In order to assess the first-order direct vitality, all product and services were plotted in a graph, where the relative value of their direct vitality is assigned to the x-axis and the relative value of their indirect vitality to the y-axis (see Figure 1). Products and services marked in the upper right-hand corner of the graph are the most vital and critical ones.

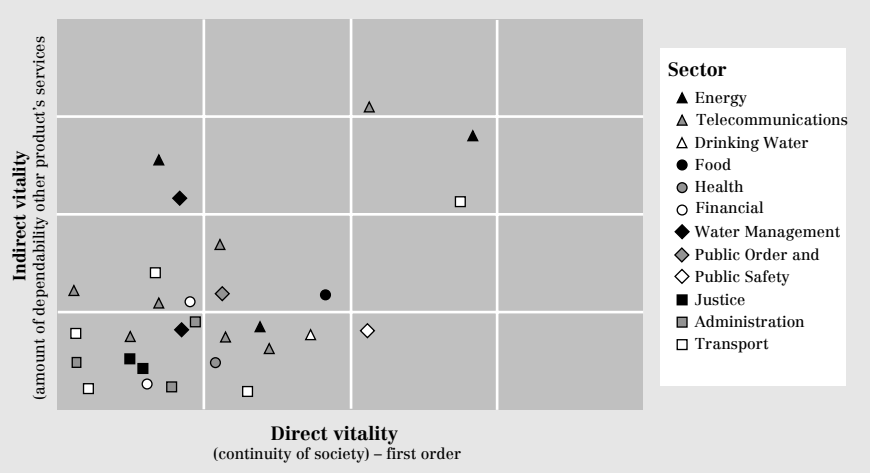


Figure 1: Quick Scan: Vital Products and Services

How to Specify Characteristics of Critical Sectors

The determination of how critical sectors function, what the influencing parameters are in particular sectors, how important specific sectors are to the economy, and who the major players are, including the identification of core functions, value chains, and dependency on information and communication technology in each critical sector, is a prerequisite for subsequent →*Interdependency Analysis* (→see also Chapter 2 on *Interdependency Analysis*).

Most critical sectors have different structures and requirements, so that the appropriate level of detail might vary considerably from sector to sector. They can, for example, be subdivided into industries, into services, into products, or combinations of the various subdivisions.[9] Different industries require different approaches to consulting experts. In some industries, workshops can produce rapid and valuable results, while in other, personal interviews might be necessary.

Often, →*Sector Models* and/or →*Layer Models* are used to illustrate parts of infrastructure systems and their relationship to each other. Usually, they are used as mere illustrations of how critical infrastructures are organized, or serve as the basis for additional steps in the determination of interdependencies. Additionally, simulation systems employ different kind of sector or layer models for visualization. Plain sector models are simple two-dimensional representations of critical sectors. Interdependencies between the sectors might be shown with one or two-way arrows, which might also be rendered with different degrees of intensity. Layer models, on the other hand, come in all variations and sizes (see examples below).

Examples of How to Specify Characteristics of Critical Sectors

In the following, we will consider seven examples of how to specify the characteristics of critical sectors:

- Example 1 (Australia) – PreDict Industry Profiles (PreDict);
- Example 2 (Canada) – Critical Infrastructure Protection Task Force Layer Model (CIPTF);
- Example 3 (Germany) – BSI Methodology for the Analysis of Critical Infrastructural Sectors (ACIS);
- Example 4 (Netherlands) – Bitbreuk Layer Model (Bitbreuk);

9 Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

- Example 5 (Netherlands) – The Four Models of the KWINT-Report (KWINT);
- Example 6 (Switzerland) – Sector Roundtables, Methodological Steps 1–4 (Roundtables);
- Example 7 (United States) – Department of Energy Layer Models (DoE).

Example 1 (Australia) – PreDict Industry Profiles (PreDict)

♦ The PreDict approach also appears in *Chapter 2: Interdependency Analysis*, and in *Chapter 5: Vulnerability Assessment.*

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.[10] Ten industries (Transport, Fuel, IT, Utilities, Health, Third Party Logistics (3PL) Providers, Education and Training, Communications, Defense-Related Manufacturing, and Financial Services)[11] were described in detail in terms of:

- Key Statistics;
- Key Market Segments;
- Regulatory Framework;
- Sector Environment;
- Industry Performance;
- Industry Trends.

The analysis section of the reports offers a summary representation of the sectors focusing mainly on the economic environment. It 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 approaches used were →*PEST Analysis* (to identify at political, economic, social, technological factors), →*Porter's Analysis* (to assess intensity of rivalry; competitors, barriers to entry, threat of substitutes; supplier power, and buyer power), and →*SWOT Analysis* (to assess

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

11 The term *industry* is used interchangeably with the term *sector* in the PreDict approach.

strength, weakness, opportunities, and threats). Additionally, a lifecycle view was drawn from the material gathered during interviews with industry representatives.

The approaches to the applied analyses were initially developed as a starting point for the determination of draft →*Vulnerabilities* for discussion and confirmation by industry and defense representatives during industry interviews and workshops. The results of the initial analysis were refined during the following project phases. The identified vulnerabilities were grouped into twelve →*Broad Risk Areas*. The twelve →*Broad Risk Areas* are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources), Operations (Training), and Flexibility/Adaptability.[12] This was done in order to compare and contrast the vulnerabilities between industry sectors and the defense sector and to group the identified vulnerabilities into common areas for analysis. The majority of the Broad Risk Area titles were drawn from the analytical perspective drawn upon in the PEST and Porter's analysis[13] (→see also Chapter 5 on *Vulnerability Assessment*).

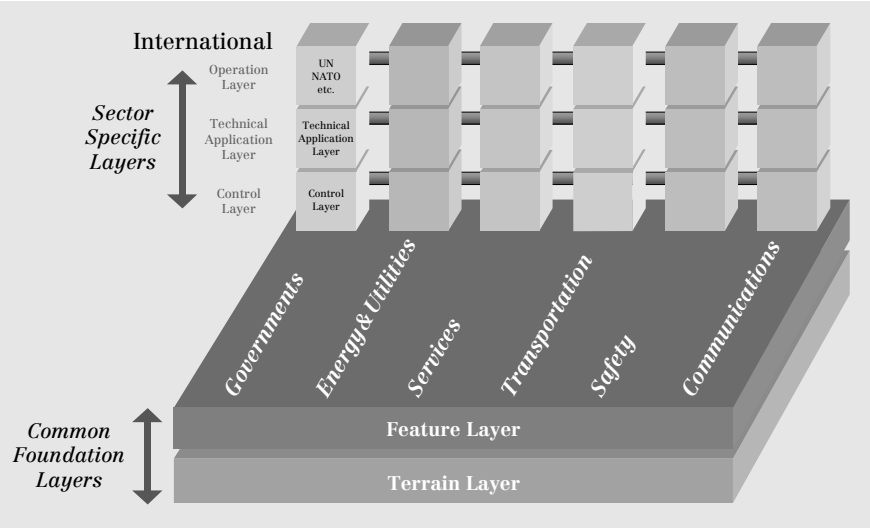


Figure 2: Canadian Layer Model

Example 2 (Canada) – Critical Infrastructure Protection Task Force Layer Model (CIPTF)

♦ The CIPTF approach also appears in *Chapter 2: Interdependency Analysis*, and in *Chapter 3: Risk Analysis*.

In the spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive review process for critical infrastructures in Canada. Based on six sectors identified as critical (Governments, Energy and Utilities; Services; Transportation; Safety; Communications),[14] the CIPTF developed a multi-dimensional →*Layer Model* that takes into consideration the responsibilities of sectors at various levels, namely at the international, federal, provincial, municipal, and the private levels.

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 2 shows the layer model in an initial phase. At this point, 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.[15] This model was used for subsequent interdependency analysis (see →*Chapter 2: Interdependency Analysis*, *Example 2*).

12 See analysis section of industry reports. http://www.defence.gov.au/predict.

13 Ibid.

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

15 Ibid.

Example 3 (Germany) – BSI Methodology for the Analysis of Critical Infrastructural Sectors (ACIS)

The *German Office for Information Security* (BSI) has developed a methodology for the *Analysis of Critical Infrastructural Sectors* (ACIS) to identify the political and economic processes critical for the society as a whole.[16]

The BSI uses a step-by-step approach. First, the sector under examination is described. Then the business processes that are relevant to the functioning of the sector are identified. They are assessed with a criticality analysis, which considers the outcomes in the case of one component of the process breaking down. The probability of the breakdown occurring is assessed. Since historical or statistical data is rarely available for incidents, the involvement of experts is of prime importance for this kind of analysis. Five →*Categories* (insignificant, minor, moderate, major, and catastrophic) are used to describe

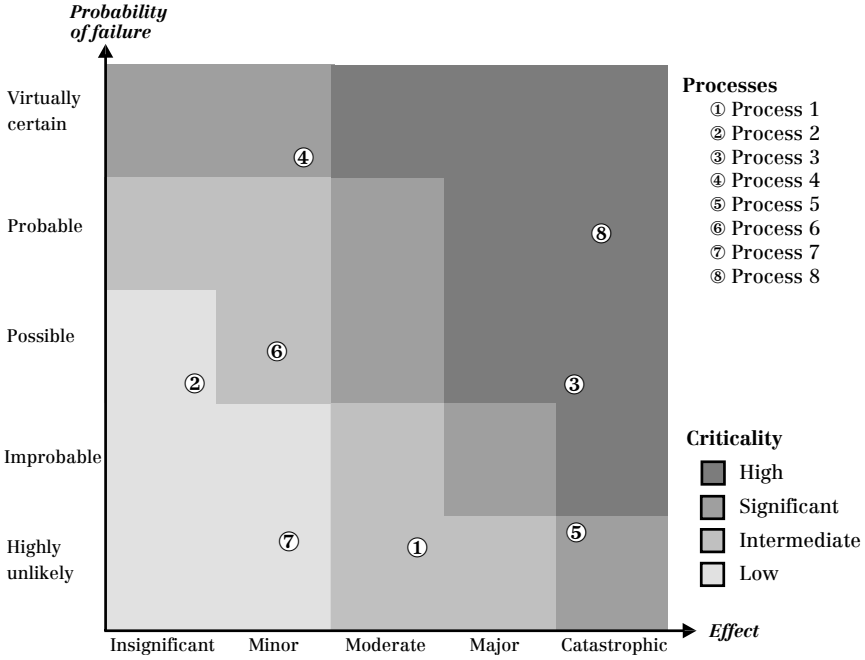


Figure 3: Criticality Matrix for Processes[17]

16 Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

17 Ibid.

the effects or the possible degree of damage, and another five →*Categories* (highly unlikely, improbable, possible, probable, virtually certain) are used to describe the probability of failure. The overall criticality of the process is derived from the combination of effects and failure probability.

The individual processes can then be plotted in a →*Criticality Matrix* (Figure 3).

Only the few business-critical processes that are also critical for a whole sector (those considered highly and significantly critical are in the top right corner in the figure) are taken to the next abstraction level in the analysis ("sector analysis level"). These samples of processes are analyzed in terms of their criticality. A second criticality matrix for sector processes helps to identify those that are also critical for the next level, namely at the abstraction level of "society". In the next step, only those processes that are deemed significantly or highly critical for the whole of society are assessed in terms of their dependence on IT. In this way, the methodology elaborated by the BSI serves as a filtering and cost-effectiveness tool, since it helps to significantly reduce the amount of work that is required for the analysis.[18]

Example 4 (Netherlands) – Bitbreuk Layer Model (Bitbreuk)

The model proposed by the *BITBREUK* report,[19] which focuses on the ICT infrastructure, is a →*Layer Model* with vertically stacked elements of CII and a focus on the IT sector (Figure 4).

Electrical power supply is considered to be the single factor underlying all ICT. Above this first layer are four more layers. The infrastructure's middle layer is located at 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

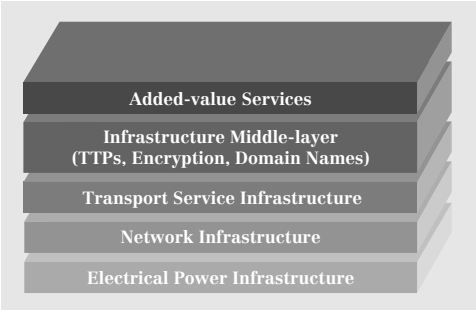


Figure 4: Bitbreuk Layer Model

18 Ibid.

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

services chains for government and for public and commercial organizations. These added-value services are dependent on the availability and integrity of the underlying layers of infrastructure. 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.[20]

Example 5 (Netherlands) – The Four Models of the KWINT Report (KWINT)

♦ The KWINT approach also appears in *Chapter 5: Vulnerability Assessment.*

The *Stratix Consulting Group/ TNO FEL* completed the so-called *KWINT-Report* (from the Dutch working title "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid") in 2001.[21] The overall aim of the project was to analyze the current vulnerabilities of the Dutch section of the Internet,[22] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[23] In order to clarify the roles of various actors and address the diversity, interdependencies, and vulnerabilities, four models with different orthogonal points of view were proposed (Figure 5).

- 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 6).

20 Luiijf, Klaver, In Bits and Pieces, pp. 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.

21 Luiijf, Eric., M. Klaver, and 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).

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

23 Luiijf, Klaver, and Huizenga, The Vulnerable Internet.

- 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 the importance of the physical location of the operational facilities when analyzing vulnerabilities.[24]

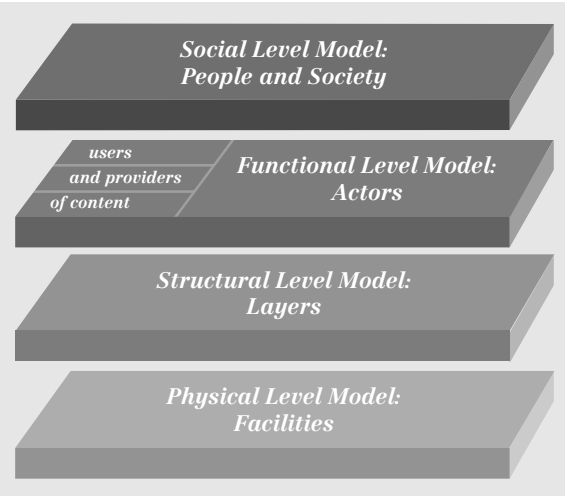


Figure 5:
Four Levels of Models

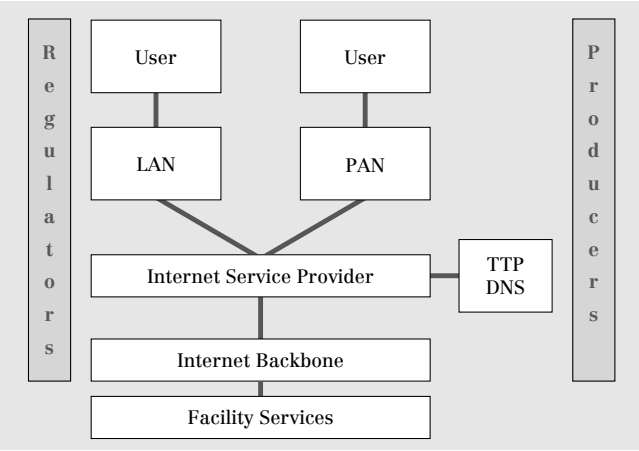


Figure 6:
Functional Model with Types of Actors

24 Luiijf, Klaver, and Huizenga, The Vulnerable Internet, pp. 3–5.

Example 6 (Switzerland) – Sector Roundtables, Methodological Steps 1–4 (Roundtables)

♦ The Sector Roundtables approach is also described in *Chapter 3: Risk Analysis.*

Under the auspices of the *Swiss InfoSurance Foundation*, sector-specific risk analysis roundtables are conducted for ten sectors, using a common methodology[25] (→see also Chapter 3 on *Risk Analysis*). The methodology used for each of the sectors is a ten-step risk analysis approach (see Table 2):

System Analysis		
Step		*Aim*
1	Sectors	Risk estimate for the 10 sectors
2	Sub-Sectors	Structure sector in organisational units
3	Core Functions	Structure sub-sectors according to functional core functions
4	Resources	Identify resources necessary for execution of core functions
5	Dependencies	Identify dependencies between sub-sectors <> core functions <> resources
6	Vulnerabilities	Identify possible weak points in resources, core functions, or sub-sectors
Risk Analysis		
7	Scenarios	Create representative scenarios for the identified vulnerabilities for each sector
8	Risk Estimation	Evaluate qualitatively for each scenario the extent of damage and frequency of damage occurrence
9	Risk Matrix	Create survey of the relevant scenarios; structure according to magnitude and frequency
10	Measures	Create ideas for measures

Table 2: Swiss Roundtables

Steps 1–4 are presented in this section since they are the core elements of sector analysis. The four steps aim to 1) gain an overview of critical sectors, 2) identify sub-sectors for each sector on the basis of organizational criteria, 3) identify core functions of the sub-sectors, and 4) assess the resources necessary for the functioning of the sub-sectors.

First the ten sectors for which the risk analysis is to be conducted were defined:[26] On this basis, sub-sectors for each of the ten sectors will be identified

25 Pfister, Ivo. *Round Tables InfoSurance: Sektorspezifische Risikoanalyse. Einführung und Methodische Grundlagen* (Luzerner Tage für Informationssicherheit LUTIS, June 2003). www.infosurance.ch/lutis/vortraege/ methodische_grundlagen.pdf. InfoSurance Fokus (November 2002): http://www.infosurance.ch/de/pdf/fokus_2.pdf.

26 These ten sectors are: (Public) Administration, Civil Defense and Emergency Services, (Tele-) Communication, Energy, Finance, Industry/ Manufacturing, Media, Public Health, Transport (and Logistics), Water (see →Part I for more details).

according to organizational standpoints. This step will also help to identify the main stakeholders and key players for each sector and sub-sector. Core functions of the sub-sectors are understood as the most important services provided by the sub-sector. Hence, in the third step these core functions have to be identified. The following information has to be gathered for each core function:

- What is required in terms of availability of service or function?
- What processes are executed for the delivery of the core function?
- Who delivers the core process?
- Which internal and external resources are needed for the normal delivery of the core process?

The sub-sectors depend on certain resources to fulfill their core function. These resources are identified in the fourth step by using a pre-fixed checklist as guidance. The list contains the following categories (of resources):

- Hardware
- Applications
- Data and Information
- Structural Infrastructure
- Technical Infrastructure
- Persons

Figure 7 shows an example of a process and technology analysis for the telecommunication sector.

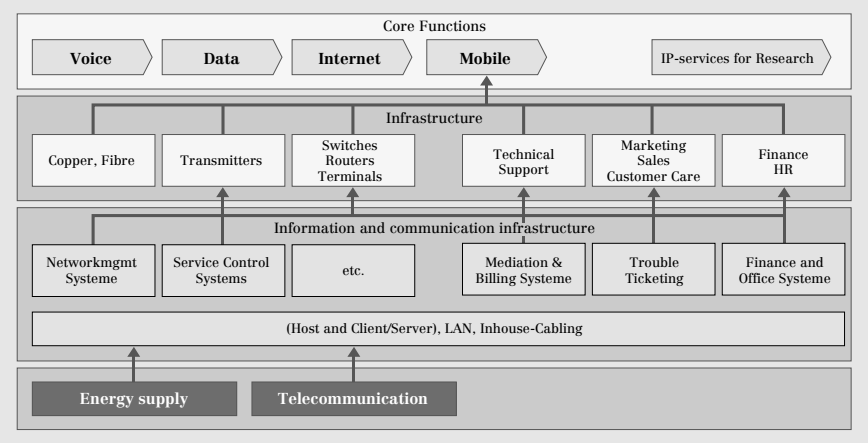


Figure 7: Core Functions, Infrastructure, and Components of the Swiss Telecommunication Sector

Example 7 (United States) – Department of Energy (DoE) Layer Models

The *Department of Energy* (DoE) uses →*Layer Models* to show interdependencies of the energy sector with other sectors and sector components (Figure 8):

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] This information can be used for the *Interdependent Energy Infrastructure Simulation System* (IEISS), which gives users a unified view of physical interdependencies.[28]

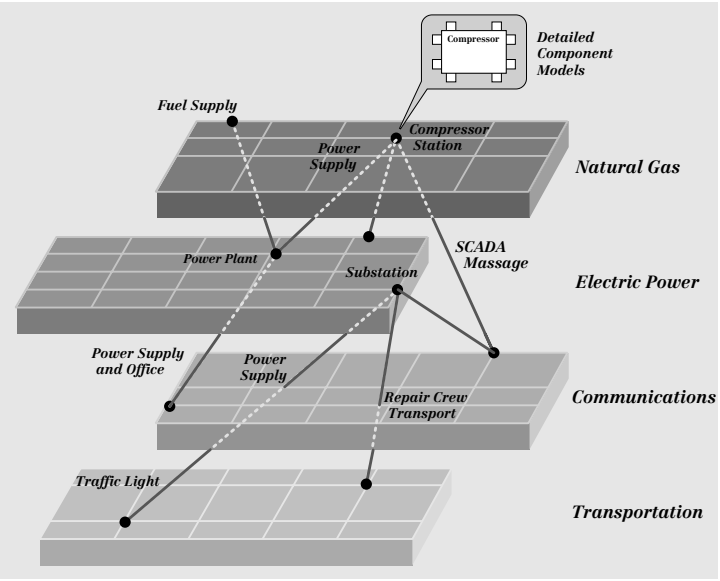


Figure 8: Interdependencies between Critical Infrastructures[29]

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

28 Varnado, Sam. "Modeling and Simulation for Critical Infrastructures – Status and Future Issues". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

29 Center for Strategic Leadership, US Army War College. *Issue Paper August 2003*, vol. 06–03. http://www.iwar.org.uk/cip/resources/csl-awc/nisac.pdf.

2 Interdependency Analysis

Critical infrastructures are frequently connected at multiple points through a wide variety of mechanisms, so that bi-directional relationships exist between the states of any given pair of infrastructures. This means that CI are highly interdependent, both physically and in their greater reliance on the information infrastructure, resulting in a dramatic increase of the overall complexity and posing significant challenges to the modeling, prediction, simulation, and analysis of CI. The information infrastructure plays a crucial role, as most of the critical infrastructures are either built upon or monitored and controlled by ICT systems, a trend that has been accelerating in recent years with the explosive growth of information technology.

An →*Interdependency* can be understood as a "bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other."[30] A →*Dependency*, on the other hand, is a unidirectional relationship.[31]

What is Interdependency Analysis?

Due to the explosive growth of information technology, the study of interdependencies and possible cascading effects in case of failures have become the focal point of research. Interdependency analysis looks to gain a better understanding of the complex (bi-) directional relationships between infrastructure components, subsystems, systems, and/or sectors.

At an initial stage, most countries have opted for qualitative, expert-based approaches to mapping interdependencies. Most countries have included in their approaches a rough analysis of dependencies and interdependencies to determine the criticality of infrastructures or sectors. Expert opinion is collected through means of working groups, →*Roundtables*, workshops, or →*Questionnaires*. However, it is generally recognized today that it is necessary to move beyond mere qualitative understanding of interdependencies and towards sophisticated modeling of cause-and-effect relationships and possible cascading failures.

A comprehensive analysis of interdependencies is a daunting challenge, though, mainly because the science of infrastructure interdependencies is relatively immature. There are many models and computer simulations

30 Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". *IEEE Control Systems Magazine* vol. 21 (6 December 2001), p. 14.

31 Ibid.

for aspects of individual infrastructures, but simulation frameworks that allow the coupling of multiple interdependent infrastructures to address infrastructure protection, mitigation, response, and recovery issues are only beginning to emerge. The operational, R&D, and policy communities have accepted the importance of infrastructure interdependencies and the need to better understand their influence on infrastructure operations and behavior. Increasingly, the complex →*Agent-Based Modeling* is used to gain a better understanding of interdependencies. These efforts are partly described in chapter on →*System Analysis*. This chapter will concentrate on the more qualitative, descriptive efforts.

How to Categorize Interdependencies in Terms of their Environment

Interdependencies are a complex and difficult problem to analyze, also because the nature of interdependencies is still very little understood. An article published by a group of US scholars (Rinadli, Peerenboom, Kelly: "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies")[32] presents a conceptual framework for

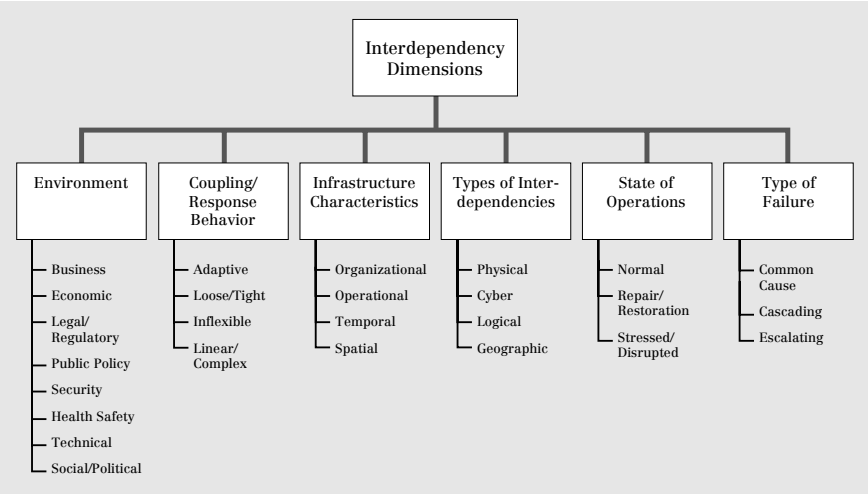


Figure 9: Interdependency Dimensions

32 Ibid. pp. 11–25.

addressing infrastructure interdependencies that is important enough to merit mention, even though it is not a country-specific approach as such. The article addresses interrelated factors and system conditions, which are represented and described in terms of six "dimensions" that complicate the challenge of identifying, understanding, and analyzing interdependencies (Figure 9):

The six dimensions that can be distinguished are:

- Environment: The environment influences normal system operations, emergency operations during disruptions and periods of high stress, and repair and recovery operations. Examples for parameters related to the environment are: Economic and business opportunities and concerns, public policy, government investment decisions, legal and regulatory concerns, and social and political concerns.
- Coupling/Response Behavior: 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.
- Infrastructure Characteristics: Infrastructures have key characteristics that figure in interdependency analyses. Principal characteristics include spatial (geographic) scales, temporal scales, operational factors, and organizational characteristics.
- Types of Interdependencies: These linkages can be physical, virtual, related to geographic location, or logical in nature.
- State of Operation: The state of operation of an infrastructure can be thought of as a continuum that exhibits different kinds of behavior during normal operating conditions (which can vary from peak to off-peak conditions), during times of severe stress or disruption, or during times when repair and restoration activities are underway. At any point in the continuum, the state of operation is a function of the interrelated factors and system conditions.
- Type of Failure: Infrastructure disruptions or outages can be classified as cascading, escalating, or common-cause failures.[33]

Even though the listed dimensions are very broad, the approach is a first step towards a comprehensive set of interdependency metrics. In a way, it is a holistic approach incorporating technical as well as socio-political issues.

33 Ibid.

Examples of Interdependency Analyses

Very often, the determination of interdependencies is closely related to the identification of vital processes and core components within sectors. During this procedure, dependencies of core infrastructure components that could lead to cascading effects of failure can be determined, with a special focus on ICT components due to their special role when it comes to interlinking other infrastructures. The identification of nodes and linkages between sectors helps to establish the degree of interdependency: Interdependencies can exist between components, but also between functions or resources; they can have different characteristics (i.e. physical, virtual, related to geographic location, or logical in nature) and may differ in degree. Other important factors to be considered include the impact of the effect caused by the dependency, time lags, redundancy, etc.

In the following, two examples are described more closely:

- Example 1 (Australia) – PreDict Interdependency Analysis (PreDict)
- Example 2 (Canada) – Critical Infrastructure Protection Task Force Dependency Analysis (CIPTF)

Example 1 (Australia) – PreDict Interdependency Analysis (PreDict)

♦ The PreDict approach is also described in *Chapter 1: Sector Analysis*, and in *Chapter 5: Vulnerability Assessment.*

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. In a first phase, the study identified vulnerabilities in fifteen infrastructure sectors and highlighted their interdependence (at the sector level). This was then used as a basis for the development of industry vulnerability profiles for each of the ten sectors (→see also Chapter 5 on *Vulnerability Assessment*).

Sector interdependencies were discussed and rated by experts (both industry and defense representatives). The interdependencies were charted over the three periods of 1999, 2005, and 2020, with additional summary pages detailing the nature of the interdependency and reasoning behind each rating. Initially identified sector interdependencies were classified as critical, significant, or moderate. The findings were shown in →*Interdependency Charts* (Figure 10), which were further commented in detail.

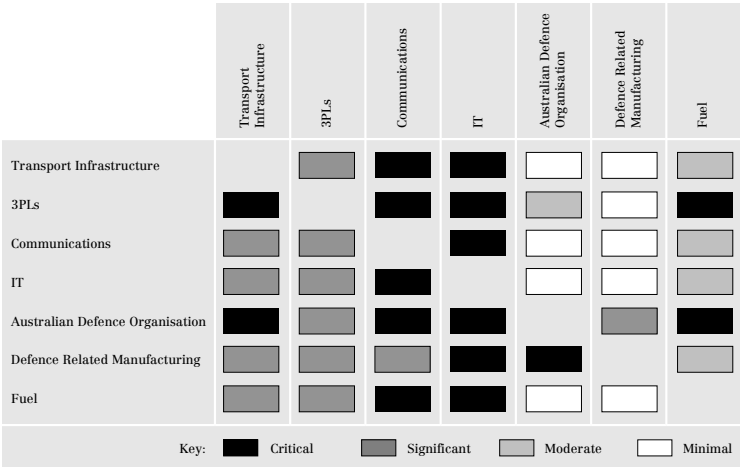


Figure 10: Section of an Interdependency Chart

Example 2 (Canada) – Critical Infrastructure Protection Task Force Dependency Analysis (CIPTF)

♦ The CIPTF approach is also discussed in *Chapter 1: Sector Analysis*, and in *Chapter 3: Risk Analysis*.

In spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive process to review critical infrastructures in Canada. One of the goals was to better understand and picture interdependencies. Based on six sectors identified as crucial (Government; Energy and Utilities; Services; Transportation; Safety; Communications), the CIPTF developed a multi-dimensional →*Layer Model* that takes into consideration the responsibilities at five levels, namely at the international, federal, provincial, municipal, and private levels. The CIPTF used this model to draw up a detailed dependency analysis, based on input from approximately sixty experts (Figure 11).[34]

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

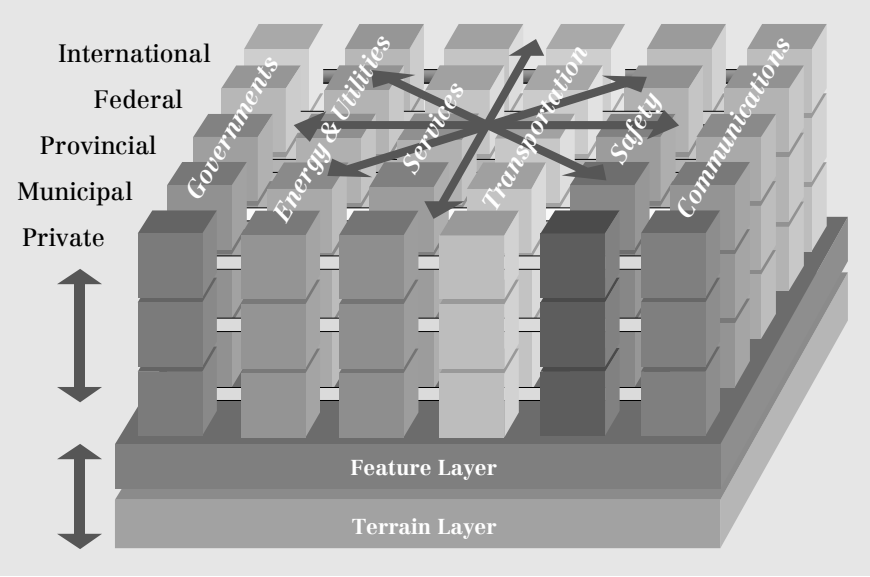


Figure 11: Canadian Critical Infrastructure Model: Dependencies

It became immediately obvious that the large number of interdependencies could not be plotted concisely this way. To better show and evaluate the level of interdependency between the different infrastructure elements, a →*Dependency Matrix* was developed (Figure 12). The extent of direct dependency between infrastructure elements is described using the →*Values* "high", "medium", "low", and "none".[35]

An application called *Relational Analysis For Linked Systems (RAFLS)* was developed for measuring and modeling the cascading effects of these direct dependencies. RAFLS, which is based on an algorithm, uses scored interdependencies and iteratively determines dependencies and impacts. It shows high and medium degrees of dependencies and can reveal second-, third-, fourth-, and fifth-level dependencies. It also helps to trace linkages and potentially interdict a path in time of crisis.[36]

35 Ibid.
36 Ibid.

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 12: Section of the Indefinite Matrix

3 Risk Analysis

One standard definition of →*Risk* is that 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.[37] *Risk analysis* refers to the processes used to evaluate those probabilities and consequences, and also to the study of how to incorporate the resulting estimates into decision-making processes. 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 existing risks.[38] Outcomes of the risk assessment process are used to provide guidance on the areas of highest risk, and to devise policies and plans to ensure that systems are appropriately protected.[39]

What is Risk Analysis?

The modern techniques of the research discipline of risk analysis originate in the engineering professions and may be traced back at least to the beginnings of the US space program. They have been developed most vigorously in the nuclear power industry.[40] However, independent developments have also taken place in various other fields.

In the context of CIP/CIIP, risk analysis could theoretically address any degree of complexity or size of system. However, when the boundaries of the evaluated system are set too wide, the lack of available data makes accurate assessment difficult or even impossible. The three most important single steps of the risk analysis process (namely threat, vulnerability, and impact analysis) are discussed in more detail in separate chapters.

37 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: U.S. Government Printing Office, January 2002), p. 8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

38 Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3*, *Risk Management* (draft version). http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3p.pdf. The Australian government is currently developing a new manual: http://www.dsd.gov.au/library/acsi33/acsi33.html.

39 Commonwealth of Australia, *ACSI 33*, *Handbook 3*, *Risk Management.*

40 In the nuclear power industry, these techniques are subsumed under the rubric of *Probabilistic Risk Assessment* (PRA).

Risk analysis is an approach that is widely used in different communities. The risk estimate is produced mainly from the combination of threat and vulnerability assessments. It analyzes the probability of destruction or incapacitation resulting from a threat's exploitation of the vulnerabilities in a critical infrastructure. In the least, risk analysis encompasses risk identification, risk quantification, and risk measurement, according to the three classic questions:

a) What can go wrong?
b) What is the likelihood of it going wrong?
c) What consequences would arise?[41]

Often, this is followed by risk evaluation, risk acceptance and avoidance, and risk management, according to the following questions:

a) What can be done?
b) What options are available, and what are their associated trade-offs in terms of cost, benefits, and risks?
c) What impact do current management decisions have on future options?[42]

Even though risk analysis is extremely well established and used in different communities, it has many shortcomings. These include especially the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decision-making processes. There are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events – and this is what we are dealing with in the context of CIIP.

There are many approaches that focus on information security for IT systems. Predominantly, this category covers locally applied measures with a localized focus within a business, agency, or organizational context. These approaches are based on the supposition that sufficient protection at the technical system level nullifies threats to the larger system of CI.

Systems-based approaches often include standard security safeguards, implementation advice, and aids for numerous IT configurations typically found in IT systems today. →*Information Security Guidelines* are suggestions or recommendations on how to address an area of →*Information Security Policy*. Technical protection manuals recommend security measures for selected IT systems.[43] The aim of these recommendations is to achieve a reason-

41 Haimes, Yacov Y. *Risk Modeling, Assessment, and Management* (New York, 1998).
42 Ibid., pp. 54–55.
43 Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards* (updated July 2001). http://www.bsi.de/gshb/english/menue.htm.

able security level for IT systems that is adequate to protection requirements ranging from normal to high degrees 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*.[44] Most of them are business-oriented and centered on organizational information systems, which precludes them from being directly applicable to larger systems.

Steps Included in an IT Risk Analysis

Risk assessment methodologies are step-by-step approaches. The number of steps may vary and can also be adjusted to the specific needs. As mentioned, the classic definition of 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.

In order to identify all the elements necessary under this definition, no less than five steps must be undertaken. Figure 13 shows a possible nine-step risk analysis approach for IT systems.[45] It is easy to do a risk analysis for a small, restricted system – but much harder or even impossible for larger, more complex systems such as an entire CI.

The nine steps are described in the following sections.

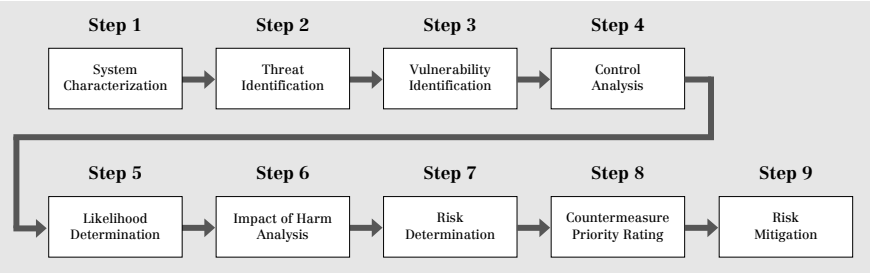


Figure 13: Possible Steps in Risk Assessment Methodology

44 Stoneburner, Goguen, Feringa, *Risk Management Guide for Information Technology Systems*.

45 It is a combination of the US approach as described in: Stoneburner, Goguen, Feringa, Risk Management Guide for Information Technology Systems, and the approach favored by Standards Australia / Standards New Zealand. Risk Management AS/NZS 4360:1999 (Strathfield, 12 April 1999).

Step 1: System Characterization

Step 1 is defining the scope of the effort and the boundaries of the system assessed. This includes the identification of all kinds of resources, assets, and information that constitute the system. An "asset" can be a tangible item (such as hardware), a grade or level of service, staff, or information. The strategic, organizational, and risk management context in which the rest of the process will take place are also established in this first step. Furthermore, criteria against which risk will be evaluated should be established, and the structure of the analysis has to be defined.[46]

Step 2: Threat Identification

Step 2 includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence. Threat probability is a measure of the likelihood of the threat being realized. Quantitative information on the nature and source of external threats can be derived from police reports, computer security surveys and bulletins, reports of an audit analysis, or actuarial studies. Information on internal threats can be estimated using previous experience and data, generic statistical information, or a combination of both. However, when dealing with actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable and thus poses significant problems for a traditional risk analysis aproach[47] (→see also Chapter 4 on *Threat Assessment*).

Step 3: Vulnerability Identification

Step 3 is about the development of a list of system vulnerabilities that could be exploited by the potential threat-sources. Recommended methods for the identification of system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist. There are several sophisticated approaches to a separate vulnerability assessment process (→see also Chapter 5 on

46 Emergency Management Australia. *Critical Infrastructure Emergency Risk Management and Assurance Handbook* (Mt. Macedon, 2003). http://www.disaster.qld.gov.au/publications/pdf/Critical_Infrastructure_handbook.pdf.

47 Zimmermann, Doron. *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception*, *Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung no. 67* (Zurich, 2003), p. 61, http://www.isn.ethz.ch/crn/extended/docs/ZB67.pdf and Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.), Stockholm International Peace Research Institute (SIPRI), *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford, forthcoming 2004).

Vulnerability Assessment). Again, assessing the vulnerabilities of a relatively restricted IT system such as a business network is far easier than doing the same at a higher system level. It is quite possible that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems, mainly due to already overwhelming system complexity.

Step 4: Control Analysis

In step 4, an organization would analyze planned or implemented controls, in order to minimize or eliminate the likelihood (or probability) of a threat exploiting any existing system vulnerability. Security controls encompass the use of technical and non-technical methods: Technical controls are safeguards incorporated into computer hardware, software, or firmware. Non-technical controls include management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

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 4). The likelihood that a potential vulnerability could be exploited by a given threat source can be described in terms of different →*Categories* (e.g. high, medium, low). Furthermore, there are several techniques to estimate probabilities in risk analysis.[48]

Step 6: Impact or Harm Analysis

In step 6 of the exemplified risk analysis approach, the adverse impact resulting from a successful threat exploitation of a vulnerability is determined. The impact of possible harm to an asset is best determined by a business executive, an asset owner, or an asset manager. The impact strongly reflects the actual value of the asset. The adverse impact of a security event in an IT system can be described in terms of loss or degradation of any, or a combination of, the →*IT-Security Objectives* (other categories might be applied if risk analysis is conducted for more abstract systems). Some tangible impacts can be measured in a quantitative manner in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused

48 Such as statistical inference, scenario technique, fault trees, and event trees; see also Stromquist, Walter R. *Uses and Limitations of Risk Analysis*. Prepared for the Royal Commission on the Ocean Ranger Marine Disaster Risk Analysis Seminar, 1 May 1984. http://www.chesco.com/~marys/ORanger.htm.

by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units, but can at least be qualified or described in terms of high, medium, and low impacts (→see also Chapter 6 on *Impact Assessment*).

Step 7: Risk Determination

The purpose of step 7 is to assess the level of risk to the (IT) 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). A →*Risk Scale* and a →*Risk Level Matrix* are appropriate tools for measuring the resultant risk.

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). It is used to provide guidance as to the importance that should be placed on security countermeasures. Again, applied values and categories may vary widely. Table 3 is an example of a *Risk Assessment Table*, which helps to calculate the level of the Countermeasure Priority Rating (column 7). Column 7 is simply the difference between the resultant risk and the required risk (Columns 6 and 5 in the example) expressed as a figure.

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
Row 1: Reliability of e-commerce-related web-site	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[49]

49 Commonwealth of Australia, *ACSI 33. Handbook 3, Risk Management.* Appendix, http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3Ap.pdf.

Step 9: Risk Mitigation

Step 9 is about risk mitigation and involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls suggested by the risk assessment process. Because the elimination of all risk is usually impractical or near impossible in reality, it is the stakeholders itself that must use the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level.[50]

Control actions occur frequently in IT systems. Different kinds of security controls can be applied at the technical, management, and operational levels, or a combination of such controls, with the goal of maximizing the effectiveness of controls for IT systems and organizations.

- *Technical security controls* for risk mitigation can be configured to protect against given types of threats. These security controls may range from simple to complex measures. They usually involve system architectures; engineering disciplines; and security packages with a mix of hardware, software, and firmware. Technical security controls can be grouped into three categories, according to primary purpose: supporting, preventing, and detecting and recovering.
- *Management security controls*, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards.
- *Operational controls*, implemented in accordance with a base set of requirements (e.g., technical controls) and good industry practices, are used to correct operational deficiencies that could be exploited by potential threat sources.

Examples of Risk Analysis Processes for CI/CII

Below, the following eight examples are described:

- Example 1 (Australia and New Zealand) – Risk Management Standard (NSW)
- Example 2 (Canada) – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)
- Example 3 (European Union) – The CORAS Project (CORAS)
- Example 4 (France) – EBIOS Method (EBIOS)

50 Stoneburner, Goguen, Feringa. *Risk Management Guide for Information Technology Systems.*

- Example 5 (Norway) – Protection of Society Project (BAS)
- Example 6 (Switzerland) – Swiss Roundtables Risk Analysis Methodology (Roundtables)
- Example 7 (United Kingdom) – NISCC Building Blocks (NISCC)
- Example 8 (United States) – OCTAVE Methodology (OCTAVE)

Example 1 (Australia and New Zealand) – Risk Management Standard (NSW)

The *Australian and New Zealand Standard for Risk Management* (AS/NZS 4360:1999) is the standard by which all critical infrastructures are assessed to assist with the review of risk management plans for prevention (including security), preparedness, response, and recovery.[51] The AS/NZS 4360:1999 standard provides a generic guide for the establishment and implementation of the risk management process involving identification, analysis, evaluation, treatment, and ongoing monitoring of risks. In accordance with AS/NZS 4360, it is necessary to establish the strategic context. In the current security environment, security risk assessments should also consider terrorism in all its forms.[52]

The Australian *Defense Signal Directorate* (DSD) has also released a new version of the *ACSI33 Government IT Security Manual* in an attempt to consolidate and restructure a number of existing Australian IT security policy documents into a single, cohesive manual.[53] The *New South Wales Office of Information and Communications Technology*'s (OICT) website additionally features a long list of guidelines for information management and information security:[54] The *Information Security Guidelines Part 1* is concerned with risk management.[55] Its objective is to assist government agencies in the identification and management of information security risks.

51 Yates, Athol. *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment* (Institution of Engineers, Australia, June 2003). http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf.

52 Ibid., pp. 10, 27, 30, 65.

53 Draft ACSI 33 Information, Government IT Security Manual. http://www.dsd.gov.au/library/acsi33/acsi33_draft_information.html.

54 http://www.oit.nsw.gov.au/pages/4.3.Guidelines.htm.

55 New South Wales Office of Information and Communications Technology's (OICT). *Information Security Guideline for NSW Government Part 1 – Information Security Risk Management*. No. 3.2, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.16-Security-Pt1.htm.

Its components are: assets, asset values, threats, vulnerabilities, security risk, security requirements, and security controls (Figure 14).

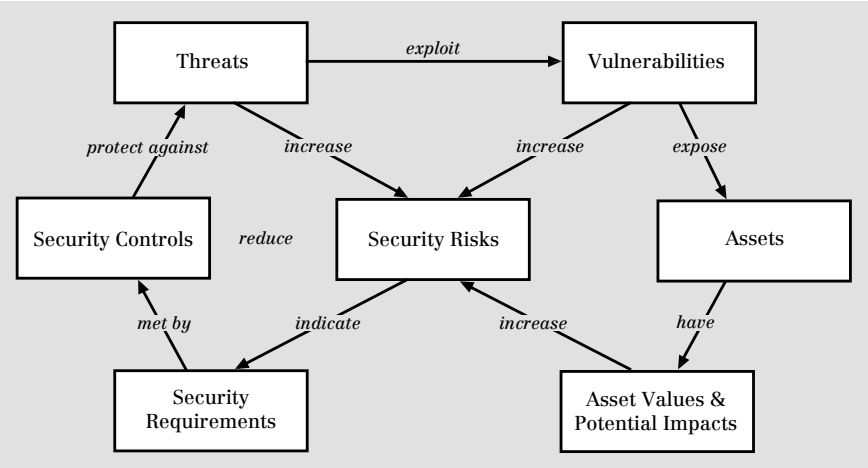


Figure 14: Risk Concept Relationship

This guideline is based on the *Australian/New Zealand Handbook on Information Security Risk Management* (HB 231:2000). It should also be read in conjunction with the *Information Security Guidelines Part 2 – Examples of Threats and Vulnerabilities*[56] and the *Information Security Guidelines Part 3 – Information Security Baseline Controls*.[57]

56 New South Wales Office of Information and Communications Technology (OICT). *Information Security Guideline for NSW Government Part 2 – Examples of Threats and Vulnerabilities*. No. 2.0., first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.17-Security-Pt2.htm.

57 New South Wales Office of Information and Communications Technology (OICT). *Information Security Guideline for NSW Government Part 3 – Information Security Baseline Controls*. No. 3.0, first published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.18-Security-Pt3.htm.

Example 2 (Canada) – Infrastructure Protection Process by the Critical Infrastructure Protection Task Force (CIPTF)

♦ The CIPTF approach also appears in *Chapter 1: Sector Analysis*, and in *Chapter 2: Interdependency Analysis.*

In the spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive review process for critical infrastructures in Canada. One of the goals was to better understand risks (Figure 15).[58]

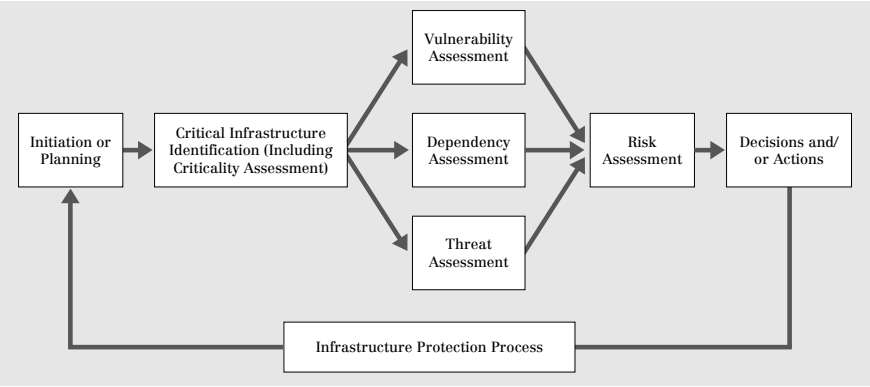


Figure 15: Canadian Infrastructure Protection Process

Risks were determined by using 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 element, between layers in the infrastructure model, and between infrastructure elements, which are called specific risks.

It was taken into account that risks accumulate when the risks of dependencies are propagated (→*Cascading Effect*). Therefore, the Canadian process conducts a →*Cumulative Risk Assessment* through dependencies. The assessment of impacts can be done with a →*Risk/Impact Scattergram*.[59]

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

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

Example 3 (European Union) – The CORAS Project (CORAS)

The EU-funded *CORAS*[60] project (IST-2000-25031) developed a tool-supported methodology for model-based risk analysis of security-critical systems. The project was initiated in January 2001 and completed in September 2003. The CORAS framework consists of terminology, languages for system modeling, processes for system development and risk management, and methodologies for security risk analysis as well as computerized tools.

The CORAS methodology for model-based risk assessment (MBRA) applies a standardized modeling technique to form input models to risk analysis methods that are used in a risk management process. This process is based on the *AS/NZS 4360:1999 Risk Management* standard.

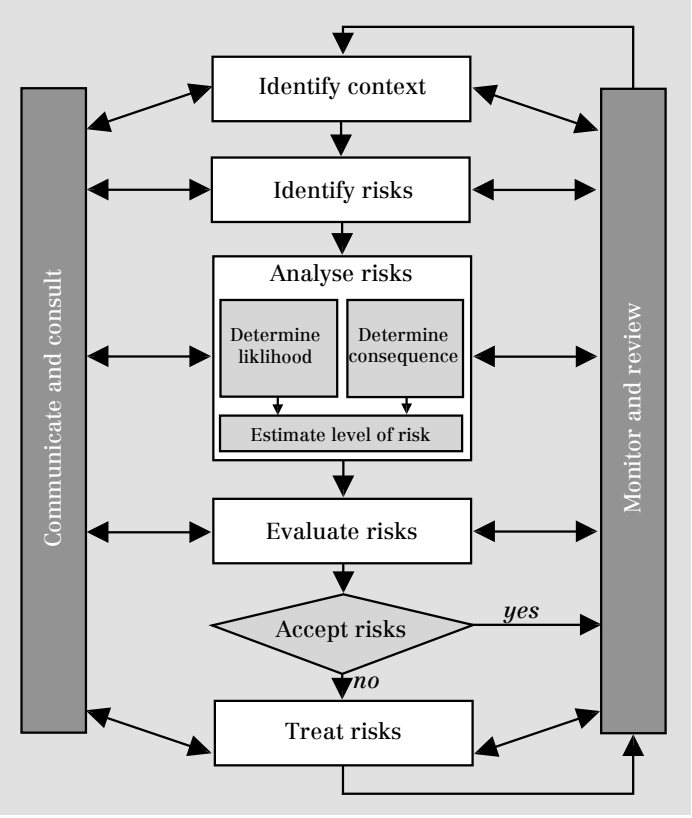


Figure 16: The CORAS Risk Management Proces

60 http://coras.sourceforge.net/

Figure 16 indicates that the AS/NZS 4360 standard provides a sequencing of the risk management process into sub-processes for context identification, risk identification, risk assessment, risk evaluation, and risk treatment. In addition, there are two implicit sub-processes targeting "communication and consultation" as well as "monitoring and review" running in parallel with the first five steps.[61]

Example 4 (France) – EBIOS Method (EBIOS)

The methodological approach EBIOS (*l'Expression des Besoins et l'Identification des Objectifs de Sécurité*) belongs to a group of methodological guides published by the *Service Central de la Sécurité des Systèmes d'Information* (SCSSI). This methodology is used in the information system-planning phase. The main goal is to allow any organization – especially the state administration – to define necessary security actions.

In addition, several other methodologies are used for design, development, and implementation, as well as the operation and maintenance of information systems (see Figure 17). The outcome of an EBIOS study provides information needed to establish the security objectives for the system and is generally useful in developing the secured functional architecture:

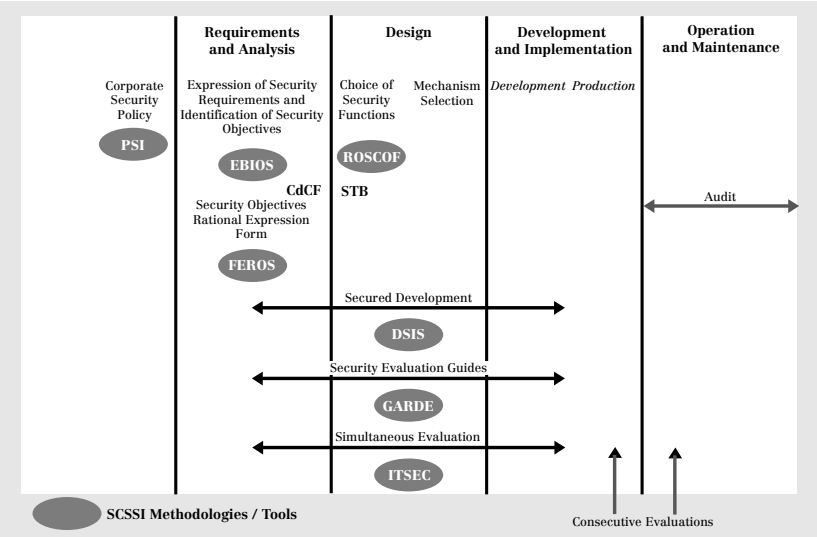


Figure 17: Security Activities during the system development life cycle (SDLC).

61 Gran, Bjørn Axel. *The CORAS Methodology for Model-Based Risk Assessment*, version 1.0, WP2, Deliverable 2.4. (29 August 2003).

The EBIOS method takes into account all technical (software, hardware, networks) and non-technical entities (organization, human aspects, physical security). It also involves all players concerned with information systems security problems. It further proposes a dynamic procedure favoring interactions between different businesses and departments of the organization. With the help of the EBIOS method, the entire life cycle of a system can be studied (design, production, implementation, maintenance, etc.).[62]

There are four principles of the EBIOS method (Figure 18):

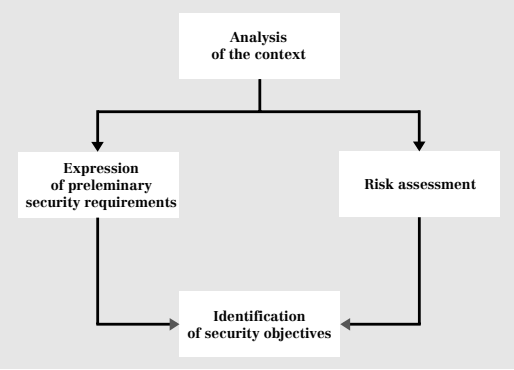


Figure 18: EBIOS Method Diagram

1) *The context study*: An information system is based on elements, functions, and information, which make up the added value of the information system for the organization. These elements are related to a set of different types of entities: hardware, software, networks, organizations, personnel, and sites.

2) *The expression of security needs*: Each element has a specific security need if the business is to operate correctly. This security need is expressed according to different security criteria such as availability, integrity, and confidentiality. If this need is not met, there will be an impact on the organization. This impact may come in different forms such as financial losses, disruptions of the smooth progress of activities, damage to the brand image, influence on personnel safety, pollution, failure to comply with laws and regulations, etc.
3) *The threat study*: In general, an organization is exposed to various potential threats from its environment. A threat may be characterized according to its type (natural, human or environmental), its cause (accidental or deliberate), and its influence on security criteria (availability, integrity, confidentiality, etc.). For an accidental cause, a certain kind of threat can also be described in terms of

62 Methods to Achieve Information Systems Security. Expression of Needs and Identification of Security Objectives (EBIOS). Memo – Version 1.4. http://www.ssi.gouv.fr/en/confidence/documents/memo-gb.html.

its exposure and the available resources. For a deliberate cause, a threat can also be characterized by expertise, available resources, and motivation.

4) Expression of security objectives: All that remains is to determine how elements can be affected by threats.[63]

Example 5 (Norway) – The Protection of Society Project (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).[64] 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 was conducted in four interlinked steps (Figure 19):

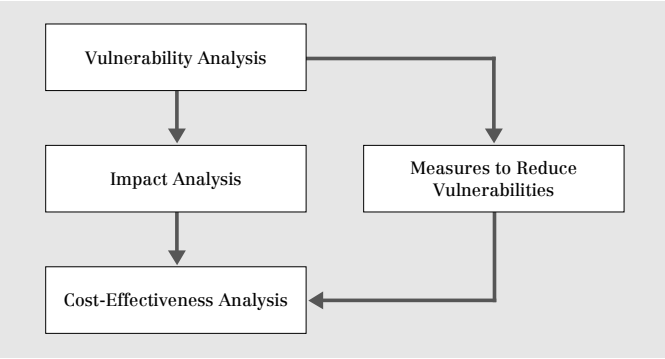


Figure 19: Steps of the Norwegian Vulnerability Analysis

63 EBIOS website: http://www.ssi.gouv.fr/en/confidence/methods.html. Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical guide – English version, Version 1.02., February 1997.

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

In a first step, a →*Vulnerability Analysis* was conducted. By using →*Seminar Games*, BAS2 mapped the dependency of modern society upon telecommunication services in crisis and conflict situations. After this, an impact analysis was conducted. In a next step, measures that might reduce the vulnerabilities were evaluated. Eventually, the actual cost-effectiveness analysis was undertaken.

Because no single method was able to handle all the problems, BAS2 had to use a combination of several techniques and methods to calculate the most cost-effective protection strategy for the telecommunication system. The additional approaches used were seminar games; use of →*Scenarios*, →*Causal Mapping*, →*Fault Tree Analysis*, Probabilistic Cost Estimation, and a →*Multi-Criteria Model*. The →*Multi-Criteria Decision Approach* systematically maps out subjective expert evaluations and combines them into a quantitative measure of effectiveness.

The →*Multi-Criteria Decision 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 top-level goal is the overall objective of the system of analysis. In this process, the complex dynamic system to be analyzed is represented by a simplified linear, easily understandable model. Lower-level technical criteria are aggregated to wider, more general criteria in a rigid linear model. The relationships between criteria at different levels can be quantified by experts expressing their subjective preferences of criteria, i.e. identifying the criteria they consider to be important for the success of the criterion on the level above. In other words, the experts *weigh* the different criteria in the model against each other, and the experts' preferences serve as a measure of the *effectiveness* of one criterion compared to the others on the same level. The top goal of the hierarchy expresses the total effectiveness of the measures involved.

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, so that the top criteria in the technical sub-system are identical to the bottom criteria in the societal sub-system (Figure 20).

Maximizing the protection of society was defined as the top goal. The top goal was further distilled into three sub-criteria, which were: minimizing loss of life, minimizing economic losses, and minimizing the danger of a loss of sovereignty. These three sub-criteria were divided into more specialized sub-criteria (Figure 21).

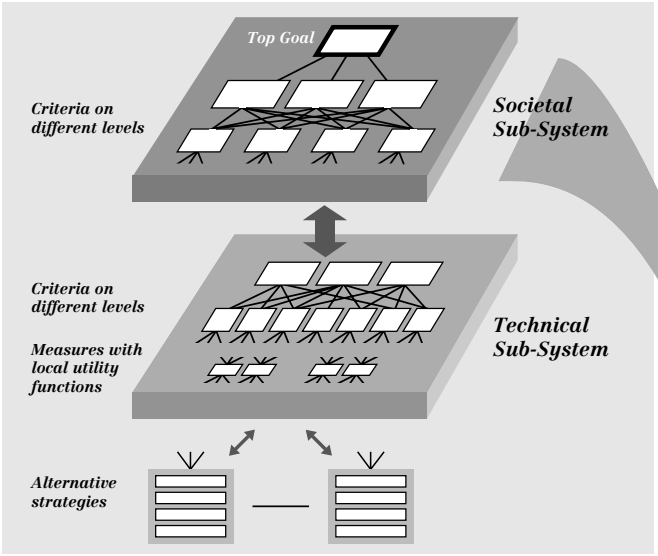


Figure 20: Multi-Criteria Hierarchy

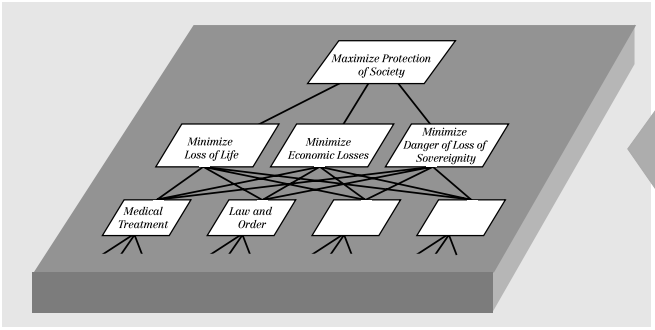


Figure 21: Parts of the Social Hierarchy for the Multi-Criteria Analysis

Creating a →*Multi-Criteria Model* is an iterative process. One of the main problems in the design process was to determine, to the greatest extent possible, exclusive criteria that were independent of the other criteria on the same level in the hierarchy. Still, the design process was extremely useful for establishing a thorough understanding of the problems that were analyzed.[65]

65 Hagen, J. and H. Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*, p. 13.

Example 6 (Switzerland) – Swiss Roundtables Risk Analysis Methodology (Roundtables)

♦ The Sector Roundtable approach also appears in *Chapter 1: Sector Analysis*

Under the auspices of the *Swiss InfoSurance Foundation*, sector specific risk analysis round tables are conducted for ten sectors identified as critical. The methodology used for each of the sectors is a ten-step risk analysis approach as shown in Figure 22:

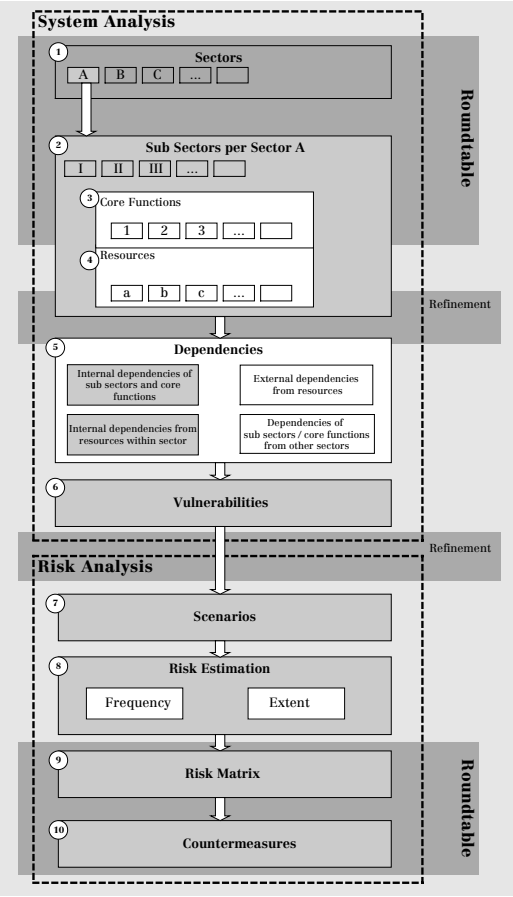


Figure 22: Swiss Critical Sector Risk Analysis Approach

Four →*Roundtables* that can be amended by working groups are planned for each sector. The processes can be divided into a system analysis and a risk analysis:

- The system analysis aims to gain an overview over structures, elements, and the dependencies in the respective sector (Steps 1–6).
- The risk analysis uses scenarios for identified weak points and focuses on them (Steps 7–10).[66]

66 InfoSurance, Wirtschaftliche Landesversorgung, Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen: Methodischer Leitfaden* (no date, no place).

Example 7 (United Kingdom) – NISCC Building Blocks (NISCC)

The UK government's CIIP center, the NISCC (*National Infrastructure Security Coordination Centre*), has developed a set of "building blocks" in order to provide protective security advice efficiently. It is an ongoing process already initiated in the UK. The building blocks are described by asking a series of key questions:

- What is critical to the UK?
- Are some sectors more critical than others?
- What would be the impact of disruption?
- What is potentially vulnerable to electronic attack?

Answers to these questions help to generate a prioritized set of services or mechanisms for the supply of goods, services or resources that are critical to the well-being of the UK and are potentially vulnerable to electronic attack. Subsequently, the following questions are asked:

- Which organizations are responsible for providing these services?
- What proportion of the service is each organization responsible for?

This generates a prioritized set of private companies, government departments, agencies, and other organizations that may be considered as part of the critical infrastructure. These organizations, agencies, and companies are asked to participate in a confidential dialog. In the context of the dialog, the following questions are asked:

- What systems, networks, components, and assets are critical for the continued provision of a critical service by each organization?
- What other services and systems do they depend on?
- Are these systems vulnerable to electronic attack?
- What would be the impact of a successful electronic attack?
- What procedural and technical measures has the organization prepared to protect its systems?

The information gained from these questions gives the NISCC a detailed insight into the protective measures and consequences of failure of these organizations and companies. In order to provide the interview partners with advice, recommendations, and information sharing opportunities, the NISCC assesses the following three points:

- What is the threat?
- How can the respective company improve its resilience?
- How can the sector improve its resilience?

Answers to these building block questions generate a 'map' of CII (networks and services), key organizations, and interdependencies. The information allows the NISCC to give the organizations feedback, including a set of

recommendations to improve safety and security; vulnerability analyses on components or networks used by the organization; and a threat assessment based on intelligence and investigatory findings. These inputs allow the organization to manage more effectively their risk management for electronic attack protection.[67]

Example 8 (United States) – OCTAVE Methodology (OCTAVE)

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)[68] is an approach to self-directed information security risk evaluations, developed by the US CERT Coordination Center at the Carnegie Mellon Software Engineering Institute[69]. The OCTAVE Method is documented in the 18-volume *OCTAVE Method Implementation Guide* (OMIG).[70] The OCTAVE Method is based on a set of criteria that define the essential elements of an asset-driven, comprehensive, self-directed security risk evaluation for organizations. Since OCTAVE was designed for a target audience of larger organizations, a version called OCTAVE-S has been developed recently for small organizations.[71]

The OCTAVE Method uses a three-phase approach to examine organizational and technology issues, assembling a comprehensive picture of the organization's information security needs (see Figure 23). The method consists of workshops that encourage open discussion and the exchange of information about assets, security practices, and strategies. Each of the three phases consists of several processes. Furthermore, one or more workshops are planned for each process. The three phases of the OCTAVE Method are briefly outlined below.

67 Barry, Ted. "Critical Information Infrastructure Protection in the United Kingdom". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29–30 September 2003).

68 http://www.cert.org/octave/.

69 http://www.cert.org.

70 Alberts, Christopher and Audrey Dorofee. *OCTAVE Method Implementation Guide*, version 2.0, vols. 1–18 (Carnegie Mellon University, June 2001). http://www.cert.org/octave/pubs.html. See also: Alberts, Christopher and Audrey Dorofee. *An Introduction to the OCTAVE Method*. http://www.cert.org/octave/methodintro.html.

71 Alberts, Christopher, Audrey Dorofee, James Stevens, and Carol Woody. *Introduction to the OCTAVE Approach* (Carnegie Mellon University, August 2003). http://www.cert.org/octave/approach_intro.pdf.

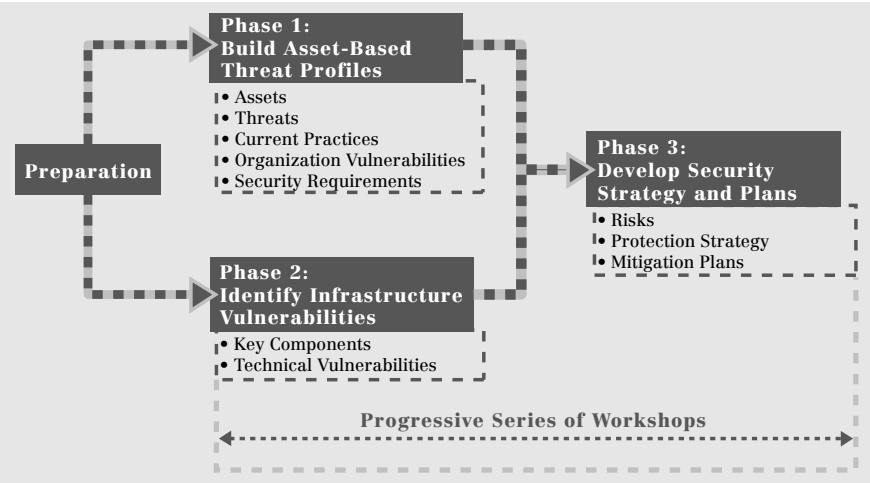


Figure 23: Three Steps of the OCTAVE Method

- *Phase 1: Build Asset-Based Threat Profiles*: This is an organizational evaluation. The analysis team determines which assets are most important to the organization (critical assets). The team identifies currently required actions to protect the determined assets;
- *Phase 2: Identify Infrastructure Vulnerabilities:* This is an evaluation of the information infrastructure. The analysis team examines key operational components in terms of weaknesses (technology vulnerabilities) that could lead to unauthorized actions against critical assets;
- *Phase 3: Develop Security Strategy and Plans:* During this phase of the evaluation, the analysis team identifies risks to the organization's critical assets. The team eventually decides on measures for managing the identified risks.

4 Threat Assessment

As critical infrastructures deliver a range of services that individuals, and society as a whole, depend on, critical infrastructures are a favored target for malicious attacks. Any damage to or interruption of critical infrastructures causes ripples across the technical and the societal systems – this principle held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure, therefore, has a "force multiplier" effect, allowing even a relatively small attack to achieve a much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors.[72]

The US Presidential Commission on Critical Infrastructure Protection (PCCIP), for example, defines "threat" as a "foreign or domestic entity possessing both the capability to exploit a critical infrastructure's vulnerabilities and the malicious intent of debilitating defense or economic security. A threat may be an individual, an organization, or a nation."[73] In publications on security of IT systems, threats are seen as the potential for a particular threat-source to successfully exploit a particular vulnerability, which means that a threat-source does not present a risk when there is no vulnerability that can be exercised.[74] Threats do not necessarily need to originate from human sources, but can be natural, human, or environmental.

What is Threat Assessment?

On the side of the government, the ability to gauge threats to critical infrastructure has traditionally depended on the ability to evaluate the intent of an actor, coupled with the motivation and the capability to carry out the action. This was easier when dealing purely with securing the physical realm – the nature and magnitude of physical threats have evolved relatively slowly over time, allowing for the establishment of indicator and warning mechanisms

72 Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Threat Analysis* no. TA03-001, 12 March 2003. http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf, p. 34.

73 President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, October 1997), Appendix, B-3.

74 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, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 12.

– but it was different for the rapidly evolving and little-known cyber-threats.[75] However, with the advent of cyber-based threat actors, the "enemy" becomes a faceless and remote entity, a great unknown almost impossible to track, opposing security institutions and laws that are ill suited to counter or retaliate against such a threat, while the overall capability of such malicious actors to do harm is believed to be enhanced by inexpensive, ever more sophisticated, rapidly proliferating, easy to use tools in the cyber domain.

Threat assessment in the risk analysis sense includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, it should be kept in mind that terrorism is an actor-based threat that is intrinsically non-quantifiable.[76]

Examples of Threat Assessment Aspects

In the following sections three different aspects of threat assessment are described: a management methodology, a general description of the threat environment, and an IT risk analysis approach.

- Example 1 (Australia) – NSW Risk Management Methodology (NSW)
- Example 2 (Canada) – OCIPEP Paper on Threat Analysis (OCIPEP)
- Example 3 (United States) – NIST Risk Management Guide (NIST)

Example 1 (Australia) – NSW Risk Management Methodology (NSW)

The example of the NSW risk management methodology shows that looking at CIP/CIIP from the point of view of threat can substantially impact on the way the infrastructures are assessed: When the list of critical infrastructures was validated with all stakeholders – this was achieved in five managed sector-specific workshops that included all owner/operators and policy owners from the utilities, transport, emergency services, major hazards (chemical), and medical sectors – it became necessary to evolve beyond the conventional 'sector'-based focus. The threat assessment was based on an *Australian Security Intelligence Organisation (ASIO) Context Statement*

75 OCIPEP, *Threat Analysis*, p. 12.

76 Zimmermann, Doron. *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception*, ed. Andreas Wenger, *Züricher Beiträge zur Sicherheitspolitik und Konfliktforschung* no. 67 (Center for Security Studies, Zurich, 2003), p. 61.

concerned with terrorist threat.[77] During the workshop, participants became aware that terrorists might attack not a whole sector, but rather key elements of an infrastructure.

Hence, it became clear that the notion of an attack on an infrastructure or a sector as a whole is not particularly useful. Categorizing targets in terms of their inherent function (such as raw material supply, distribution node, or command and control center) was considered far more meaningful. The notion of a more manageable 'target category' evolved in this context. This approach also facilitated a far better understanding of the differences between the sectors in terms of their perceptions of 'consequence' and 'vulnerability'. For example, the time at which an outage has an adverse effect on the population and the environment varies dramatically from sector to sector. This had to be taken into account to ensure the accuracy of the final risk assessment.[78]

The *NSW Information Security Guideline Part 2* on threats and vulnerabilities provides examples of the threats posed to information assets. It also identifies the vulnerabilities to be considered in the process of risk assessment. The guideline addresses the following key areas:

- The general definition of threats and vulnerabilities in relation to information assets;
- Environmental threats resulting in the loss of availability of information, such as natural disasters, contamination, and power fluctuations;
- Accidental threats arising from human errors and omissions, including fire, communication failures, and technical difficulties;
- A threat, whether it comes from an internal or external source, has the potential to cause harm to information assets, in which it exploits vulnerabilities. Vulnerability can be a weakness in the physical environment, organization and management, procedures, personnel, operations, software and hardware, or communications equipment.[79]

77 http://www.asio.gov.au/.

78 Yates, Athol. *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment* (Institution of Engineers, Australia, June 2003). http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf, p. 65.

79 New South Wales Office of Information and Communications Technology's (OICT), *Information Security Guideline for NSW Government Part 2 – Examples of Threats and Vulnerabilities*, No. 2.0. First published in September 1997, current version: June 2003. http://www.oit.nsw.gov.au/pages/4.3.17-Security-Pt2.htm.

Example 2 (Canada) – OCIPEP Paper on Threat Analysis (OCIPEP)

A paper published by the Canadian *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) in March 2003 aims to provide a taxonomy of the threats seen as most likely to impact upon Canada's national critical infrastructure.[80] The report, which does not focus exclusively on the cyber-infrastructure, wants to provide owners and operators, emergency managers, and the government with baseline information regarding potential threats to the networks and systems.

The publication defines the threat environment by the interaction of the infrastructure elements and the threat agents (Table 4). The means of attack or incident can be both physical and cyber-based. The target can be virtual, such as the information or applications on a network, or physical, such as a telecommunications cable. In reality, it is becoming increasingly difficult to distinguish between purely physical and cyber components of the infrastructure:

		Means	
Target		*Physical-based*	*Cyber*-based
	Physical	-Bombing of hydro tower - Severing a telecommunications cable with a backhoe - Explosion at an oil refinery - Ice storm debilitating hydro towers	- Hacking into the SCADA system that controls municipal sewage and water - Geomagnetic storms affecting CI elements
	Virtual	- Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components.	- Hacking into a critical government network - Penetrating the SS7 telecommunications transmission controls

Table 4: The CI Threat Environment[81]

The publication distinguishes between natural, accidental (physical and cyber), and malicious threats (physical and cyber) against CI and CII. In the context of CIIP, the characteristics of malicious computer-based threats to CI/CII ("cyber-based means"), which make them both difficult to predict and detect, are especially interesting:

- The problem of actor identification is particularly difficult in a domain where maintaining anonymity is easy and where there are sometimes time lapses between the intruder action, the intrusion

80 Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), *Threat Analysis* no. TA03-001, 12 March 2003. http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

81 Ibid., p. 12.

itself, and the actual effects. In addition, the continuing proliferation of sophisticated computer technologies into the mainstream population makes assigning attribution increasingly difficult.
- The threat is not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world, and may be launched from multiple locations simultaneously. Investigations and backtracking through a web of false leads and unwittingly slaved systems can be time-consuming and resource-intensive.
- The threat environment is extremely fluid. The window of opportunity between the discovery of vulnerabilities and the elaboration and implementation of a new tool or technique to exploit the vulnerability is narrowing rapidly.
- Technologies for attacks are simple to use, inexpensive, and widely available. Computer intruder tools and techniques, for example, are widely available on computer bulletin boards and various websites, as are encryption and anonymity tools.
- The methods of attack have become increasingly automated and more sophisticated, resulting in more damage from a single attack.
- The methods and tools used for attacks are often similar or identical to technologies used to ensure network reliability.
- The cost required to develop a significant attack capability continues to decrease.

Example 3 (United States) – NIST Risk Management Guide (NIST)

The *Risk Management Guide for Information Technology Systems* of the National Institute of Standards and Technology (NIST) sees threat assessment as a step in the overall risk analysis process. The aim is to identify the potential →*Threat-Sources* and to compile a list of threats applicable to the IT system. A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The common threat-sources for the CII can be natural, human, or environmental:[82]

- *Natural Threats*: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- *Human Threats*: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry)

82 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, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 13.

or deliberate actions (network-based attacks, malicious software upload, unauthorized access to confidential information).

- *Environmental Threats*: Long-term power failure, pollution, chemicals, liquid leakage.

The *Risk Management Guide* states that it is important to consider all potential threat-sources that could cause harm to an IT system and its processing environment. Humans may be threat-sources through intentional acts (such

Human Threat-Sources	Motivations	Methods/Threat Actions
Hacker, cracker	Challenge, ego, rebellion	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g. cyber-stalking) Fraudulent act Information bribery Spoofing System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	Bomb/terrorism Information warfare System attack (e.g., distributed denial of service) System penetration System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	Assault on employee Blackmail Browsing of proprietary information Computer abuse Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g., virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

Table 5: Human Threats – Threat Source, Motivation, and Threat Actions[83]

83 Ibid., p. 14.

as deliberate attacks by malicious persons) or unintentional acts (such as negligence and errors). A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality, or (2) a benign, but nonetheless purposeful, attempt to circumvent system security.

Individuals with the motivation and the resources for carrying out an attack are potentially dangerous threat-sources. Table 5 shows an overview of common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack, as identified by the Risk Management Guide. This information is considered useful to organizations studying their human threat environments and customizing their human threat statements.

After the identification of the potential threat-sources an analysis of the possible motivation, resources, and capabilities should be undertaken in order to determine the likelihood of a threat exercising a specific vulnerability[84] (→see also Chapter 3 on *Risk Analysis*).

84 Ibid.

5 Vulnerability Assessment

Vulnerability can be defined as susceptibility to injury or attack. It can be defined in the context of CIP/CIIP as "a characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat".[85] Considering limited, technical subsystems, vulnerabilities may be seen as "flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy".[86]

What is Vulnerability Assessment?

Vulnerability assessment is often seen as a single step in the overall risk analysis methodology. It is about the systematic examination of critical infrastructure, and the interconnected systems on which it relies (including information and products) to identify those critical infrastructures or related components that may be at risk from an attack, and to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation.[87]

Assessing the vulnerabilities of a relatively restricted IT system such as a business network is far easier than doing the same on a higher system level. There are numerous vulnerability assessment tools that scan operating systems and applications for potential problems.

However, it may well be that vulnerabilities and infrastructure disruptions will not be traceable in any useful way to single technical subsystems – this could be due to a consequence of a overwhelming system complexity.[88] The

85 President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, October 1997), Appendix, B-3.

86 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, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 15.

87 President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, October 1997), Appendix, B-3.

88 Westrin, Peter. "Critical Information Infrastructure Protection", in: Wenger, Andreas (ed.), *The Internet and the Changing Face of International Relations and Security*. Information & Security: An International Journal, Volume 7 (2001), pp. 67–79.

analysis of vulnerability should therefore be based instead on *functional units*, whose interactions with each other and with their environment can best be described by way of their societal manifestations as a whole, with less emphasis placed on technical issues.[89]

Additionally, threats and vulnerabilities must be seen as two sides of the same coin: As a threat-source does not present a risk when there is no vulnerability that can be exercised, a vulnerability on its own also does not represent a risk when there is no threat. Besides, especially when considering human threats, for example terrorism, a sole focus on vulnerabilities, sensible though it may be with respect to cost-benefit arguments, often implicitly assumes that terrorist actors will also recognize and identify the same infrastructures as priority targets – an assumption which might backfire.[90]

Examples of Vulnerability Assessments

There is a lot of emphasis on vulnerabilities in the current CIP/CIIP debate, resulting in variety of vulnerability assessment methods and tools. However, they vary considerably in terms of the size and nature of the system they can evaluate. Below, the following five examples are described:

- Example 1 (Australia) – PreDict Vulnerability Assessment Process (PreDict)
- Example 2 (Germany) – Vulnerability Assessment CYTEX 200x (CYTEX)
- Example 3 (Netherlands) – KWINT Vulnerability Assessment (KWINT)
- Example 4 (United States) – DoE Vulnerability Assessment Methodology (DoE)
- Example 5 (United States) – CIAO Vulnerability Assessment Process/Project Matrix (CIAO)

89 Ibid.

90 Zimmermann, Doron. *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception*, ed. Andreas Wenger, *Züricher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 67* (Zurich, 2003), pp. 61–65.

Example 1 (Australia) – PreDict Vulnerability Assessment Process (PreDict)

♦ The PreDict approach also appears in *Chapter 1: Sector Analysis* and in *Chapter 2: Interdependency Analysis.*

In 1998, Australian government officials decided to analyze the national defense-related infrastructure in order to develop strategies to remove, ameliorate, and avoid identified vulnerabilities. A multi-step →*Vulnerability Assessment* Process was developed for this project (Figure 24).[91]

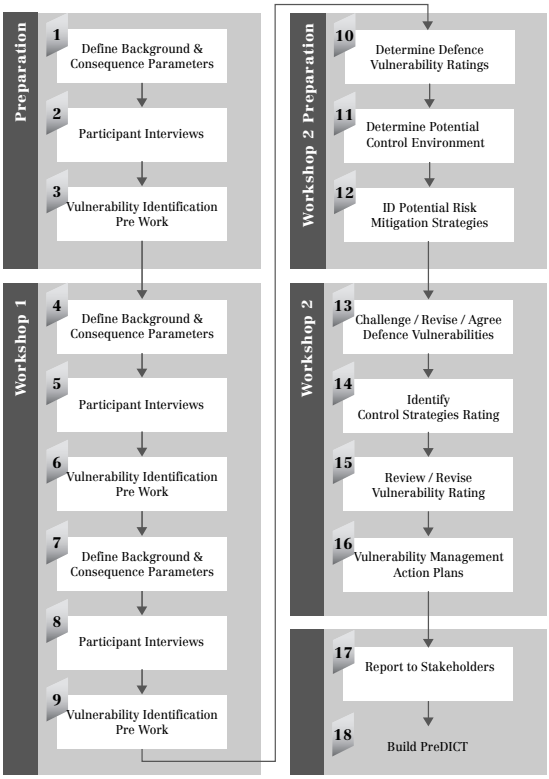


Figure 24: PreDict Vulnerability Assessment Process

In the first phase, the study identified vulnerabilities in fifteen infrastructure sectors and highlighted their interdependence. In a second phase, the project identified preliminary strategies aimed at removing the vulnerabilities, with a special focus on defense needs.

In a next step, industry *Vulnerability Profiles* were developed for each of the ten sectors, based on industry analysis and interviews, with a focus on the critical interdependencies between them. The vulnerabilities were grouped into twelve "Broad Risk Areas" in order to compare and contrast vulnerabilities between industry sectors and defense, and to group the identified vulnerabilities into common

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

areas for analysis. The majority of the Broad Risk Area titles were drawn from →*Sector Analysis* (PEST, Porter's analysis, and SWOT analysis).[92]

The vulnerabilities were rated first by quantifying the consequence of each vulnerability by degree (→*Categories*: "insignificant", "minor", "moderate", "major", "catastrophic"), and then by determining the likelihood of the occurrence of the vulnerability. 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 25):

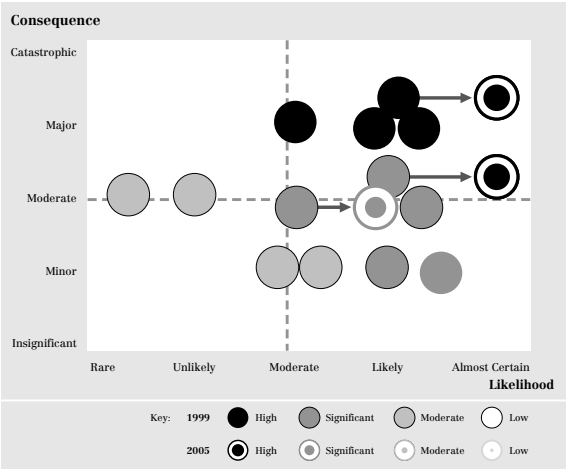


Figure 25: Vulnerability Profile for the Technology Sector

Vulnerabilities with the highest rating by sector using this method were prioritized for the development of mitigation strategies in the following steps.[93]

*Example 2 (Germany) – Vulnerability Assessment CYTEX 200x (CYTEX)**

Initiated by the *German Group on Infrastructure Protection* (AKSIS),[94] the cyber-terror exercise "CYTEX 2001" was organized in 2001 to study the impact of terrorist cyber-attacks against the CI of an urban region. Participants in this exercise included governmental agencies, major infrastructure providers (such as public services, power generation, telecommunication, public

92 The twelve "Broad Risk Areas" are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources and Training), and Flexibility/Adaptability.

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

* This section is based on information provided by Thomas Beer, IABG.

94 http://www.aksis.de.

transport, air traffic control, and banks), companies dependent on the CI, and private service providers.

The storyboard entailed coordinated and concerted cyber-attacks of various kinds against CI conducted by a terrorist movement specialized on cyber-attacks. In the scenario, the series of cyber-attacks led to the breakdown of public life for hours, until the functions of the attacked CI could be reactivated as the result of disaster management. The exercise simulated a time period of 24 hours.

The overall aim of the exercise was to study the impact of specific attacks on selected infrastructures in public life, the disaster management process (including the information and communication flow between the actors), steps taken to reestablish the functioning of urban life, and the sensitization of stakeholders.

Various computer simulation models were used in the preparation of the exercise and during the exercise, as a way for the Directing Staff to exercise control. The *Powersim* and *GAMMA* tools were applied. The exercise led to important insights into the vulnerability of infrastructures, disaster management deficiencies, and structural shortfalls.[95]

Example 3 (Netherlands) – KWINT Vulnerability Assessment (KWINT)

♦ The KWINT approach also appears in *Chapter 1: Sector Analysis.*

In 2001, the *Stratix Consulting Group/ TNO FEL* completed the so-called *KWINT-Report* (from the Dutch working title "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid").[96] The aim of the KWINT report was to analyze the current vulnerabilities of the Dutch section of the Internet,[97] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[98] The vulnerability analysis was conducted for the social level, the functional level, the structural level, and the physical level (→see Chapter 1 on *Sector Analysis*), as well

95 This section is based on information provided by Thomas Beer, IABG.

96 Luiijf, Eric, M. Klaver, and 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).

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

98 Luiijf, Klaver, Huizenga. The Vulnerable Internet.

as 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.

This resulted in six tables (matrices) that were aggregated and condensed. The final outcome is a matrix showing the most important vulnerabilities of the (Netherlands' section of the) Internet (Figure 26, excerpt of the whole matrix):

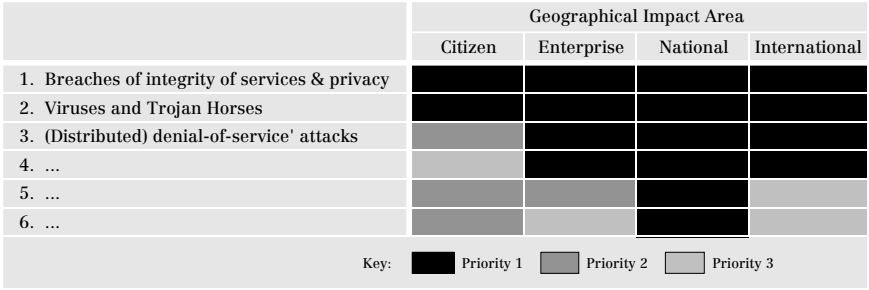


Figure 26: Geographical Impact Area Matrix (Excerpt)

The impacts of selected vulnerabilities on citizens, enterprises, the nation, and society were assessed in this matrix, as were vulnerabilities with global impact (geographical impact area). A number of measures derived from these results were subsequently proposed to the Dutch government.

Example 4 (United States) – DoE Vulnerability Assessment Methodology (DoE)

The *National Strategy for Homeland Security* (2002) and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* clarify federal responsibilities and assign primary responsibility for coordinating protection activities within the energy sector to the Department of Energy (DoE). It is the Office of Energy Assurance (OEA) that leads the federal government's effort to ensure a robust, secure, and reliable energy infrastructure in the new threat environment that includes malevolent threats and increasing complexity due to interdependencies.

The OEA has developed a three-step Vulnerability Assessment Process, described in the *Vulnerability and Risk Analysis Program: Overview of*

Assessment Methodology, published on 28 September 2001.[99] The methodology is divided into three basic phases: pre-assessment, assessment, and post-assessment. Each phase consists of a series of elements or tasks, as shown in Figure 27:

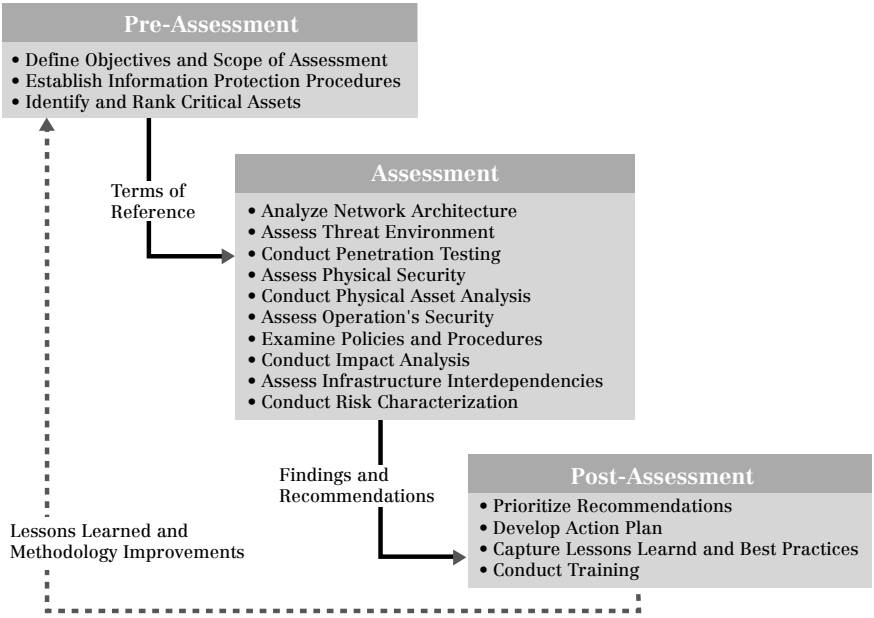


Figure 27: DoE Vulnerability Assessment Process

The updated version of the aforementioned report focuses on the methodology in more detail. Since a general vulnerability assessment methodology is lacking, the DoE has developed a methodology that is tailored to assessing the electric power industry. Companies were asked to consider individually the applicability of the vulnerability assessment elements to their situation.[100]

99 US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology* (28 September 2001). http://www.esisac.com/publicdocs/assessment_methods/OEA_VA_Methodology.pdf.

100 US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment Methodology. Electric Power Infrastructure* (draft, September 2002). http://www.esisac.com/publicdocs/assessment_methods/VA.pdf.

Example 5 (United States) – CIAO Vulnerability Assessment Process/Project Matrix (CIAO)

On the basis of *Presidential Decision Directive* (PDD) 63 and the National Plan 1.0, CIAO developed "Project Matrix™". It is 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. 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.[101]

The comprehensive methodology as such is confidential. However, a comparable approach, called *Vulnerability Assessment Framework* (VAF), is publicly available.[102] Figure 28 shows the three steps of the VAF Evaluation Process approach.

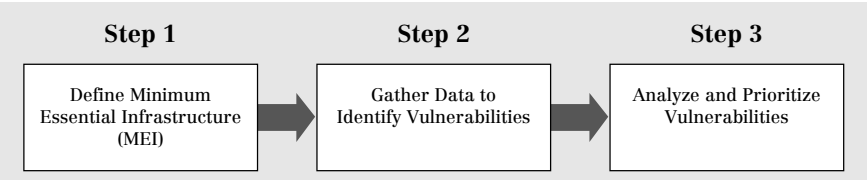


Figure 28: Steps of the VAF Evaluation Process

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

102 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 draws 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 1: Define Minimum Essential Infrastructure (MEI)

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

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 essential for achieving the organization's core mission(s). The criteria used to identify these vulnerabilities are depicted in Figure 29, showing the so-called "VAF Cube":

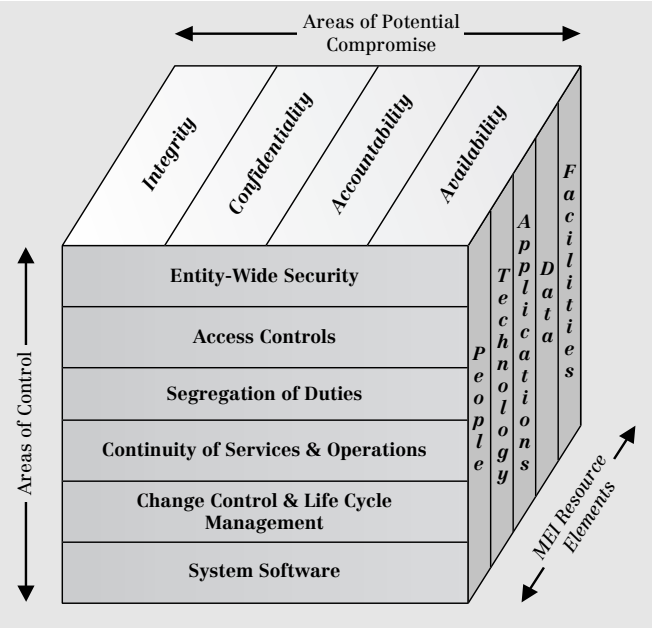


Figure 29: The VAF Cube

Step 3: Analyze and Prioritize Vulnerabilities

In Step 3 the vulnerabilities identified with Step 2 are defined and analyzed. This allows a first order of prioritization for the purpose of remediation or minimization. Figure 30 shows the activities conducted in Step 3:

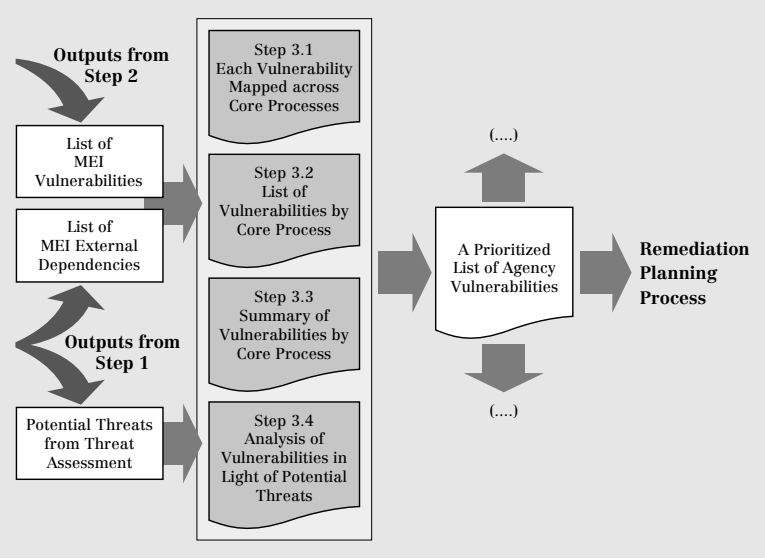


Figure 30: Step 3 Activities

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 processes; (3) a graphical summary of the number of vulnerabilities by core processes 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.

6 Impact Assessment

An isolated vulnerability and an isolated threat are not enough to cause harm or damage to CI/CII. Rather, the convergence of a threat with a specific vulnerability, combined with the possibility of a *harmful impact*, produces the risk. Such impacts are disruptive challenges of different types, durations, and levels of severity, and can be measured using different parameters such as economic loss or social and political damage. The term "impact" is also used interchangeably with the terms "harm", "effect", or "consequence".

What is Impact Assessment?

Impact assessment is one step in the overall risk analysis process. Its aim is to determine the impact resulting from a successful threat exercise of a vulnerability. The grade of possible harm to an asset must be determined by a number of experts familiar with the assets, be they executives (such as experts within the administration), asset owners, or asset managers.

The adverse impact of a security event on IT-systems can be described in terms of loss or degradation of any, or several, of the →*IT-Security Objectives:* integrity, availability, and confidentiality. Other categories might be applied if risk analysis is conducted for more abstract systems: Some tangible impacts can be expressed quantitatively as lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, or damage to an organization's interest) cannot be measured in specific units. But they can at least be described qualitatively (e.g., using the impact categories "high", "medium", and "low").[103] However, in interdependent systems, assessing the impact of the loss of a critical asset becomes fairly complex.

103 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, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 22.

There are several quantitative and/or qualitative assessment approaches to impact assessment, which have both specific advantages and disadvantages:

- Quantitative Impact Assessment:
  - The major advantage of a quantitative impact analysis is that it provides a measurement of the impact's magnitude, which can be used in the cost-benefit analysis of recommended controls.
  - The disadvantage is that, depending on the numerical ranges used to express the measurement, the outcome of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Hence, additional factors must often be taken into account to determine the magnitude of impact.
- Qualitative Impact Assessment:
  - The main *advantage* of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
  - The *disadvantage* of the qualitative analysis is that because the magnitude of impacts cannot be measured in quantitative terms, a cost-benefit analysis of any recommended controls is not feasible.[104]

104 Ibid., p. 23.

Examples of Impact Assessment

Below, the following two examples are described:

- Example 1 (Canada) – OCIPEP Model for Impact Assessment (OCIPEP)
- Example 2 (United Kingdom) – NISCC Impact Model (NISCC)

Example 1 (Canada) – OCIPEP Model for Impact Assessment (OCIPEP)

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is developing a guideline aimed at assisting CI owners and operators in developing criteria for critical →*Assets* and to establish their relative criticality. CI owners and operators are asked to identify critical assets in infrastructures and assess the potential effects of loss of the asset.

The Canadian model for impact assessment distinguishes six impact categories (service delivery, public, economic, political, environmental, interdependency). The impact of the loss or disruption of the asset is assessed by the use of three impact factors: scope, magnitude, and effects of time:

- Scope: The loss of an asset is rated by the extent of the geographic area affected (impacted), usually "local", "provincial/territorial", or "national".
- Magnitude: The degree of the impact or loss is assessed in the context of the impact category using the →*Categories* "none", "minimal", "moderate", and "mjor".
- Effects of Time: The passage of time may have an affect on the loss of an asset's magnitude and scope of impact.

The following table (Table 6) is used to depict the information collected for a specific asset (e.g., a server) in a specific sector (e.g., telecommunications) for easier analysis.

Example 2 (United Kingdom) – NISCC Impact Model (NISCC)

The UK's *National Infrastructure Security Coordination Centre* (NISCC) is currently developing a procedure for impact analysis that will allow NISCC to compare disruptive challenges of different types, durations, and severities, by using a single model. This allows for the assessment of the significance or criticality of a single IT system, critical service, or attack scenario, using a common 'currency'. It is designed to produce a standard scale, or profile over time, of the impact of any 'disruptive challenge' to a country. The scale has three axes: area of impact, severity of impact, and time.

Asset Name:	**Impact Factors**		
Sector:			
Impact Categories	**Magnitude**	**Scope**	**Effects of Time**
Service Delivery			
What will be the impact of the loss of this element/asset on the delivery or level of the particular service/product within the respective sector?			
Public			
Could the loss of this asset result in death, serious injury, or displacement of people?			
Could the loss of this asset result in low morale, panic, rioting, or civil disorder?			
Economic			
What economic impact would arise from the loss or degraded services of the asset?			
Political			
What impact could the loss of this asset have on public confidence, either directly or through related service degradation or loss?			
Will the loss of this asset significantly reduce the ability of government to deliver basic government services in the areas of public health, safety, and economic security, or to provide essential services?			
Environmental			
What would be the environmental impact of the loss or degradation of service of this asset/element?			
What would be affected by the loss or degradation of service of this asset/element (insert all that apply in the Scope box)?			
Interdependency			
Are assets/elements within the sector dependent upon this asset?			
Are assets/elements outside the sector dependent upon this asset?			

Table 6: Canadian Impact Analysis Table

- Area of Impact: The four areas of impact for the model are derived from the definition of the UK critical infrastructures:[105]
  - Loss of life,
  - Economic consequences,
  - Social consequences,
  - Political consequences.
- Severity of Impact: Severity is measured on a →*Logarithmic Scale* up to a maximum of 10. For each of the four areas there is a logical ceiling – corresponding to a score of 8 or 10, depending on the area. The impact scales in the four areas are designed to be of approximately equivalent severity. The ceilings for each of the four impact areas are shown in Table 7.

Impact Area	Scale Max	Impact Severity
Loss of Life	10	Death of 10% to 100% of population of country
Economic	8	Loss of between 10% and 100% of annual GDP
Social	8	Complete collapse of society; anarchy and chaos
Political	8	Total failure of political machine

Table 7: Ceilings for each of the four Impact Areas

The logarithmic scale allows for much greater granularity at the lower end of the axis: for example, for 'economy', the full scale for the UK, with a population of about 60 million and a GDP of £1 trillion, runs as shown in Table 8. Gradations in the scale for social and political impacts can also be set out. Social and political scales will be more subjective, using examples rather than number ranges.

105 "Those parts of the United Kingdom's infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening serious economic or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the Government." Barry, Ted. "Critical Information Infrastructure Protection in the United Kingdom". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003). →See Part I for more detail.

Scale	Economic range	
	from…	to…
10	greater than total UK GDP	
9		
8	£100'000'000'000	£1'000'000'000'000
7	£10'000'000'000	£100'000'000'000
6	£1'000'000'000	£10'000'000'000
5	£100'000'000	£1'000'000'000
4	£10'000'000	£100'000'000
3	£1'000'000	£10'000'000
2	£100'000	£1'000'000
1	£10'000	£100'000

Table 8: Scale for Economic Range

- Time: The duration of a disruptive impact is measured by again using a logarithmic scale. For some events (such as electronic attacks), occurrence, detection, and remedial action may all take place within a matter of days. Others will have a much longer time-frame: for example, the impact of global warming will be felt over decades and centuries.

An event or scenario can be represented in a three-dimensional graph. The example shows a terrorist attack, which may cause short-term loss of life, longer-term economic damage, and medium-term social and political consequences (Figure 31):

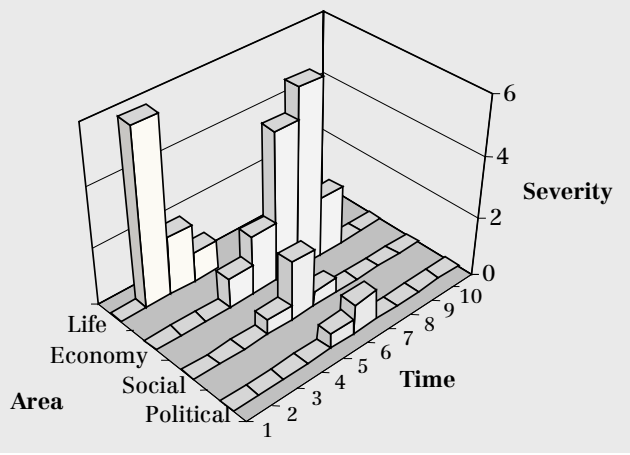


Figure 31: UK Impact Three-Dimensional Graph

7 System Analysis

The term →*System* has many definitions: It often refers to a combination of related elements organized into a complex whole, or to any collection of component elements that work together to perform a task. In the engineering disciplines, the term is often applied to an assembly of mechanical or electronic components that function together as a unit. In computing, it describes a set of computer components, an assembly of computer hardware, software, and peripherals functioning together.

In the context of CIP/CIIP, a system can be seen as a compound of several CI, a single infrastructure, an infrastructure-dependent enterprise, or a particular system within a given infrastructure, according four hierarchy levels: 1) System of systems; 2) Individual infrastructures; 3) Individual system or enterprise; and 4) Technical components.[106]

What is System Analysis?

System analysis in the context of CIIP is concerned with gaining a better understanding of any part of a defined system. While sector analysis is mainly concerned with the qualitative assessment of various aspects of industry sectors, such as their critical properties or the identification of vital processes, system analysis is a more complex approach. It employs mathematical models and *Simulation Tools* to model interdependent behavior. Especially when dealing with a →*System of Systems* (such as the energy infrastructure), the identification of critical properties requires a system analysis approach.[107]

A →*Model* is a simplified representation of a system intended to facilitate an understanding of the actual system. System modeling is the process of describing both natural and engineered systems in precise mathematical terms. Thus, a model is a simplified representation of the real world intended to promote the development of understanding.[108]

A →*Simulation* is the compressed version of a model that leaves aside considerations of time or space, thus enabling one to perceive interactions that would not otherwise be apparent because of their separation in time or

106 Schmitz, Walter. *ACIP D6.4 Comprehensive Roadmap – Analysis and Assessment for CIP*. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Program, May 2003), p. 52.

107 Office of Energy Assurance, Goal 1: Identify Systems and Critical Infrastructure Assets, http://www.ea.doe.gov/goal1.html.

108 Definition inspired by Bellinger, Gene. *Modeling and Simulation: An Introduction.* Online at: http://www.systems-thinking.org/modsim/modsim.htm.

space. Simulation is the exploitation of a model in order to predict logical consequences of hypothetical situations. A simulation is generally used to study the implications of the defined interactions of developed models running over time.[109]

Traditionally, many models and computer simulations exist for aspects of isolated infrastructures. However, these efforts are not sufficient for modeling cascading failure in complex networks. Developing a comprehensive architecture or framework for interdependency modeling and simulation is a major challenge. It requires the coupling of multiple interdependent infrastructures. Furthermore, a comprehensive architecture or framework should be able to address all aspects of CIP/CIIP, including mitigation, response, and recovery issues. Generally speaking, simply "hooking together" existing infrastructure models is not feasible, as the differences between the models would be too large. Furthermore, such models generally do not capture →*Emergent Behavior*, a key element of interdependency analysis.[110]

Today, many experts believe that the most effective investigation of CI interdependencies is achieved by comparing infrastructures to →*Complex Adaptive Systems* (CAS), which are populations of interacting agents where an agent is an entity with a location, capabilities, and memory. With this perspective, each component of an infrastructure constitutes a small part of the intricate web that forms the overall infrastructure. This viewpoint incorporates benefits for modeling and simulation (one computational approach to understanding CAS is →*Agent-based Modeling and Simulation* (ABMS)) and is able to explain emergent behavior.[111] For situations with sparse or non-existent macro-scale information, as is the case for infrastructure interdependencies, agent-based models may utilize rich sources of micro-level data to develop interaction forecasts. Modern simulation technology capitalizes on recent technological advances in evolutionary learning algorithms and massively parallel computing.[112] The big disadvantage of these simulation models is that the complexity of the computer programs tends to obscure the underlying assumptions and inevitable subjective inputs. Faulty assumptions can distort results significantly. Also, emerging Agent-Based Modeling focuses on the individual parts of a system rather than on the system as a whole. This is

109 Ibid.

110 Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine* (Vol. 21, 6, December 2001), p. 23.

111 Ibid.

112 Sandia Laboratories Fact Sheet on Modeling on Interdependencies: http://www.sandia.gov/CIS/facts.htm.

often due to reasons of practicality; however, this simplification may render results questionable.

Examples of Modeling and Simulation Research Projects

So far, the ability to deal with complex networks is generally limited by the incomplete understanding of the fundamental driving forces affecting the network's evolution. Currently, research is being conducted on various aspects of complexity, as shown in five short descriptions below:

- Example 1 (European Union) – ACIP
- Example 2 (European Union) – COSIN
- Example 3 (European Union) – DepAuDE
- Example 4 (European Union) – Safeguard
- Example 5 (United States) – National Infrastructure Simulation and Analysis Center (NISAC)

Example 1 (European Union) – ACIP

The goal of ACIP (Analysis and Assessment for Critical Infrastructures Protection) is to determine how protection of critical infrastructures can be analyzed and assessed by modeling and simulation (M&S). It provides a roadmap for the development and application of modeling and simulation, gaming, and other adequate methodologies and tools for the following purposes: identification and evaluation of the state of the art of CIP; analysis of mutual dependencies of infrastructures and cascading effects in case of disturbances; investigation of different scenarios in order to determine the gaps, deficiencies, and robustness of CIS, and identification of technological development and necessary protective measures with respect to CIP.[113]

Example 2 (European Union) – COSIN

COSIN (COevolution and Self-organization In dynamical Networks) is a research project financed by the European Commission through the 5th Framework Program. It involves six nodes in five countries. The project's main aim is to develop a series of theoretical, graphical, analytical, and computational tools to describe the complex behavior of networks. It is also planned to develop statistical models for network growth and evolution, and to extend these to social and economic networks.[114]

113 http://www.iabg.de/acip/index.html.
114 http://www.cosin.org/.

Example 3 (European Union) – DepAuDE

The overall goal of DepAuDE (Dependability for embedded Automation systems in Dynamic Environment) is the development of a methodology and architecture to improve the dependability of non-safety critical, distributed, embedded automation systems with both IP (inter-site) and dedicated (intra-site) connections.[115]

Example 4 (European Union) – Safeguard

Safeguard aims to enhance the dependability and survivability of Large Complex Critical Infrastructures (LCCIs), such as distributed electric and telecommunication networks. The main objectives are to develop conceptual and software tools (integrated methodologies, models, methods, and middleware) that will enhance the dependability and survivability of LCCIs, including the underlying Networked Information Intensive Systems (NIISs), which control these LCCIs.[116]

Example 5 (United States) – National Infrastructure Simulation and Analysis Center (NISAC)

The *National Infrastructure Simulation and Analysis Center* (NISAC) is to be established as the first comprehensive capability for assessing a system of infrastructures and its interdependencies. NISAC's core partners are *Sandia National Laboratories* and *Los Alamos National Laboratory*.[117]

At Sandia, efforts are currently underway to develop computer simulation tools to predict, in real time, the consequences of disruptive events on a nation's critical infrastructures. The modeling approach utilizes an agent-based methodology to predict critical infrastructure interactions. This simulation technology capitalizes on recent technological advances in evolutionary learning algorithms and massively parallel computing. Interactions among infrastructure elements are modeled individually by smart agents, one for each interaction. This modeling protocol can utilize thousands of agents to model very complex systems, and offers several advantages over traditional modeling techniques for modeling disruptions or shocks to interdependent infrastructure systems. For example, unlike analytic models, functional forms of the model's endogenous relationships are not required. For problems where macro-scale information is sparse or non-existent, as is the case for infrastructure interdependencies, agent-based models can utilize existing rich sources

115 http://lesbos.esat.kuleuven.ac.be/depaude/index.php.
116 http://www.ist-safeguard.org/.
117 http://www.sandia.gov/CIS/NISAC.htm.

of micro-level data to develop interaction forecasts. The product relies upon the development of improved analytic modeling methods, dynamic object-oriented programming, improved visualization, and highly scalable simulation modeling methods that will leverage Sandia's high-performance computing capability and will produce meaningful systems-level models.[118]

118 http://www.sandia.gov/Surety/Facts/Modeling.htm.

Part III
Overview Chapters

Structure of Part III

Introduction

Part III of this handbook contains three short overview chapters:

(1) The first describes CIIP efforts by international organizations, namely the European Union (EU), the G8 Group, the North Atlantic Treaty Organization (NATO), the Organization for Economic Cooperation and Development (OECD), and the United Nations (UN).
(2) The second chapter deals with legal issues at both the international and the national levels. Some interesting examples of national developments are provided .
(3) The third chapter gives an overview of recent research and development (R&D) efforts concerning CIP/CIIP. The aim is not to give a detailed picture for each country, but rather to summarize the "big picture"; therefore the focus is on the EU and the US.

International Organizations

The threats to CIP/CIIP do not respect functional or geographic boundaries, and the various sectors share cross-border vulnerabilities and interdependencies. This is especially true as all infrastructures rely on energy and telecommunications for support. All of the above factors strengthen the case for making CIP/CIIP an international co-operation effort: strong international partnerships between governments and critical infrastructure owners and operators are becoming essential. Many international organizations are dealing with this challenge and have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices.

This section gives an overview of CIIP efforts of the following international organizations: The *European Union* (EU), the *G8 Group*, the *North Atlantic Treaty Organization* (NATO), the *Organization for Economic Cooperation and Development* (OECD), and the *United Nations* (UN).

European Union (EU)

The EU is a key player at the international level concerning CIIP. CIIP, the Information Society, and Information Security are increasingly recognized as key issues. The EU is supporting these issues and investigating them by

- Considering its various aspects and impacts on citizenship, education, business, health, and communications;
- Supporting relevant programs and initiatives, such as the eEurope Action Plan, Information Society Technologies Research, eContent, eSafety, the Internet Action Plan, etc.[1]

The following sections give a short overview of important steps taken by the EU in the past.

"eEurope 2002 – An Information Society for all"

The program "*eEurope 2002 – An Information Society for all*" was launched by the EU on 8 December 1999. It is a key initiative within the EU's strategy for modernizing the European economy.[2] The EU has identified a tremendous economic and social potential offered by new information and communication technologies. The "eEurope 2002 action plan" was launched to ensure that everyone in Europe is able to benefit from the new technological develop-

1 http://europa.eu.int/information_society/index_en.htm.
2 http://www.etsi.org/eeurope/home.htm.

ments. The plan outlines eleven main action lines for the future (including e-Security).[3]

As the information society becomes more and more important to business and society, the EU regards ensuring the security of CI/CII as an important task. To this end, the EU argues that the Internet must be available to everyone at all times without time interruptions. Furthermore, the Internet must be protected against hacker and virus attacks. The EU believes that the full development of the information society cannot take place until security issues are addressed. Information security, which includes CIIP, has become a key component of the EU's vision for the so-called "*Next Generation Internet*". Hence, it is included among the policy priorities for "*eEurope 2005*", which are: modern online services such as e-Government, e-Learning, online Health services, a dynamic e-Business environment, widespread availability of broadband access at competitive prices, and finally, a *secure information infrastructure*.[4]

"eEurope 2005: An Information Society for all"

The action plan "*eEurope 2005: An Information Society for all*" was adopted in June 2002. It is an extension of the successful "*eEurope 2002*" initiative.[5] With the "*eEurope 2005*" initiative, the EU clearly recognizes information security to be more than a purely technological challenge. The EU states that information security is mainly dependent on human behavior, on the knowledge of threats, and on the management of these threats. Hence, the social and political aspect of information security is stressed. Since information security embraces a number of policy fields such as privacy, civil rights, law enforcement, international trade, and defense, the EU promotes a "holistic approach" concerning CIIP.[6] This means that an effective CIIP approach depends on the cooperation of all actors involved (public, private, individual) and on a multi-dimensional approach to establishing protective measures (including technical aspects, social and political aspects, and legal aspects.)

Implementing Information Security in Europe

In order to fulfill the goals of the action plans, the EU has initiated and supports different implementation activities (publications, setting of standards). One of these activities was the establishment of a special *EU Forum on*

3 http://www.e-europestandards.org.
4 http://europa.eu.int/information_society/eeurope/2005/index_en.htm.
5 http://www.e-europestandards.org.
6 http://europa.eu.int/information_society/eeurope/2005/all_about/security/print_en.htm.

Cybercrime. The Forum aims to raise awareness, promote best practices for security within the EU, identify counter-crime tools and procedures to combat computer-related crime, and to develop early warning and crisis management systems.[7]

In June 2001, the *European Commission* issued a communication entitled "*Network and Information Security: Proposal for a European Policy Approach*", including recommendations directed toward the *European Standardization Bodies* for the further development of their activities.[8]

A joint group of the *European Committee for Standardization* (CEN) and the *European Telecommunications Standards Institute* (ETSI) was set up in October 2001 and issued a draft report of network and information security recommendations, which were finalized in July 2003.[9]

European Network and Information Security Agency (ENISA)

On 11 February 2003, the *European Commission* presented a proposal for "*Establishing the European Network and Information Security Agency*" (ENISA). With the decision on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security. The agency has advisory and coordinating functions concerning data-gathering and data analysis on information security. Furthermore, the agency serves as a centre of expertise and excellence for the EU member states and EU institutions. The agency helps to establish broader cooperation between the key players and to ensure the interoperability of networks and information systems by promoting security standards.[10] The ENISA agency will become operational on 1 January 2004.[11] This will be a major step towards improving CIIP at the international level.

The Sixth Framework Program FP6 IST

The overall objective of the *IST* (Information Society Technologies) efforts within the EU's *Sixth Framework Program* (FP6) is to contribute directly to realizing European policies for the knowledge society as agreed at the Lisbon Council of 2000, the Stockholm Council of 2001, the Seville Council of 2002, and reflected in the eEurope Action Plan. The IST component within

7 http://cybercrime-forum.jrc.it/default.
8 http://www.etsi.org/frameset/home.htm?/public-interest/Network_Information_Security.htm.
9 Ibid.
10 http://europa.eu.int/abc/doc/off/bull/en/200301/p103146.htm.
11 http://www.terena.nl/tech/task-forces/tf-csirt/meeting9/vietsch-nisa.pdf and http://europa.eu.int/information_society/eeurope/2002/news_library/documents/nisa_en.pdf.

FP6 aims at ensuring European leadership in the generic and applied technologies at the heart of the knowledge economy. The IST research efforts within FP6 reinforce and complement the eEurope 2005 objectives. Among the strategic objectives of IST FP6 are: "Towards a global dependability and security framework", "Semantic-based knowledge systems", "Networked business and government", "eSafety for road and air transport", "eHealth", "Cognitive systems", "Embedded systems", "Improving risk management", and "eInclusion". As in FP5, the focus of the projects is mainly on technical issues, whereas policy aspects (such as organizational aspects, ethical questions, etc.) concerning CIIP are hardly discussed and somewhat undervalued in the strategic objectives.

Group of Eight (G8)

Since 1995, the G8 has become more and more involved in issues relating to cybercrime, the information society, and critical infrastructure protection. At the Halifax summit in 1995, a group of senior experts was set up with the task of reviewing and assessing existing international agreements and mechanisms to fight organized crime. This *G8 Senior Experts Group* took stock extensively and critically before drawing up a catalogue of 40 operative recommendations. These recommendations were approved at the G8 summit in Lyon in 1996. The so-called *Lyon Group* was the first international political forum to fully recognize the significance of high-tech crime. The work of the Lyon Group has an impact beyond the G8 member states and their efforts concerning CIIP. One of the main tasks of the Lyon Group is to establish best-practice guides.[12]

A next important stage for the G8 and CIP/CIIP was in spring 2000. On 15–17 May 2000, government officials and industry participants from G8 countries and other interested parties attended the "*G8 Paris Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace*".[13] The aim was to discuss common problems and to find solutions associated with high-tech crime and the exploitation of the Internet for criminal purposes. The G8 member states were convinced, that a dialog between governments and the private sector was essential in the fight against the illegal or prejudicial use of ICT and they agreed on defining a clear and transparent framework for addressing cybercrime.[14]

12 http://www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html.
13 http://www.g8.utoronto.ca/crime/paris2000.htm.
14 Ibid.

Okinawa Charter on Global Information Society

The *Okinawa Charter on Global Information Society* was published in July 2000.[15] The Charter states that ICT is one of the most potent forces shaping the 21st century, enabling many communities to address social and economic challenges with greater efficiency and imagination.[16] One of the key principles and approaches of the Charter is that international efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. In this respect, the Okinawa charter refers to the *OECD Guidelines for Security of Information Systems*. Moreover, in the Okinawa Charter, the G8 asked both the public and private sectors to make efforts to bridge the international information and knowledge gap. The G8 is determined to continue to engage industry and other stakeholders to protect critical information infrastructures.[17]

G8 Principles for Protecting Critical Information Infrastructures

G8 members met in Paris in March 2003 for the first multilateral meeting devoted to CIP/CIIP. Top-level experts from G8 member states, together with the major CIP/CIIP operators (e.g., France Telecom for France) came together to define common principles for the protection of vital CI/CII.[18] The eleven clearly defined CIIP Principles were adopted on 5 May 2003 by the *G8 Justice and Interior Ministers*. They cover the following topics:

- The establishment of warning networks;
- Raising awareness about CIIP and their interdependencies;
- Promoting partnerships;
- Maintaining crisis communication networks;
- Facilitating the tracing of attacks;
- Training and exercising;
- Having appropriate laws and trained personnel;
- International co-operation;
- Promoting appropriate research.[19]

With the adoption of these principles, the G8 member states suggested that the emergence of a new "security culture" should encourage them to strengthen

15 http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm.

16 DDSI, Dependability Overview – *International Organisations and Dependability-Related Activities* (2002), p. 36.

17 Ibid., p. 4.

18 www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html.

19 "G8 Principles for Protecting Critical Information Infrastructures", in: *NISCC Quarterly* April–June 2003, p. 9. http://www.niscc.gov.uk/Quarterly/NQ_APRIL03_JUNE03.pdf.

international co-operation, implement the best professional practices in the field of computerized surveillance and alert, to conduct common exercises to test the reaction capabilities in case of incidents, to make other countries aware of the problems and to invite them to adopt the main lines of actions, etc.[20] The eleven principles are intended to guide national responses to CIIP. However, to this end it is crucial that the principles be communicated to all concerned parties.

*North Atlantic Treaty Organization (NATO)**

The *Ministerial Guidance for NATO Civil Emergency Planning* (CEP) for 2003–2004 includes several references to critical infrastructure protection. The *Senior Civil Emergency Planning Committee* (SCEPC) has stated that it sees a need for exploratory and definitional work on the problems that may result from attacks on critical infrastructures.[21] Moreover, the SCEPC has tasked the *Planning Boards and Committees* (PB&Cs) with exploring the general aspects of critical infrastructure, as well as the social consequences of the non-availability of critical infrastructure, including transportation assets.[22]

Civil Communication Planning Committee (CCPC)

The *Civil Communication Planning Committee* (CCPC) is responsible for reviewing existing and planned electronic public and non-public communications infrastructures, services, associated facilities, postal services, and any related services with a view to determining their suitability to meet the requirements of all vital users (civil and military) during emergencies. Recommendations are made to nations, taking into consideration new and emerging technology, national legislation and arrangements, and the role of international organizations in this field.

The CCPC has published a number of documents and studies on civil communications infrastructures, such as

- 'Critical telecommunications infrastructure protection';[23]
- 'CEP consequences of disruption of critical postal infrastructure';[24]

20 "G8 Principles for Protecting Critical Information Infrastructures", in: NISCC Quarterly April-June 2003, p. 9. http://www.niscc.gov.uk/Quarterly/NQ_APRIL03_JUNE03.pdf.

* This chapter was written by Silla Jonsdottir, NATO Headquarters, Brussels.

21 EAPC(SCEPC)N(2002)51, §12.6.

22 EAPC(SCEPC)N(2002)51, §13.8.

23 EAPC(CCPC)D(2002)8.

24 EAPC(CCPC)D(2003)2.

- 'New risks and threats to civil telecommunications';[25]
- 'CEP requirements for coordinated national telecommunications regulatory measures';
- 'New risks and threats to the postal services'.[26]

In addition, the CCPC has contributed to the *North Atlantic Council's Action Plan on Cyber Defense*. Several other studies are underway, such as:

- 'CEP consequences of the introduction of the Computer Emergency Response Teams (CERTs) / CEP consequences regarding cyber-attacks and information warfare on critical civil communication infrastructure';
- 'Identification and assessment of the interdependencies of other critical infrastructures on civil communication networks';
- 'Impact and opportunities for NATO CEP in information society developments'.

Civil Protection Committee (CPC)

In 2001, the *Civil Protection Committee* (CPC) set up an *Ad Hoc Group* (AHG) to work on issues related to CIP. One of the first tasks of the AHG was to develop and circulate to the CPC a critical infrastructure mapping survey, which invited nations to indicate how they were structurally organized to deal with critical infrastructure protection, and their state of readiness in terms of planning and infrastructure mapping.[27] A report on the analysis of the mapping survey was endorsed by the CPC in October 2002 and forwarded to the SCEPC.[28] Subsequently, the CPC developed and approved a working definition for critical infrastructure, which was endorsed by the SCEPC on 4 November 2002.[29]

On 10 September 2003, the CPC approved a paper developed by the AHG that attempts to explain the CIP concept and its link with CEP.[30] The *Concept Paper* also proposes a way forward for work to be carried out by the CPC in this field. Attached to the Concept Paper is a road map detailing immediate, mid-term, and long-term actions. Also attached is a scenario that attempts to further explain the concept, and a glossary of frequently-used CIP terms. On 6 November 2003 the SCEPC endorsed the Concept Paper prepared by the CPC AHG.

25 EAPC(CCPC)WP(2002)1, REV1.
26 EAPC(CCPC)D(2003)1.
27 EAPC(CPC)N(2002)6.
28 EAPC(CPC)D(2002)4.
29 EAPC(SCEPC)D(2002)14, REV1.
30 EAPC(CPC)WP(2003)3.

Industrial Planning Committee (IPC)

The 2003 *Industrial Planning Committee* (IPC) Seminar was held in Slovakia on 8–9 September 2003 and was attended by senior officials and representatives from EAPC governments, industry, and trade. It focused on "Industrial Interdependencies". The aim of the seminar was to examine industrial interdependencies and resulting vulnerabilities, and to discuss potential preventive and/or consequence management measures. These issues were introduced by plenary presentations, including two case studies – a Canadian paper on industrial interdependencies and a Slovakian case study on aspects of electricity, water, gas, and chemical utilities. Other presentations looked at "Preventive Measures for the Protection of Critical Infrastructure", "The Military Experience in Infrastructure Protection in France" and "Protecting Critical Infrastructure during Disasters". The results of the subsequent group discussions will be summarized in a report soon to be published.

After this seminar and based on a questionnaire circulated in April 2003[31] and replies to it,[32] the IPC agreed at its meeting in September 2003 to develop a guide containing criteria for identifying critical infrastructure in industry and the energy sector, and to compile active and passive methods of critical infrastructure protection.

Food and Agriculture Planning Committee (FAPC)

In its work program, the *Food and Agriculture Planning Committee* (FAPC) looks at how CIP impacts on food, agriculture, and water production. In particular, the FAC looks at threats, risks, and vulnerabilities affecting the water sector. The FAPC is considering setting up a multi-disciplinary training seminar in 2005, which will make better use of the wealth of knowledge of all NATO experts by bringing them together to work on this subject under exercise conditions. Other planning boards and committees, particularly the Transport, Telecommunications, and Energy Committees will be approached to encourage cross-discipline co-operation in planning and response.

Civil Aviation Planning Committee (CAPC)

The *Civil Aviation Planning Committee* (CAPC) has begun identifying critical infrastructure vulnerabilities and possible protective measures in the area of civil aviation. While the protection of airports, equipment, and resources is primarily a national responsibility, the *Civil Aviation Working Group* has discussed minimum standards that can help to make national efforts more

31 EAPC(IPC)N(2003)6.
32 EAPC(IPC)WP(2003)2.

effective. These will soon be released in a report. Any large-scale military deployment would require the transport capabilities of the civil aviation sector and the related infrastructure elements, which together with the air traffic control network, the power grid, fuel supplies, and supporting surface transportation, are all essential parts of NATO's deployment capability.

Planning Board for Inland Surface Transportation (PBIST)

The *Planning Board for Inland Surface Transportation* (PBIST) has conducted exploratory and definitional work on problems that may result from attacks on critical inland surface transport infrastructure. A PBIST report emphasizes that the civilian transport infrastructure is considered an attractive target, as global trade depends heavily on transportation.[33] The report aims to reach conclusions on threats to the inland transport infrastructure, characteristics of likely targets, possible protective measures, and the potential role of the PBIST. The report was discussed during the PBIST meeting on 17 November 2003.

Planning Board for Ocean Shipping (PBOS)

At the behest of the Council and the SCEPC, the *Planning Board for Ocean Shipping* (PBOS) continues to serve as the NATO focal point for advice and assistance on the protection of civilian maritime assets against acts of terrorism. This work includes: monitoring the work and activities of other international bodies, gathering and exchanging information from international and national sources, and providing advice and assistance as necessary. An updated progress report, which was endorsed by the PBOS on 24 September 2003, will be submitted to the SCEPC in autumn of 2004.

Coordination

The overall responsibility for coordinating CIP work lies with the SCEPC. However, on the initiative of the CPC, representatives of the *Planning Boards & Committees* (PB&Cs) meet on a regular basis to discuss various issues related to CIP. These meetings are an opportunity for all PB&Cs to present work that is underway and/or planned within their respective areas of interest, in addition to fostering closer cooperation and coordination.

33 EAPC(PBIST)D(2003)8.

Organization for Economic Cooperation and Development (OECD)

The *Organization for Economic Cooperation and Development* (OECD) is becoming more and more involved in the issue of CIIP. The OECD is committed to the fight against cybercrime in two ways: it produces documentation (resolutions and recommendations) to help governments and businesses in this fight and it raises awareness through the publication of information and statistics.[34] There is a consensus among the member states that secure and reliable (information) infrastructures and services are a necessary requirement for trustworthy e-Commerce, secure transactions, and personal data protection. This is the main reason why the OECD *Working Party on Information Security and Privacy* (WPISP) promotes a global approach to policymaking in these areas to help build trust online.[35] In addition, the *Committee for Information, Computer and Communications Policy* (ICCP) analyses the broad policy framework underlying the e-Economy, information infrastructures, and the information society.[36]

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

The events of 11 September 2001 in the US marked a turning point for the OECD's efforts for CIIP. In order to better counter cyberterrorism, computer viruses, and hacking, the OECD drew up new guidelines. At their 1037th session on 25 July 2002, the OECD members adopted the new "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*"[37]. These guidelines are designed to develop a "culture of security" among the government, businesses, and users with respect to the rapid worldwide expansion of network communication systems.

The guidelines are not binding. However, they are the result of a consensus between OECD governments and of discussions involving representatives of the information technology industry, business users, and civil society.[38] The OECD invites governments in other countries to adopt a similar approach to CIIP. Furthermore, the private sector representatives are asked to im-

34 DDSI, Dependability Overview – *International Organisations and Dependability-Related Activities* (2002), p. 67.
35 http://www.oecd.org/topic/0,2686,en_2649_34255_1_1_1_1_37409,00.html.
36 http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.
37 http://www.oecd.org/documentprint/0,2744,en_2649_33703_15582250_1_1_1_37409,00.html.
38 http://www.oecd.org/documentprint/0,2744,en_2649_34255_1946997_1_1_1_37409,00.html.

prove security aspects in their own environment, and so to provide security information and updates to the users. The individual users are urged to be more aware and responsible, and also to take the best preventive measures possible to decrease the risks to CI/CII.

In December 2003, the OECD has launched a *"Culture of Security" Web site* as part of the 30-member country Organizations' initiative to promote a global culture of security. This site primarily provides member and non-member governments with an international information-exchange tool on initiatives to implement the *OECD Guidelines* and serves as a portal to relevant Web sites as a first step towards creating a global culture of security.[39]

OECD Global Forums

Other OECD efforts concerning CIIP included the *OECD-APEC Global Forum on Policy Frameworks for the Digital Economy*, held in Honolulu in January 2003, and the *OECD Global Forum on Information Systems and Network Security*, which was convened in Oslo in October 2003. The Honolulu Forum emphasized the importance of security of information systems and networks, as well as the need for the OECD to implement the *OECD Security Guidelines* (see above). Furthermore, the importance of the preparation for the *World Summit on the Information Society* (WSIS) in December 2003 in Geneva (Switzerland) was also stressed. Many *Asia-Pacific Economic Cooperation* (APEC) member countries were invited to the Oslo conference due to an agreement made in Honolulu to increase the co-operation between the OECD and APEC. This is another major step towards international and transnational management of CIIP efforts.

Among the main intended policy impacts of the Oslo Forum are:

- Raising awareness of the importance of secure information systems and networks for safeguarding critical infrastructures, as well as business and consumer information;
- Increasing knowledge of the OECD Security Guidelines;
- Encouraging the development and the promotion of security architectures for organizations that effectively protect information systems;
- Exploring the use of technology and security standards in safeguarding IT infrastructures.[40]

39 http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

40 http://www.oecd.org/document/14/0,2340,en_2649_34255_8165070_1_1_1_37409,00.html.

United Nations (UN)

Issues related to CIIP have been discussed by different *United Nations* (UN) bodies since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several steps have since been undertaken towards better work coordination. Among these are initiatives taken by UN institutes, UN resolutions, and the establishment of *UN Task Forces* with a focus on CIIP.

UN Institute for Disarmament Research

An important step was the organization of a workshop in July 1999 by the *UN Institute for Disarmament Research* in Geneva. The main topic was how to better achieve worldwide information security and assurance in a global digital environment. In this context, a variety of issues such as Revolutions in Military Affairs (RMA) and the proliferation of offensive tools for attacking information systems and networks were discussed in Geneva. There was a consensus among the participants that the vulnerability of national and international information infrastructures to cyberattacks was increasing, and that international co-operation had to be improved in order to meet this challenge. One other conclusion was that the issue of CIIP is not only of military or strategic importance, but that it is mainly a political, economic, and social issue.[41] Hence, it is crucial to achieve cooperation between public and private actors as well as between nations.

UN Resolutions about ICT

In December 2000, the 55th *UN General Assembly* issued Resolution 55/63 on "*Combating the criminal misuse of information technologies*".[42] This was a next important step in the efforts of the UN concerning CIIP. This resolution emphasizes in particular that the *Commission on Crime Prevention and Criminal Justice* is intended to make law enforcement more efficient and effective. Furthermore, the importance of co-operation among countries and between the public and private sectors was stressed once again. The resolution also mentions the *Cyber Crime Convention* of the Council of Europe and the work done by the G8 as crucial milestones in the international field.[43]

41 Dependability Development Support Initiative (DDSI): *International Organisations and Dependability-related Activities* (draft, 31 May 2002), p. 66. http://www.ddsi.org/Documents/CR/DDSI_International_organisations.pdf.

42 UN General Assembly Resolution 55/63 (22 January 2001). http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement.

43 Ibid.

The UN Information & Communications Technologies Task Force

The establishment of the *UN ICT Task Force* in November 2001 in response to a request by the *UN Economic and Social Council* was a further important step. The task force was mandated to mobilize worldwide support for attaining the *Millennium Development Goals* with the use of ICT.[44] In September 2002, the task force published a guide called "*Information Security – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security*".[45] This publication depicts the problem of information insecurity in general, provides possible solutions for prevention and response to security incidents (including standards and best practices).[46]

UN Resolution to Improve Cybersecurity

The US intends to propose a resolution at the *UN General Assembly* to highlight key elements needed for an effective cybersecurity environment. The US is convinced that, no matter what steps individual nations take to safeguard their own CII, a global approach is required for CIIP. Therefore, the US intends to encourage other nations to join in its efforts to protect CII. With this resolution, the US seeks to encourage as many other nations as possible to establish own national CIIP programs with the help of the governments, the public sector, and the public.[47]

It is hoped that this resolution will strengthen public-private partnerships, promote international cooperation in CIIP, and improve future efforts for national and international information-sharing and incident-reporting.

44 http://www.unicttaskforce.org/about/principal.asp.

45 Gelbstein, Eduardo and Ahmad Kamal. *Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security* (New York, 2002). http://www.unicttaskforce.org/community/documents/764021661_unicttf_infosec.pdf.

46 Ibid.

47 http://www.state.gov/p/io/rls/fs/2003/24184.htm.

Current Topics in Law and Legislation

The following section provides an overview of the main national and international respectively EU-level legal issues in the area of CIIP. The development of effective regulation, law, and criminal justice mechanisms are essential in deterring virtual abuse and other offences against information infrastructure. Moreover, a strict regulation may create trust in the new ICT and encourage the private sector and individuals to make better use of e-Commerce or e-Government services.

The following is an overview of important common issues currently discussed in the context of legislation procedures in the countries covered in the handbook:[48]

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-Commerce and e-Business;
- International harmonization of cybercrime law;
- Minimum levels of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

48 Finnish Communications Regulatory Authority. *Information Security Review Related to the National Information Security Strategy* (24 May 2002). http://www.ficora.fi/englanti/document/review.pdf; includes information on national approaches from experts involved.

International Level

Due to the inherently transnational character of CI/CII, there is a need to harmonize national legal provisions and to enhance judicial and police co-operation. However, so far, the international legal framework has remained rather confused and is actually an obstacle to joint action by the actors involved.

At the European level, the *Council of Europe Convention on Cybercrime* and the proposed *European Framework Decision on Attacks Against Information Systems* are currently among the most important pillars of transnational CIIP legislation efforts.

Council of Europe Cybercrime Convention

International cooperation is crucial when it comes to tackling cybercrime. The most important legislative instrument in this area is the *Council of Europe Cybercrime Convention*[49], which was signed on 23 November 2001 by twenty-six members and four non-members of the Council. The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.[50] An additional protocol to the Convention outlaws racist and xenophobic acts committed through computer systems. The criminal offences concerned are:

- Crimes against the confidentiality, integrity, and availability of computer data or systems, such as spreading of viruses;
- Computer-related offences such as virtual fraud and forgery;
- Content-related offences, such as child pornography;
- Offences related to infringements of intellectual property and related rights;

Another objective of the convention is to facilitate the conduct of criminal investigations in cyberspace.[51]

49 http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.
50 http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
51 http://press.coe.int/cp/2001/893a(2001).htm.

European Framework Decision on Attacks Against Information Systems

An important step is the *Framework Decision on Attacks against Information Systems*, as proposed by the *European Commission* in April 2002.[52] The Framework seeks to address cybercrime in a harmonized manner throughout Europe, including prosecuting attacks against critical civil infrastructures such as power plants, water supply systems, airports, and hospitals. It also plans to ensure that European law enforcement authorities can take action against offences involving illegal access, hacking, or interference with information systems, such as denial of service attacks, web-site defacements, and viruses.

Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries

Computer Security Incident Response Teams (CSIRTs) operate in an environment where the legal codes of the different member states diverge in dealing with computer crime and misuse. Moreover, the law enforcement authorities of the EU member states often have varying approaches to similar problems. Therefore, the *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries*[53] was designed to help Europe's CSIRT to meet the challenge of dealing with incidents. The handbook was funded by the EC and commissioned to RAND Europe, who led the project.

The *Handbook of Legislative Procedures* is useful for organizations involved in the incident-handling phase (e.g., CSIRTs and CERTs) and for law enforcement agencies engaged in incident response and investigation. Although the handbook focuses on the 15 EU member states, it is also of interest to CSIRTs in other countries.

The *Handbook of Legislative Procedures* has two sections: The first covers incident descriptions, international legal and forensic principles, and incident surveys. Particular attention is paid to the examination of the content of the *Council of Europe's Cybercrime Convention* and the proposed *European Framework Decision on Attacks Against Information Systems*. The second

52 Commission of the European Communities. *Proposal for a Council Framework Decision on Attacks Against Information Systems.* COM (2002) 173 final. http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf.

53 http://www.iaac.org.uk/csirt.htm.

section of the handbook contains an analysis for each EU member state and its legislation in the area of computer crime.[54]

Cyber Tools On-Line Search for Evidence (CTOSE)

The *EU Cyber Tools On-Line Search for Evidence* (CTOSE)[55] project, a research project funded by the *European Commission's Information Society Technologies* (IST) program, has developed forensic standards for prosecuting cybercrime. The standards are based on a methodology that identifies, secures, integrates, and presents electronic evidence. This methodology should enable system administrators, information technology security staff and computer incident investigators, police and law-enforcement agencies, etc., to follow consistent and standardized procedures when investigating computer incidents. Furthermore, the methodology ensures that all electronic evidence is gathered and stored in a way that meets legal standards. Backers of the methodology hope it will be adopted as a best-practice standard throughout Europe.[56]

National Level

Although many developed countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have only begun to review and adapt their CIIP legislation after 11 September 2001. Because national laws are developed autonomously, some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cybercrime.

National Examples

This section lists some interesting examples of CIIP legislation. This includes a wide variety of 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.

54 RAND Europe. *Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries* (study for the European Commission Information Society Directorate-General, 2002). http://www.iaac.org.uk/CSIRT%20Handbook-v24.pdf.

55 http://www.ctose.org.

56 http://www.ctose.org/info/index.html.

Legal Issues in Australia

The *Australian Security Intelligence Agency* (ASIO) has the power to covertly enter and search the premises of those it suspects of espionage or terrorism. The *ASIO Act* (1979) was subsequently amended *(ASIO Amendment Act)*[57] in 1999, to give the organization the same covert access to targets' computer systems.

The Australian Government has introduced new computer crime legislation, the *Cybercrime Act* (2001),[58] to implement the rulings on computer offences proposed in the recently released *Model Criminal Code Report*.[59] 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. It is hoped that the penalties will provide a strong deterrent to those who engage in cybercrime such as hacking, computer virus propagation, and denial of service attacks. Serious offences, such as stalking and fraud, are also covered.[60]

Since the introduction of the *Cybercrime Act* (2001),[61] the ASIO has enjoyed considerably more leeway and may now conduct CIIP investigations. Under new counter-terrorism legislation introduced in 2003, the ASIO can detain and question suspects without charge for up to seven days. Previously, the ASIO had not been allowed to interrogate suspects, and relied on the *Australian Federal Police* (AFP) to carry out police actions on its behalf or based on the intelligence that the ASIO had covertly generated.

The introduction of the *Cybercrime Act* (2001) prompted the AFP to join forces with state and territory police to create a national organization against cybercrime. The line dividing cybercrime and cyberterrorism is blurred, because many of the tools and techniques are common to both activities.

Further Acts:

- Crimes Act 1901 Part VIA: This act deals with attacks against computers in Australia, and with all computer attacks using the Australian telecommunications system;

57 http://www.aph.gov.au/library/pubs/bd/1998-99/99bd172.htm#Passage.

58 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

59 http://www.aic.gov.au/links/mcc.html.

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

61 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd048.htm.

- Telecommunications (Interception) Act 1979: This act prohibits the interception of telecommunications (including data transmissions) within Australia, except under warrant. There are also provisions in the *Telecommunications Act of 1997* that require carriers or carriage service providers to enter into an agreement with the government about planning for network survivability or operational requirements in time of crisis, and which stipulate that rules and licenses for carriers or service providers may require compliance with a disaster plan;
- 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.

Legal Issues in Italy[62]

Italy has specific laws and ministerial decrees devoted to CIP and CIIP. In the early 1990s, a new law related to computer crimes was introduced (Law 547 of 23 December 1993), giving more power to investigators in the evidence-collection phase, and also allowing computer and telecommunication interceptions. Italy was one of the first European countries to adopt such legislation, mainly due to new crime figures concerning computer frauds, forgery, data damaging, computer misuse, unauthorized interceptions of computer communications, and sabotage. The great attention given to such crimes is highlighted by the fact that computer intrusions are treated as a domestic property violations.

An innovative concept of *High-Tech Crime*, which already enjoyed currency in the Italian penal legislation for different type of offences, was introduced with Law 547. According to article 420 of the *Italian Penal Code* (attempt to damage public utilities systems), actual damage or destruction to the systems are not required for such activities to constitute an offense; the mere intention suffices. Such cases will be prosecuted, even if the attempt has not been successful.

Other relevant laws include:

- Law 547, enacted on 23 December 1993, a comprehensive and integrated law against ICT crimes;

62 Information based on Roberto Setola, Secretary of the Working Group on Critical Infrastructure Protection coordinated by the Cabinet Office of the Italian Government.

- Legislative Decree 518, enacted on 29 December 1992 and modified by Law 248 (18 August 2000), a legislative decree against illicit ICT piracy;
- Law 675, enacted on 31 December 1996, a law governing personal data protection, integrated by subsequent legislation (DPR 318/1999, Law 325/2000, Legislative Decree 467/2001, and Legislative Decree 196/2003);
- Legislative Decree 374/2001, changed into Law 438/2001, a law devoted to better law enforcement instruments and the repression of terrorism.

Note that Law 374/2001, transformed into Law 438/2001 after 11 September 2001, has updated the Penal Code, so that now, crimes committed in Italy are liable to prosecution, even if they are directed against a foreign state or against a multilateral institution.

Legal Issues in New Zealand

The *Crimes Amendment Act* came into force in October 2003. It includes four new offences relating to the misuse of computers and computer systems. These offences are:

- Accessing a computer system for a dishonest purpose (section 249);
- Damaging or interfering with a computer system (section 250);
- Making, selling, or distributing or possessing software for committing a crime (section 251);
- Accessing a computer system without authorization (section 252).

The expressions "access" and "computer system" are defined in section 248.

The first two offences carry a range of penalties depending on the seriousness of the offence, with a maximum of 7 and 10 years imprisonment respectively, while the remainder carries a maximum penalty of 2 years imprisonment.

The section 249 offence involves accessing a computer system directly or indirectly, either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the offence in either case is dishonesty, or deception (which is separately defined in section 240(2)).

The section 250 offence involves intentional or reckless destruction, damage, or alteration of a computer system. At its most serious, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of 10 years imprisonment. Where a person damages, deletes, modifies or otherwise interferes with or impairs any data or software without authorization, or causes a computer

system to either fail or deny service to any authorized users, the maximum penalty is 7 years imprisonment.

The key element of the section 251 "sale, supply, or distribution" offence is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commission of a crime, knowing that or being reckless as to whether it will be used for such a purpose. In the case of the "possession" offence, the key element is intention to commit a crime.

The more significant in practice of these two offences is likely to be section 252, which in effect makes computer "hacking" a criminal offence. The offence is simple unauthorized access, whether direct or indirect, to a computer system, knowing that or being reckless as to whether one is unauthorized to access that computer system.

Sections 253 and 254 contain qualified exemptions in respect of the section 252 offence for the *New Zealand Security Intelligence Service* and the *Government Communications Security Bureau* respectively, where those organizations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorization issued under section 19 of the GCSB Act 2003.

Legal Issues in Norway

The §151b of 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 supply plants, broadcasting facilities, telecommunications services, or other kinds of communication, will be punished by a maximum of 10 years imprisonment. 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 law came into effect on 12 June 1987.[63]

In Norway, the laws generally tend to place responsibility 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.[64]

63 Information provided by a Norwegian expert of the Directorate for Civil Defense and Emergency Planning (DSB), March 2002.

64 http://www.ocb.se/dokument/filer/5b_gjengsto_henriksen_abstract.pdf.

Legal Issues in Switzerland

A number of articles in the Swiss Penal Code are of relevance in the context of CIIP.

- Article 143 (unauthorized procurement of data);
- 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;[65]
- 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;[66]
- 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;[67]
- 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 electronic procedure through the unauthorized use of data, shall be punished by community service of up to five years or imprisonment;[68]

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.

In November 2001, the Federal Council accepted the "*Convention on Cybercrime of the Council of Europe*".[69] It should be noted that the Swiss

65 Based on the official English translation of the Swiss Penal Code.
66 Based on the official English translation of the Swiss Penal Code.
67 Based on the official English translation of the Swiss Penal Code.
68 Based on the official English translation of the Swiss Penal Code.
69 ISPS News (Infosociety.ch), press release: *Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats*. http://www.isps.ch.

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.

Legal Issues in the US

In the US, legislative awareness of computer crimes grew dramatically in the early 1980s, as computers became increasingly important for the conduct of business and politics. The *Computer Fraud and Abuse Act* (CFAA) of 1986 was the conclusion of several years of research and discussion among legislators.[70] It established two new felony offenses consisting of unauthorized access to "federal interest" computers[71] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, most medical, and "federal interest" computers.

The *Computer Abuse Amendments Act* of 1994 expanded the 1986 CFAA to address the transmission of viruses and other harmful code.[72] The measures provided by this act were further tightened on 26 October 2001 by the *USA PATRIOT* anti-terrorism legislation.[73] 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.[74]

Much of the federal legislation concerning CIP/CIIP was written before the emergence of "cyberthreats". 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.[75]

70 http://www4.law.cornell.edu/uscode/18/1001.html.

71 Federal interest computers are defined as two or more computers involved in a criminal offense, if they are located in different states.

72 See also http://www.digitalcentury.com/encyclo/update/comfraud.html Jones Telecommunications and Multimedia Encyclopedia.

73 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.

74 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.

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

While the overall act established the *Department of Homeland Security* (DHS), Title II of the *Homeland Security Act* (of 2002) specifically addresses information analysis and infrastructure protection. It created the *IAIP Directorate*, transferred the various agencies (like CIAO, NIPC, and others mentioned above) into the DHS, and established the categories of information to which the secretary of homeland defense has access. In order to adequately protect the nation, the secretary has access to certain intelligence analysis, infrastructure vulnerabilities, and any "raw" data that the president discloses to the secretary.

CIIP is an important issue in the US, primarily because many of critical sectors are regulated by the government, but controlled by private entities. As part of the regulation, the private entities must regularly file reports and disclose sensitive information to the government. This could place such information in jeopardy, since under the *Freedom of Information Act* (FOIA), the public can request such information from the government. However, as part of the Homeland Security Act of 2002, a *FOIA exemption* was created. Any information regarding critical infrastructures (including security systems, warnings, or interdependency studies) is exempt from disclosure.

The "*Terrorism Risk Insurance Act of 2002*" is a new law that creates a federal program for public and private compensation for insured losses resulting from acts of terrorism. All commercial insurance providers must offer terrorism risk insurance, and the federal government agrees to underwrite some of the losses in the event that a terrorist event takes place. Under this law, an act of terrorism includes any act of violence against infrastructure.[76] This could include catastrophic network assaults as well as physical attack.

After the attacks of 11 September 2001, the *Federal Energy Regulatory Commission* (FERC) removed certain information from its website and its public reading room. This included detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February, 2003, FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take the need/purpose of the information into account. Access is granted on a case-by-case basis, and only to individual applicants.

76 Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002).

Research and Development

This section gives an overview of recent efforts in Research and Development (R&D) concerning CIP/CIIP.[77] The aim is not to give a detailed picture for each country, but rather to summarize the "big picture". At the moment, the US and the EU are the major players in the field of CIP/CIIP R&D. The US has a leading role in identifying and promoting relevant research topics. The EU plays a crucial role in supporting cross-national R&D and information exchange in the field of CIIP in Europe, although its role could be even stronger. The focus in the section is on these two major actors.

There is no doubt that CIIP will be a major R&D challenge in the future. Recent publications and overviews show that R&D in the field of CIP/CIIP is undertaken by a large variety of actors in each country: research institutes at universities, private sector research institutes and laboratories, networks of excellence, national research councils, etc. There is also a large number of R&D topics ranging from technical aspects to rather social themes. Since the issue of CIIP is largely interdisciplinary, the best approach in R&D would be a cooperative one, to define a common R&D strategy for CIIP. However, so far, there has been rather little coordination and cooperation between R&D actors at the *national level*. It is therefore hard to give a full overview of key R&D actors involved in CIP/CIIP.

The inherently transnational nature of CI/CII and the growing international dependency on CI/CII, threats and vulnerabilities to the national CI/CII (a good example is the big blackout in Italy's electric power system in October 2003) make the topic of CIP/CIIP R&D an obvious issue for international cooperation. New approaches are needed in R&D, from design through operation to management. A common R&D strategy in the field of CIIP has to transcend the component and system level. However, so far, there has been rather little effort in *international R&D cooperation* and collaborative action concerning CIIP. The rationale for strategic coordination of R&D at the international level was outlined at a December 2001 EU–US workshop on R&D in the field of CIIP.[78] On that occasion, a list of important drivers for international collaboration on R&D was outlined. Among these drivers are:[79]

77 → *All R&D dealing with methods and models and CIIP are excluded here but can be found in Part II of this Handbook.*

78 EU-US Workshop Report. *R&D Strategy for a dependable information society: EU-US collaboration*, (1–2 December 2001 Düsseldorf, Germany), available from www.ddsi.org.

79 DDSI, R&D Strategy Roadmap for Information Infrastructure Dependability, November 2002, p. 17.

- Increasingly networked and more complex embedded systems;
- Growing interdependencies between essential infrastructures;
- A shared understanding that global problems require global solutions;
- Improved cost-effectiveness through greater efficiency and faster results;
- Improved access to relevant data that is not available nationally.

European Union

For the EU, R&D is important due to several reasons: By 2010, the EU will be the largest knowledge-based economy; the EU is evolving in the direction of a single market; the information society as a whole will also develop in the coming years; dependencies among CI/CII are generally increasing, etc.

Therefore, there are several efforts for improving the coordination of CIP/CIIP R&D within the EU. One of the most important "instruments" is the *IST (Information Society Technologies) Framework Program (FP)*.[80] Sponsored by the EC, the Program helps to develop CIP/CIIP skills. Within the *Fifth Framework Program (FP5)*, out of a total of 59 R&D projects dealing with security in general, 16 were R&D projects related to CIP/CIIP. Some of the crucial CIP/CIIP projects of FP5 were:

The Dependability Development Support Initiative (DDSI)

The main aim of the *Dependability Development Support Initiative* (DDSI) was to establish networks among leading European and international stakeholders concerned with cybersecurity policies; to provide baseline data about dependability initiatives around the world; and to prepare policy roadmaps for national governments and European institutions, as well as for stakeholders in the private sectors. The results of the study should provide suggestions for action in the framework of the Europe 2005 Action Plan.[81]

Accompanying Measure System Dependability (AMSD)

The *Accompanying Measure System Dependability* (AMSD) project aimed to support the full range of dependability-related activities through the creation of roadmaps and consensus-building. Eventually, the results will result in an overall dependability roadmap that considers dependability in a holistic manner.

80 http://europa.eu.int/comm/research/fp6/index_en.html.
81 http://www.ddsi.org/DDSI-F/home.htm.

The Complex Systems Network of Excellence (EXYSTENCE)

The *Complex Systems Network of Excellence* (EXYSTENCE) project fostered multidisciplinary approaches to various aspects of complexity, ultimately creating a bridge between complexity theory and the full spectrum of "real-life" complex systems. EXYSTENCE also aimed at disseminating a kind of complexity culture in the context of decision-making, management, and production.

It is also important to note that a joint EU-US task force on R&D in CIP/CIIP was established within the FP5. In FP6, CIIP is defined as a key topic.[82] *FP6* is the *European Community Framework Programme for Research and Technological Development* and is a major tool in support of the creation of the *European Research Area* (ERA). The IST in FP6 aims at ensuring European leadership in the generic and applied technologies at the heart of the knowledge economy. The research efforts within IST FP6 are aimed at reinforcing and complementing the "*eEurope 2005*" objectives.[83] However, as in FP5, the focus of the projects in FP6 is mainly on technical issues, whereas other important CIIP aspects (policy issues, human factor issues, economic aspects, organizational aspects, ethics questions, etc.) are hardly recognized. They are rather undervalued in the strategic objectives.

The *European Commission Directorate-General's Joint Research Centre* (JRC)[84] plays an important role within the EU concerning R&D. The JRC's principal task is to provide the EC as well as the Council, the European Parliament, and member states with independent scientific and technical advice and to support policies that harmonize standards and regulate activities across the EU.[85]

The JRC supports the EU's cybersecurity policies, encompassing citizen issues such as privacy and data protection, economic issues such as fraud, abuse attacks on personal and company resources, cybercrime, and societal issues such as vulnerabilities of information-processing infrastructure and their impact on the integrity of infrastructures vital to society. The role of

82 Servida, Andrea. "The European initiatives on network and information security", *Presentation at the international workshop "Critical Infrastructure Protection (CIP) – Status and Perspectives within the Annual Meeting "Informatik 2003"* (Frankfurt, 2003).

83 Among the strategic objectives of IST FP6 are: "Towards a global dependability and security framework", "Semantic-based knowlege systems", "Networked business and government", "eSafety for road and air transport", "eHealth", "Cognitive systems", "Embedded systems", "Improving risk management", and "eInclusion".

84 http://www.jrc.org.

85 http://europa.eu.int/comm/research/fp6/index_en.html.

the JRC is to develop an integrated set of activities to support EU policies and cooperation between the JRC, R&D labs, the EU, and its member states' institutions.[86] The JRC's work in cybersecurity involves the *Institute for the Protection and Security of Citizen* (IPSC)[87] and the *Institute for Prospective Technological Studies* (IPTS),[88] supporting the *European Dependability Initiative* and the *European Working Group on Information Infrastructures Interdependencies and Vulnerabilities*, and the roadmap for a *European Warning and Information System* for network and information security threats.[89]

United States[*]

The other "big player" in R&D in the field of CIIP is the US. This is the main reason why the following section will present a more extensive overview of US efforts. The fact that, unlike the EU, the US is an independent country facilitates the R&D efforts in several ways. This is most obvious in the case of coordination efforts within the US R&D community. The following subsection focuses on coordination efforts in the US.

R&D efforts in the US deal with a large variety of issues such as interdependency analyses, threat analysis, vulnerability and risk assessments, system protection and information assurance, and intrusion detection and monitoring.[90] The degree of R&D coordination in the US is considerable. Government entities, private-sector actors, and academia all play a large role in US R&D initiatives. The following short overview focuses on activities at the *government level*.

Office of Science and Technology Policy (OSTP)

The *Office of Science and Technology Policy* (OSTP) serves as an important source of scientific and technological analysis and judgment for the US president with respect to major policies, plans, and programs of the federal government. The OSTP plays a significant role in the development of strategies for R&D prioritization. Within the OSTP, the *President's Council of Advisors on*

86 http://cybersecurity.jrc.it/policy.html.
87 http://ipsc.jrc.it.
88 http://www.jrc.es/home/index.html.
89 http://cybersecurity.irc.it/Support.html.
* This overview was mainly written by Emily Frye, Associate Director Legal Programs, CIP Project, National Center for Technology & Law, George Mason University School of Law, Arlington, US.
90 http://www.ciao.gov/CIAO_Document_Library/Report_on_Federal_CIP_R&D.pdf.

Science and Technology (PCAST) receives advice from the private sector and academic community on technology, scientific research priorities, and math and science education. Furthermore, the *National Science and Technology Council* as part of the OSTP serves as the principal means through which the president coordinates the different elements of federal R&D with regard to science and technology. An important objective of this cabinet-level council is the establishment of clear national goals for federal science and technology investments. The *National Science and Technology Council* prepares R&D strategies that are coordinated across federal agencies to form an investment package aimed at accomplishing multiple national goals.[91]

Technical Support Working Group (TSWG)

Under the policy oversight of the *Department of State* and the *Department of Defense*, the *Technical Support Working Group* (TSWG) also plays a role in the national agenda for R&D in the field of CIIP. The TWSG's mission is to conduct the national interagency R&D program for combating terrorism. The TWSG strives to identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national economic security of the United States. Membership in the TWSG includes representatives from over 80 organizations in the federal government. They work together through participation in nine subgroups, one of which focuses on CIP/CIIP. Cybersecurity projects focus on preventing or mitigating threats to computer networks vital to defense and transportation. This research will provide detection, prevention, response, and alert capabilities to counter such attacks and harden computer systems. Representatives from DOD and the NIPC chair the subgroup.[92]

National Institute of Standards and Technology (NIST)

The *Computer Security Division* (CSD) at the *National Institute of Standards and Technology* (NIST), an agency of the US Commerce Department's Technology Administration, is tasked with improving information systems security. It is one of eight divisions within the NIST's *Information Technology Laboratory*. Its mission includes raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies; researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive

91 http://www.ostp.gov/

92 http://www.tswg.gov/tswg/home/home.htm.

federal systems; developing standards, metrics, tests, and validation programs; and developing guidance to increase secure IT planning, implementation, management, and operation.[93]

In May 2003, the NIST and the *Department of Homeland Security* (DHS) signed a Memorandum of Understanding to develop a formal working relationship. It is viewed as a mutually beneficial agreement. The new arrangement will provide the NIST with an opportunity to play a research and technology development role supporting the DHS mission and will allows the DHS to tap into the science and technology strengths as well as expertise that the NIST has in the area of security and technical standards.[94]

Department of Homeland Security's Science & Technology (S&T) Directorate

In addition to working more closely with the NIST, the *DHS's Science & Technology (S&T) Directorate* is tasked with organizing and leveraging R&D for the DHS. Universities, the private sector, and the federal laboratories are viewed as key DHS partners in this endeavor. DHS is also creating the *Homeland Security Advanced Research Projects Agency* (HSARPA) to jump-start and facilitate early research and development efforts to address critical needs in homeland defense on the scientific and technological front. The HSARPA will serve as the external funding arm of S&T and will release solicitations for research opportunities. The *Homeland Security Act* also mandates the creation of a 20-member *Science & Technology Advisory Committee*.[95]

The Defense Advanced Research Projects Agency (DARPA)

The *Defense Advanced Research Projects Agency* (DARPA) within the *Department of Defense* sponsors "revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their military uses."[96] While DARPA research and development in the CIIP arena is specifically focused on the security and reliability of US military networks, it often proves useful for networks in federal agencies as well as commercial systems. The DARPA utilizes a "layered approach" to cybersecurity (information assurance) research, taking a broad-based view. The DARPA has a number of methods for coordinating and disseminating the results of its research to other federal

93 http://csrc.nist.gov/.
94 http://www.dhs.gov/dhspublic/display?content=776.
95 http://www.dhs.gov/dhspublic/theme_home5.jsp.
96 Dr. Tony Tether, Director DARPA, statement to the Committee on Science, US House of Representatives, May 2003.

agencies and the commercial world. For example, the DARPA sponsors the *DARPA Information Survivability Conference and Exposition* (DISCEX), aimed at an audience that includes the extended research community, the operational military, developers of military systems, and the commercial industry that generates "off-the-shelf" systems that compose most military information systems.[97]

97 http://www.darpa.mil/body/newsitems/pdf/cyber.pdf.

Part IV
Analysis and Conclusion

Analysis and Conclusion

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

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

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

Analysis and Conclusion Part I: Country Surveys

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

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

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

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

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

Critical Sectors

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

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

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

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

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

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

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

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

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

Initiatives and Policy

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

In countries such as France, New Zealand, and Sweden, CIIP is mainly led by the defense establishment, whereas in other countries, such as the UK or Switzerland, approaches to CIIP are jointly led by the business community and public agencies. Furthermore, in Australia as well as the US and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role.

Many of the national CIIP efforts were triggered by the *Presidential Commission on Critical Infrastructure Protection* (PCCIP) set up by former US president Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000 (Y2K problem). This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included scenario work, the evaluation of a variety of measures, or assessments of early warning systems. These efforts resulted in policy statements – such as recommendations for the establishment of independent organizations dealing with information society issues – and reports laying down basic CIIP policies.

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

Organizational Overview

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

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

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

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

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

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

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

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

Public-private partnerships are becoming a strong pillar of CIIP policy. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. In Switzerland, the UK, and the US, strong links have already been established between the private business community and various government organizations.

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

Early Warning Approaches

The general trend in early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early-warning organizations are various forms of *Computer Emergency Response Teams* (CERTs), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents

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

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

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

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

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

General Thoughts

The need for assessment of CII is indisputable, and new vulnerabilities due to society's dependence on CII are acknowledged by all surveyed countries. In order to plan adequate and cost-effective protection measures, the working of these systems and their role for society should be sufficiently understood. But such an understanding is not at all given today, mainly because the complex behaviors of infrastructure networks present numerous theoretical and practical challenges for various stakeholders.

In addition, current methodologies for analyzing CII often prove to be insufficient. A lot of conceptual shortcomings become apparent when it comes to addressing the systems that have become vital to modern society, of which the major manifestation is the failure to understand interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic, security-related, and economic importance of CII.

Each of the methods and models used for the assessment of CII can only be applied to certain limited aspects of the problem, meaning that no single one is sufficient to address the whole range of CIIP issues. This requires a combination of different methodological elements, as shown in the patchwork application and multi-step approaches used in certain countries, such as Australia, Canada, or the Netherlands. Additionally, only few approaches have been developed for the purpose of analyzing CII specifically – most methodological elements originate in risk analysis.

Expert involvement in CII analysis is predominant, where an expert is usually a person closely familiar with the infrastructures in question. This means that crucial knowledge often resides in actors that are outside the state's direct sphere of influence. As a rule, this knowledge is not "academic", but generated directly for problem-solving. The pivotal role of academia in clarifying various crucial CIIP issues is only slowly evolving, and it may still take some time until CIIP issues gain ground in various disciplines.

Finally, CIIP efforts currently face one major problem: Protection is aimed at the present status of existing CII – and thus always lags one step behind. This is problematic as a lot of the challenges and problems are only just emerging, so that the system characteristics of future information infrastructures will differ fundamentally from traditional structures. Understanding them will require new analytical techniques and methodologies that are not yet available. Their development will, in turn, require great efforts in unconventional and forward thinking.

Sector Analysis

Sector analysis is a "grab-bag" label for approaches that aim to identify which aspects of the CI/CII are critical and why. They further the understanding of the working of sectors by highlighting important aspects such as the economic environment, underlying processes, stakeholders, or resources needed for crucial functions.

The choice of the "sector" as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry sectors. Many countries have followed the path-breaking and hugely influential example of the *Presidential Commission on Critical Infrastructure Protection* (PCCIP), which was the first official publication to equate critical infrastructures with business sectors or industries. This division also mirrors the fact that the majority of infrastructures is owned and operated by private actors and government officials acknowledge the need for partnerships between infrastructure owners and operators on the one hand and the government on the other.

However, the focus on sectors is far too artificial to represent the realities of complex infrastructure systems. For a more meaningful analysis, it is therefore necessary to evolve beyond the conventional 'sector'-based focus and to look at processes, functions, and services. This is done in the Netherlands, for example. Often, sector analysis is preparatory work for more in-depth analysis such as interdependency analysis and is also used to raise awareness of the CIIP problem among stakeholders.

Interdependency Analysis

Due to the explosive growth of information technology, the study of interdependencies and possible cascading effects in case of failures has become one of the most pressing, but least understood issues in CIIP. Most countries have so far approached the issue from qualitative, expert-based perspectives. These rough analyses of dependencies and interdependencies often aim to primarily determine the criticality of infrastructures or sectors. Often, this is done with the help of interdependency matrices that visualize the strength of interdependencies between sectors with different colors that represent values such as "high", "medium", "low", or "none". In this view, an asset is deemed the more critical the more interdependent it is.

Interdependencies serve as a benchmark for CII methods and models because the major shortcomings of present approaches become particularly apparent in their inability to cope with the problem of interdependencies. This is true for risk analysis methodologies as well as for technical security

models – in fact, for practically all of the approaches currently in use. What becomes abundantly clear is that it will be necessary to move beyond mere estimates of interdependencies, towards sophisticated modeling of cause-and-effect relationships and possible cascading failures.

A satisfactory set of metrics or models that can articulate the risk of failures, either due to natural causes or human-induced, for highly interdependent infrastructures will have to include a range of economic, social, and national-security considerations. This is particularly true because the importance of laws, regulations, policies, and other socio-political concerns to the infrastructure environment make it indispensable to study their impacts on interdependent infrastructures. The ideal way to approach the issue of interdependencies would therefore be a mix between qualitative and quantitative approaches. Additionally, to arrive at a broader understanding of interdependencies, we will require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, psychology, and sociology.

Risk Analysis

The majority of approaches used for CII analysis originate in risk analysis. The latter appears in a variety of forms, and some processes have been adapted specifically for the analysis of CI/CII. This is most likely due to the knowledge and experience that already exists in this field and has been applied by the engineering sciences to system analysis for decades.

Risk analysis could theoretically address any degree of complexity or size of system. When the boundaries of the evaluated system are set too wide, however, a lack of available data will make accurate assessment difficult or even impossible. For IT systems, there may be a very large number of approaches with a focus on information security. However, most of them are business-oriented and centered on organizational information systems, which does not make them applicable to larger systems.

Even though there are different methods of conducting a risk analysis, they often entail a very similar structure under which objects, threats, vulnerabilities, and probabilities are catalogued and links between them are defined. One of the main difficulties is that there are both theoretical and practical difficulties involved in estimating the probabilities and consequences of low-probability high-impact events – since no useful statistics for possible damage and failure probabilities exist. It also appears that there is no way of cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way. Risk analysis methodol-

ogy further fails to address interdependencies directly, which is a major shortcoming.

Additionally, there is a danger that risk analysis, especially because it is so well established and used in different communities, becomes a "false friend". Methodologies that have proven useful in the past are not necessarily good enough for the future. New sets of problems require new analytical tools. A fixation on quantifiable factors may be severely misleading.

Threat Assessment

Threat assessment can be seen as one part of risk analysis. In the risk analysis sense, threat assessment includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, when dealing with human actor-based threats such as terrorism, we are dealing with phenomena that are simply non-quantifiable and thus make traditional risk analysis aproaches obsolete.

Qualitative threat assessment has traditionally been very important in security policy. It is perceived by decision-makers today that the threat environment has changed substantially. Since the ability to estimate threats to critical infrastructure has been dependent upon the ability to evaluate the intent of an actor, coupled with the motivation and the capability to carry out the action, new problems arise with the advent of rapidly evolving and little-known cyberthreats, characterized by a number of elements that make them both difficult to predict and detect.

In general, threat assessment in connection with actor-centered research has been largely neglected in the field of CIIP. Many aspects of the threat appear unsubstantiated at a closer look: due to the lack of experience, statements on the scope of the danger often seem purely speculative. This could be resolved with more research into the changes in the threat environment and its impacts on CIIP.

Vulnerability Assessment

Vulnerability assessment can be seen as a specific step in the overall risk analysis methodology. It aims at identifying flaws in the design, implementation, or operation of critical infrastructures that make them susceptible to injury or attack, and attempts to determine the adequacy of security measures in place. Assessing the vulnerabilities of a relatively restricted IT-system such as a business network is far easier than doing the same on a higher system level.

Due to system complexity, it is likely that vulnerabilities and infrastructure disruptions will no longer be traceable in any useful way to single technical subsystems and vice versa.

There is much emphasis on vulnerability assessment in CIIP. However, it is easy to deceive oneself through over-confidence: when looking at relatively limited systems, many factors are known, and data may even be available. This may create a false sense of accuracy. However, very often the threat side of the equation is neglected in the process. This is a treacherous trend, because a vulnerability on its own does not represent a risk when there is no threat. Additionally, there is no certainty that potential malicious actors consider the same points as targets that we have identified as being vulnerable. Wrong assumptions, and hence wrong protection measures, are therefore one possible outcome of a misled vulnerability assessment.

Impact Assessment

There are few approaches to impact assessment. As one specific step within the whole risk analysis process, impact assessment aims to determine the impact resulting from a successful threat exercise of a vulnerability. The problem with current approaches to impact assessment is similar to the problems outlined above: when conducted for limited systems, i.e. IT-systems, consequences can be described in terms of loss or degradation of the IT-security objectives (integrity, availability, and confidentiality). However, when dealing with more abstract systems, measuring impacts becomes a major challenge. Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other major impacts, such as loss of trust, cannot be measured in specific units, but will have to be described qualitatively.

System Analysis

System analysis employs mathematical models and simulation tools to model various aspects of CII – mostly, their interdependent behavior. Existing efforts are not yet sufficient for modeling cascading failure in complex networks.

Developing a comprehensive architecture or framework for interdependency modeling and simulation is a major challenge. A comprehensive architecture or framework should be able to address all aspects of CIP/CIIP, mitigation, response, and recovery issues. Simply "hooking together" existing infrastructure models generally does not work, as the differences between

the models are too large. Furthermore, such models generally do not capture the characteristics of emergent behavior, a key element of interdependency analysis.

CIIP as Major Future Research Challenge

The differences in the state and quality of the protection practices in the fourteen studied countries are substantial. They are so great that we must even ask ourselves if we are perhaps comparing apples and oranges, especially in the view of the fact that "CIIP" is just one of many labels among many in use for the securing of information, and not even the most suitable term for what it wants to describe. The main problem with the term is the same as with its twin concept, "CIP": It originated in the technical context of limited or "closed systems", and is now used in the totally different context of networks and systems whose boundaries are no longer clearly discernible. When we add socio-political and cognitive dimensions to the equation, it becomes clear that we are dealing with a "new" problem that requires new analytical techniques and methodologies that are not yet available.

Maybe it is necessary to compare apples and oranges in a field that is still emerging. Whether "CIIP" will be the label that sticks remains to be seen. Despite the differences, a number of mutual key issues and major future challenges can be identified. Next to more or less well-discussed topics, such as the need for better public private partnerships, information-sharing concepts, or improved early-warning schemes, two issues have emerged that have received very little scholarly attention so far. The first is the apparent difficulty to distinguish between CIP and CIIP, the second deals with the implications of diverse viewpoints of what is "critical" for current and future protection practices. From both these points, and from our lack of understanding of complex interdependencies, arises an urgent future challenge for interdisciplinary research.

The need for more research into methodologies for the analysis of CII and CIIP is acknowledged. However, puzzles persist – such as the functioning of interdependencies; identifying what is critical to whom, when, and why; vulnerabilities and dispersions of disturbances; the influence of threat perceptions; or even the consequences of specific risks to the information infrastructure. Solving them requires an integrated set of methods and tools for analysis, assessment, protective measures, and decision-making. Research on interdependencies and cascading effects in case of failures is especially essential. Moreover, more research into the question of what is critical is

necessary, with a strong focus on the socio-political dimension, including terrorism research, while we must keep in mind that vulnerability-centered analyses that blend out the actor dimension are insufficient. There is a clear need for computer models for all protection phases – such as state-of-the-art-evaluation, the definition of potential improvements, assessment, and to some extent implementation and control.

This points to one fundamental issue and major challenge in terms of research: Only interdisciplinary approaches do sufficient justice to an issue that is *inherently* interdisciplinary due to its multifaceted nature. However, the question of CIIP and related topics has received little attention from large parts of academia up to now. Research is generally focused on aspects of IT-security, on the technical level, and on local or closed subsystems. These aspects are important – but they often miss crucial key features of the complex systems at hand and are inadequate for problem solution.

It is true that the putative new societal risks and vulnerabilities are directly or indirectly related to the development and utilization of new technologies. However, it is likely that critical vulnerabilities, and even the worst consequences of infrastructure disruptions, will not be traceable in any useful way to single technical subsystems – as a consequence of an already overwhelming complexity of open socio-political systems. Also, in view of the rapid technological developments constantly taking place, and the particular nature of their implementations, even if one carefully examines a relatively localized subsystem from the point of view of risks and threats, thereby identifying certain of its vulnerabilities, these insights can hardly be generalized and established in order to utilize them "beyond" the subsystem itself and on a higher system level.

Effective protection for critical infrastructures, therefore, calls for holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels as the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary R&D agenda encompassing fields ranging from engineering and complexity sciences to policy research, political science, and sociology.

Wrap-Up and Outlook

At present, open, pressing, but unanswered questions abound in the field of CIIP. As a result, there is not just one research gap – there is a research canyon to be filled with knowledge; and the research community is just beginning to single out the correct and the most important questions that need to be asked. Academia and practitioners will have to work hand in hand to resolve these issues, especially with the constant danger of being outpaced by the rapid developments. In such a dynamic field, the need to pinpoint the underlying urgent questions that are not subject to erratic change is a big challenge.

One such question concerns the role that states can and should play in CIIP, when the developments of the past decade have led many observers to assume that the forces driving global change are acutely undermining the state and its political agency. What is clear already is that any conception of security capable of dealing with the current world order needs to be linked to a much wider notion of governance than that which characterized the Cold War. In the realm of CIIP, governments are challenged to operate in unfamiliar ways, sharing influence with experts in the IT community, with businesses, and with nonprofit organizations, because the ownership, operation, and supply of the critical systems are in the hands of a largely private industry.

Furthermore, sharing of power with non-state actors is not the only difficult issue: Like other problems involving security, this one has global origins and implications, and its solution will ultimately require transnational institutions. But most states still focus on CIIP as a primarily *national* security issue, even though the (emerging) information infrastructure transcends many boundaries, and it is even possible that essential information services reside outside the nation-state. Effective (national) protection policies must therefore be backed by efforts in the international arena, such as an international regulatory regime for the protection of cyberspace.

As stated more than once in this Handbook, continuing efforts of CIIP policy evaluation and more research into CIIP matters are necessary. In order to stay abreast of the dynamics in the field, additional updates of the CIIP Handbook are planned. These updated versions will try to keep pace with developments in the various countries and on the international stage. It will be most fascinating to observe how the various policies evolve and "ripen" over the coming years.

Appendix

A1 Key Terms

Agent-Based Modeling

See →*Agent-Based Modeling and Simulation (ABMS)*.

Agent-Based Modeling and Simulation (ABMS)

Agent-based models are computer-driven tools to study the intricate dynamics of →*Complex Adaptive Systems;* those real-world systems in which very complicated behaviors emerge from the relatively simple, local interaction of many different individual components. The primary assumption in ABMS is that system behavior can be explained by individual traits, as the individuals interact and adapt to each other and their environment. In ABMs, complex interactions are emergent, whereas in other models the types of interactions must be foreseen and written into the model.[1]

Broad Risk Areas

The Australian PreDict approach[2] has developed industry →*Vulnerability Profiles* for ten sectors and focused on the critical interdependencies between them. The magnitude of the identified vulnerabilities was assessed and categorized into 12 groupings of →*Broad Risk Areas*, namely: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources), Operations (Training), and Flexibility/Adaptability. The majority of the Broad Risk Area titles were drawn from the analytical perspective resulting from a →*PEST* and →*Porter's Analysis*.

Cascading Effect

A cascading effect occurs when a condition in one section of an infrastructure system causes a fault that then, in turn, causes another fault somewhere else in the system, and then ripples across the sector or the whole system of complex infrastructures.

1 http://www.cas.anl.gov/.
2 http://www.defence.gov.au/predict/.

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 provide a basis for confirmatory empirical testing.

Computer Emergency Response Team (CERT)

CERTs are an integral part of current early warning efforts in all surveyed countries. They are established on the premise that any understanding of current security problems and potential solutions has to be derived from an analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities. Their role is to analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community. The first CERT (today, the CERT Coordination Center, or CERT/CC) was founded in 1988 and is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania.[3]

Common Criteria

The *Common Criteria for Information Technology Security Evaluation* (CC) defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing

3 http://www.cert.org/.

IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.[4]

Complex Adaptive Systems (CAS)

CAS are real-world systems that are characterized by apparently complex behavior, which emerges as a result of often nonlinear spatio-temporal interactions among a large number of component systems at different levels of organization.

Consequence

The consequences of an infrastructure disruption are sometimes also called →*Damage*, →*Harm*, or →*Impact*. Consequences usually entail either physical harm or injury that makes something less useful, valuable, or able to function; a harmful effect on somebody or something; or the cost or price of something.

Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) includes components such as telecommunications, computers/ software, the Internet, satellites, fiber optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows, as well as for that part of the global or national information infrastructure that is essentially necessary for continuity of the critical infrastructure services.

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, the Internet, satellites, fiber optics, etc., and on interconnected computers and networks and the services they provide.

4 http://www.commoncriteria.org/index.html.

Critical Infrastructure (CI)

Critical Infrastructure (CI) includes all systems and assets whose incapacitation or destruction would have a debilitating impact on 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 national security, and the economic and social well-being of a nation. CIP is more than CIIP, but CIIP is an essential part of CIP.

Criticality Matrix

Criticality, e.g. the criticality of processes, can be derived from the combination of effects and failure probability (see Table 2).

Failure Probability	Insignificant	Minor	Moderate	Major	Catastrophic
Virtually Certain	Significant	Significant	High	High	High
Probable	Intermediate	Significant	Significant	High	High
Possible	Low	Intermediate	Significant	High	High
Improbable	Low	Low	Intermediate	Significant	High
Highly Unlikely	Low	Low	Intermediate	Significant	Significant
	Effects/Degree of Damage				

Table 2: Assessment of Criticality

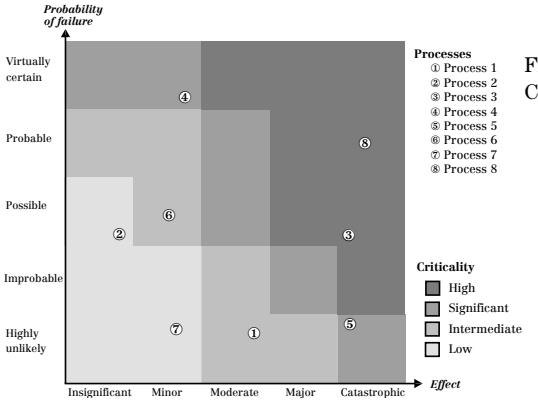
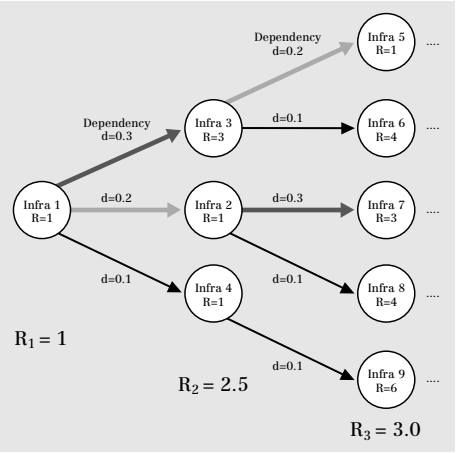


Figure 1:
Criticality Matrix for Processes[5]

5 Reinermann, Dirk and Joachim Weber. *Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)* Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt a.M., 29–30 September 2003).

The result of the criticality analysis can then be entered into the criticality matrix, which is a graphical representation of the failure mode and effects, usually graphed as the probability of occurrence vs. severity level.

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 2, the cumulative risk to Infrastructure 1 rises from 1 to 2.5 to 3.0 (etc.) as one goes into more depth.

Figure 2: Cumulative Risk Tree[6]

Damage

Damage is also called →*Harm*, →*Impact*, or →*Consequence*. It is manifested either as physical harm or injury that makes something less useful, valuable, or able to function; as a harmful effect on somebody or something; or as the cost or price of something.

Denial of Service (DoS)-Attack

A denial of service (DoS) attack is any attack that occupies enough of a limited resource to make the resource unusable for legitimate purposes. There are two types of DoS attacks: local and distributed.

6 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.

Distributed Denial of Service (DDoS)-Attack

A DDoS-Attack is a →*Denial of Service (DoS)-Attack* involving two or more machines. DDoS attacks entail breaking into hundreds or thousands of machines all over the Internet. Then the attacker installs DDoS software on them, allowing them to control all these stolen machines to launch co-ordinated attacks on victim's internet sites. These attacks typically exhaust bandwidth, CPU capacity, or other resources, breaking network connectivity to the victims.

Dependability

Dependability is the collective term used to describe availability performance and factors influencing it: reliability performance, maintainability performance, and maintainability support performance. The term "Dependability" is used only for general descriptions in non-quantitative terms.[7]

Dependency

Dependency may exist between two components, often within a sector. The term describes a specific, individual connection between two infrastructures, such as the electricity used to power a telecommunications switch. 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. 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.

7 http://www.asq-rd.org/depend.htm.

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 3: Dependency / Interdependency Matrix

Direct Vitality

Direct Vitality is the contribution that a product or service delivers to the continuity of the society, which is equivalent to the amount of direct (first-order) damage caused by a loss or serious disruption of the product or service.

Emergent Behavior

The idea behind emergent behavior is that from simple interactions and/or rules, complex behaviors can emerge at the group level that would not at the individual level. An emergent property is one that appears as the unpredictable result of the complex interactions of parts that themselves obey simple rules or laws.

Event Tree Analysis

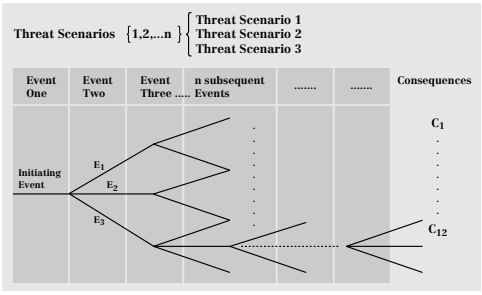


Figure 4: Event Tree (Source: Ezell, Farr, Wiese)

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 an exceedance 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 4 is an example of an event tree.

Expert Assessment / Interviews

A very effective way of getting information on various aspects of CII is to circulate a questionnaire among key persons and 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.

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 5).

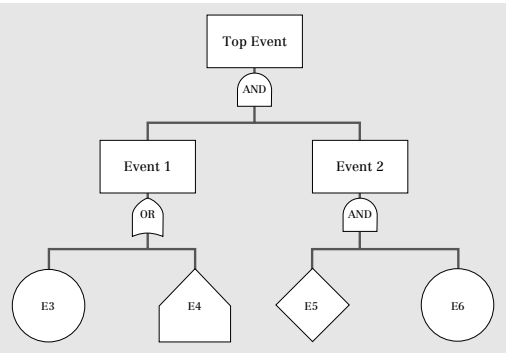


Figure 5: Example of a Simple Fault Tree

Harm

Harm to CI/CII is also called →*Damage*, →*Impact*, or →*Consequence*. It is either physical harm or injury that makes something less useful, valuable, or able to function; a harmful effect on somebody or something; or the cost or price of something.

Impact

The Impact of a disruption in CI/CII is also called →*Damage*, →*Harm*, or →*Consequence*. It manifests itself either as physical harm or injury that makes

something less useful, valuable, or able to function; as a harmful effect on somebody or something; as or the cost or price of something.

Impact Assessment

Impact assessment is one step within the whole risk analysis process that aims to determine the impact resulting from a successful threat exercise of a vulnerability. The grade of possible harm to an asset must be determined by a number of experts familiar with the assets, be they executives such as experts within the administration, asset owners, or asset managers.

Indicator

There are many definitions for the term "Indicator" in many different communities. It can be understood as a way of measuring, indicating, or identifying more or less exactly a sign, symptom, or index of a system.

Indirect Vitality

Indirect Vitality is the extent to which other vital products and services contribute to the dependability of the vital service or product

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.

Information Security Guidelines

Information Security Guidelines are suggested actions or recommendations to address an area of →*Information Security Policy*. A security guideline is not a mandatory action. However, Information Security Guidelines are considered best practices and should be implemented whenever possible.

Information Security Policy

Information Security Policy is an organizational document usually ratified by senior management. It aims to reduce the risk of, and minimize the effect (or cost) of, security incidents. It establishes the ground rules for the organization's information systems operations. The formation of an Information Security Policy is driven by many factors, the key part of which is →*Risk*.[8]

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.

Interdependency

An 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.

Interdependency Chart

See →*Dependency/Interdependency Chart*.

IT-Security Objectives

There are four basic IT-security objectives:[9]

(1) Availability (of systems and data for intended use only): Availability is required to assure that systems work promptly and service is not denied

8 http://www.yourwindow.to/information-security.

9 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.

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 a 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), and
- 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.

(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.

Logarithmic Scale

On a linear scale, the ratio of successive intervals is equal to "1". A logarithmic scale is different in that the ratio of successive intervals grows exponentially. Each interval on a logarithmic scale exceeds the previous interval by an order of magnitude. A typical ratio is 10, so that the marks on the scale read: 1, 10, 100, 1'000, 10'000, etc. Such a scale is useful if you are plotting a graph of values which have a very large range The logarithmic scale allows for much greater granularity at the lower end of the axis. Gradations in the scale for social and political impacts can also be set out. Social and political scales will be more subjective, using examples rather than number ranges.

Model

A model is a simplified representation of a system at some particular point in time or space, intended to promote understanding of the real system. System modeling is the process of describing both natural and engineered systems in precise mathematical terms. Thus, a model is a simplified representation of the real system intended to promote the development of understanding.

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 into 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*.

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 3 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 3: PEST Example

Porter's Analysis

Michael 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, or the threat of substitutes; supplier power, and buyer power. Figure 6 shows Porter's "five forces" model.

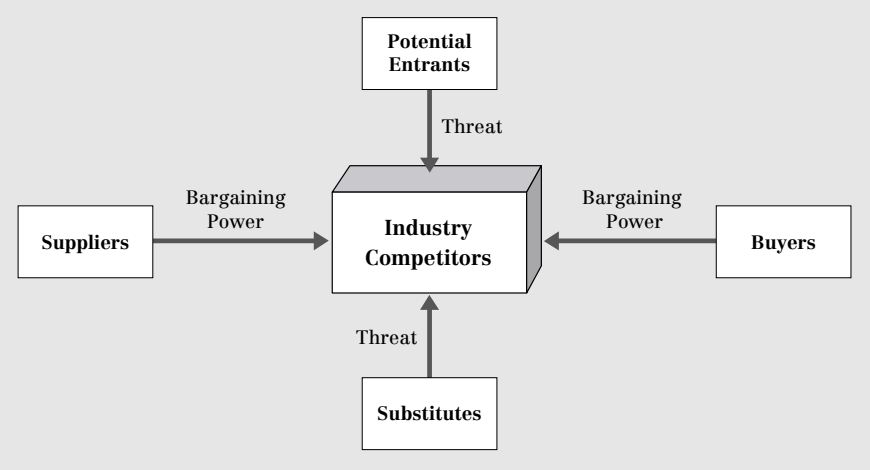


Figure 6: Porter's Five Forces Model

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.

Questionnaire

A Questionnaire is a set of specially designed questions to which answers are written on a pre-prepared form. Questionnaires are used in CIP/CIIP to get crucial information from stakeholders on issues such as products and services regarded vital, underlying processes and dependencies, or possible damage.

Risk

Risk is often defined quantitatively as a function of the *likelihood* of a given *threat source* displaying a particular potential *vulnerability*, and the resulting *impact* of that adverse event. However, risk sociologists have identified the importance of a third element: the ability of humans to influence both the probability of a risk occurring and the extent of the damage.

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 7).

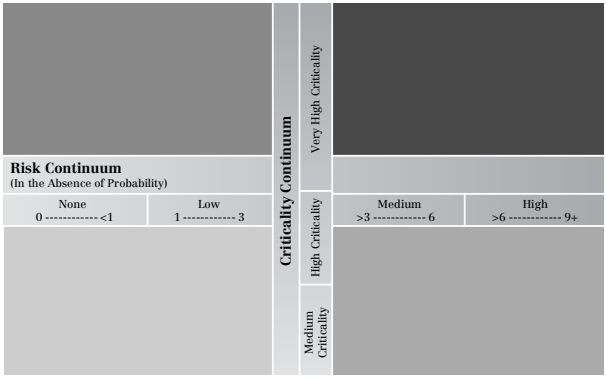


Figure 7: Risk/ Impact Scattergram

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 Analysis

Risk analysis is a systematic approach to gaining a more comprehensive assessment of risks that aims at bringing transparency into complexity and at addressing uncertainties or knowledge gaps. It supports risk management decisions and communication about risk. It is a procedure that helps to identify threats and vulnerabilities, analyze them to ascertain the exposures, and highlight ways in which the impact can be eliminated or reduced.

Risk Level Matrix

A risk level matrix is used in connection with a →*Risk Scale* to determine and describe the intensity of risk. It establishes a relationship between two categories (such as threat likelihood and impact) and multiplies the values assigned to each category (Figure 8).

		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: Risk Scale:		High > 50 - 100	Medium > 10 - 50	Low > 1 - 10

Figure 8:
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 9). This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructures.

Threat Assessment					
	High 3	0	3	6	9
	Medium 2	0	2	4	6
	Low 1	0	1	2	3
	None 0	0	0	0	0
		None 0	Low 1	Medium 2	High 3
		Vulnerability Assessment			

Figure 9: Basic Risk Rating Matrix

Risk Scale

A risk scale assigns numeric values to →*Categories* of risk, such as “high”, “medium”, or “low”. (See Figure 8).

Roundtable

A Roundtable is a discussion group for professionals in any industry who come together to discuss a number of issues.

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.[10]

Sector

a) One of the two divisions of the economy (private or public); b) a group of industries or infrastructures that perform similar functions within a society (e.g., vital human services)

Sector Analysis

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

Sector Model

Sector and layer models are mainly used as illustrations of how critical infrastructures are organized. They vary considerably from country to country

Seminar Games

Seminar gaming is an approach to understanding complex problems that capitalizes on the inherent expertise of groups of participants, who discuss complex topics by way of scenarios.

Simulation

A *Simulation* is the manipulation of a model in such a way that time or space are compressed, thus enabling one to perceive the interactions that would not

10 Cf. von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung.* (Wiesbaden, 1992).

otherwise be apparent because of their separation in time or space. Simulation is the exploitation of a model in order to predict logical consequences of hypothetical situations. A simulation is generally used to study the implications of the defined interactions of developed models running over time.

Sub-Sector

A sub-sector is the next smallest unit within a →*Sector*, often in terms of organizational standpoints or services delivered.

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 4 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 4: Typical SWOT Worksheet

System

A system can be a compound of several CI, a single infrastructure, an infrastructure-dependent enterprise, or a particular system within a given infrastructure, according to four hierarchy levels: 1) The system of systems; 2) individual infrastructures; 3) the individual system or enterprise; and 4) technical components.

System of Systems

The term "system of systems" has no clear and accepted definition, but the phenomenon is widespread and generally recognized. It can be seen as an emergent class of systems that are built from components which are large-scale systems in their own right (e.g., the energy system).

Threat Assessment

Threat assessment in the risk analysis context includes the determination of (1) the nature of external and internal threats, (2) their source, and (3) the probability of their occurrence, which is a measure of the likelihood of the threat being realized. However, when dealing with human actor-based threats such as terrorism, we are dealing with a "people business" that is intrinsically non-quantifiable – and thus poses significant problems for traditional risk analysis aproaches.

Values

See →*Categories*.

Vulnerability

Vulnerability can be understood as the collective result of risks and as 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 stable situation has been reached (see also →*Vulnerability Assessment*).

Vulnerability Analysis

See →*Vulnerability Assessment*.

Vulnerability Assessment

Vulnerability assessment is one step within risk analysis methodology. Its goal is to develop a list of vulnerabilities that could be exploited by a potential threat-source ("exposure analysis"). There are several sophisticated approaches to Vulnerability Assessment

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.

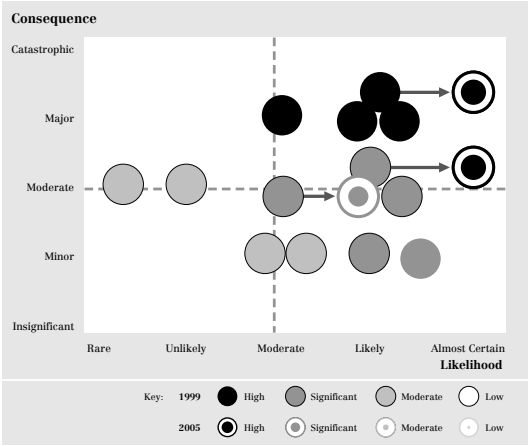


Figure 10: Vulnerability Profile Chart (Source: PreDICT)

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 11).

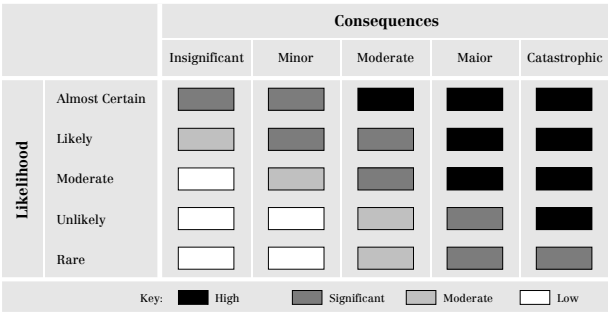


Figure 11:
Vulnerability Rating Table

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).
- Australia leaves the hack door open to cyber sabotage. *The Sydney Morning Herald*, 8 April 2003. http://www.smh.com.au/articles/2003/04/07/1049567603965.html.
- Brigitte 'in plot to blow up reactor'. *Australian Financial Review*, 12 November 2003. http://203.26.51.49/articles/2003/11/11/1068329561183.html.
- *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. *Australia's Vulnerability to Information Attack: Towards a National Information Policy*. Strategic and Defence Studies Centre, ANU, Working Paper, No. 306, 1997.
- Cobb, Adam. *Critical Infrastructure Attack: An Investigation of the Vulnerability of an OECD Country.* In: Information Operations. Bosch, J.M.J., Luiijf, H.A.M., Mollema, A.R (eds.). Netherlands Annual Review of Military Studies (NL ARMS) 1999. online version: http://www.tno.nl/instit/fel/refs/pub99/nlarms.html.
- 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).
- Email forces $25m Telstra credit. *The Australian*, 17 October 2003. http://www.theaustralian.news.com.au/common/story_page/0,5744,7587362%255E15306,00.html.

* This bibliography is a compendium of the literature used in the CIIP Handbooks 2002 and 2004. It does not claim to be comprehensive.

- 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).
- Gunaratna, R. *Inside Al Qaeda: Global Network of Terror* (Scribe: Melbourne, 2002).
- 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.
- National Counter Terrorism Plan. http://www.nationalsecurity.gov.au/www/nationalsecurityhome.nsf/AllDocs/RWPCD8501294925DA06CA256D42001C1A4C?OpenDocument.
- Rathmell, Andrew. Trip Note, Australian Business-Government Task Force on *Critical Infrastructure*, 26–27 March 2002.
- Ruddock silent on 'plot to attack reactor' claim. *Sydney Morning Herald*, 10 November 2003. http://www.smh.com.au/articles/2003/11/10/1068329468981.html.
- Storm on BigPond, users attack Telstra. *The Sydney Morning Herald*, 21 October 2003. http://www.smh.com.au/articles/2003/10/20/1066631346473.html?from=storyrhs.
- Telstra: $100m for Internet. *The Australian*, 28 October 2003. http://australianit.news.com.au/articles/0,7204,7687253%5e15346%5e%5enbv%5e15306-15316,00.html.
- Terrorists could radiate Sydney: Report. *The Bulletin Magazine*, 12 November 2003. http://news.ninemsn.com.au/National/story_8377.asp.
- Wenger, Andreas, Jan Metzger and Myriam Dunn (eds.). *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries (*Zurich: Center for Security Studies, 2002).

Austria

- Hollosi Arno. *Sicherheit mit offenen Standards für die Verwaltung* (Vienna 2002).
- Pankratz Thomas. "Information warfare – Eine Bedrohung der wired society". In: Gärtner, Heinz and Höll Otmar. *Comprehensive Security* (Vienna 2001).
- Resolution by the Austrian Parliament. *Security and Defence Doctrine: Analysis.* Draft expert report of 23 January 2001.
- Stabsstelle IKT-Strategie des Bundes. *Österreichisches IT-Sicherheitshandbuch* (Mai 2003). http://www.cio.gv.at/securenetworks/sihb.
- *Zivilschutz aktuell*, No. 4/ 1999; p. 13–19; Anfragebeantwortung 6111/ J XX. GP.

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.
- Harlick, J.E. "Understanding Critical Infrastructure Protection". Presentation at the *PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century.* Stockholm, 17–18 November 2003.

- 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.

Finland

- Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Finland* (Version April 2002).
- Finnish Communications Regulatory Authority (FICORA). *Annual Report 2001*. http://www.ficora.fi/2001/VV_vsk2001.pdf.
- Finnish Communications Regulatory Authority (FICORA). *Information Security Review related to the National Information Security Strategy* (May 2002). http://www.ficora.fi/englanti/document/review.pdf.
- Hagman, Rauni. "Finnish Communications Regulatory Authority (FICORA). ICT Security – Finland's Strategy and Action Plan". *International Northern eDimension* Forum, Pori, 11–12 November 2002. http://www.pori.fi/ned2002/esitykset/hagman_p.pdf.
- Information Society Advisory Board. *Finland as an Information Society. Report of the Information Society Advisory Board to the Government* (Helsinki 2000). http://www.vn.fi/vm/english/public_management/information_society.pdf.
- Ministry of Defence. *Finnish Security and Defence Policy 2001*. Report by the Government to Parliament on 13 June 2001. http://www.defmin.fi/index.phtml/page_id/13/topmenu_id/7/menu_id/13/this_topmenu/7/lang/3/fs/12.
- Ministry of Transport and Communications. *Finland in eEurope. Summary* (March 2001) http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2001/16en_tiivistelma.pdf.
- Proposal of the Advisory Committee for Information Security. *National Information Security Strategy Proposal* (25 November 2002). http://www.ficora.fi/englanti/document/infos.pdf.

France

- Dependability Development Support Initiative (DDSI). *Dependability Overview: National Dependability Policy Environments* (September 2002).
- Haut Comité Francais pour la Défense Civile. *Livre Blanc HCFDC: 20 ans*, *20 constats et propositions (*2003).
- Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical Guide – English Version, Version 1.02 (February 1997).
- Présentation des nouvelles orientations de l'Etat en sécurité des systèmes d'information. Séminaire DCSSI-AFNOR, 27 March 2003. http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.
- Service d'Information du Gouvernement. *Four years of Government measures to promote the information society* (August 2001). http://archives.internet.gouv.fr/francais//textesref/agsi4years.pdf.

Germany

- AG KRITIS. *Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS* (Entwurfsversion 7.95, Dezember 1999).
- *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.
- *Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002* (2nd Edition 2003). http://www.sachsen.de/de/bf/hochwasser/programme/download/Kirchbach_Bericht.pdf.
- 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.
- Bundesamt für Sicherheit in der Informationstechnik (BSI). *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit "Kritische Infrastrukturen in Staat und Gesellschaft"* (Januar 2002). http://www.bsi.de/literat/faltbl/kritis.pdf.
- 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 des Innern. *Co-ordination and Advisory Board of the Federal Government for Information Technology (KBSt). Berlin-Bonn Information Network (IVBB) (*November 2002). http://www.kbst.bund.de/Anlage303608/pdf_datei.pdf.
- 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". *KES Zeitschrift für Kommunikations- und EDV-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik (BSI) (Bonn, June 2001): pp. 35–41.
- Fischer, Wolfgang, Brigitta Krüger, Niels Lepperhoff, and 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". *Aus Politik und Zeitgeschichte* (vol. 10/11, 2002): pp. 31–39.
- 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". *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit* (January 2001). http://www.bsi.bund.de/.

- Kühn, Klaus Dieter. "Katastrophenresistente Infrastrukturen". *Bevölkerungsschutz (*vol. 4, 2001): pp. 46–47.
- *Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations*. Bundesgesetzblatt (Part 1, 21 May 2001): p. 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?". *politik-digital (*19 April 2001). http://www.politik-digital.de/text/netzpolitik/cyberwar/bundeswehr.shtml.
- Zentralstelle für Zivilschutz. *Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem* (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.

Italy

- Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. *Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana* (Ottobre 2003).
- Ministero per l'innovazione e le tecnologie. *Le politiche governative in tema sicurezza (*no date). http://securit.cineca.it/eventi/atti_290503/cilli.pdf.
- Minister for Innovation and Technologies. *The Government's guidelines for the development of the Information Society* (June 2002). http://www.innovazione.gov.it/eng/documenti/linee_guida_eng.pdf.
- Dependability Development Support Initiative (DDSI). *Dependability Overview: National Dependability Policy Environments* (2002).

The 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).
- 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).
- 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".*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.
- 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. "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).
- Ministerie van Defensie, *Defensienota 2000* (1999).
- Ministry of the Interior and Kingdom Relations. *The Netherlands*, *April 2003: Critical Infrastructure Protection in The Netherlands*.
- 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 (17 October 2000, Version 2.2).

New Zealand

- Cabinet Paper. *Centre for Critical Infrastructure Protection* (13 August 2001). http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.
- Department of the Prime Minister and Cabinet. *Security in the Government Sector* (2002). http://www.security.govt.nz/sigs/index.html.
- Domestic and External Security Secretariat. *Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies* (December 2000). http://www.dpmc.govt.nz/dess/securingoursafety/index.html.
- E-Government Unit, State Services Commission. *Protecting New Zealand's Infrastructure from Cyber-Threats* (8 December 2000). http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.
- E-Government Unit, State Services Commission. *Towards a Centre for Critical Infrastructure Protection* (11 June 2001). http:// www.ccip.govt.nz/about-ccip/ccip-final-report.htm.
- Minister of Defence. *The Government's Defence Policy Framework* (June 2000). http://www.executive.govt.nz/minister/burton/defence/index.html.

Norway

- Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Norway* (Version April 2002).
- Dependability Development Support Initiative (DDSI). *European Dependability Policy Environments*, *Country Report Sweden* (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 and the Norwegian Academy of Science and Letter, Centre for Advanced Study (June 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1074.doc.
- 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* (Oslo, 7 January 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).
- Ministry of Trade and Industry. *Information and Infrastructure Protection – a Norwegian View* (no date). http://www.ntia.doc.gov/osmhome/cip/workshop/norway.ppt.
- 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

- Coherent strategy for the society's information assurance (Sammanhållen strategi för samhällets IT-säkerhet, rapport Statskontoret rapportserie (1998).
- Security related to electronic identification (Säkerhet med elektronisk identifiering, rapport i Statskontorets rapportserie (1999).
- SEMA document 0160/2003. *Account of what measures that have been accomplished to take over the responsibilities from the working group on Information Operations* (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).
- 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". *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).
- Haefelfinger, Rolph L. "The Swiss Perspective on Critical Infrastructure". Presentation at the *PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century* (Stockholm, 17–18 November 2003).
- Informatikstrategieorgan Bund. *Einsatzkonzept Information Assurance Schweiz. Melde- und Analysestelle Informationssicherheit (MELANI)*, *Sonderstab Information Assurance (SONIA)*. Schlussbericht vom 30. November 2001 (Zollikon, 2001).
- InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen – Methodischer Leitfaden*, 2002.
- 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).
- OFCOM. *5th Report of the Information Society Coordination Group (ISCG) to the Federal Council* (June 2003).
- Rytz, Ruedi and Römer, Jürg. "MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age". *Workshop on Critical Infrastructure Protection (CIP)* (Frankfurt a. M., 29–30 September 2003). Available at http://www.isb.admin.ch.
- 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. "Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik".*NFP 42 Synthesis*, Nr. 11 (Bern, Schweizerischer Nationalfonds, 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 (Basel, 1997).
- *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.
- *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.

United Kingdom

- *Monthly Report from the e-Minister and e-Envoy* (3rd March 2003). http://www.e-envoy.gov.uk/oee/OeE.nsf/sections/reports-pmreports-2003/$file/3march03.htm.
- Parsons, T. J. "Protecting Critical Information Infrastructures. The co-ordination and development of Cross-sectoral research in the UK". *Plenary Adress at 'The Future of European Crisis Management* (Uppsala, Sweden, March 2001).
- Performance and Innovation Unit Report. *e-commerce@its.best.uk* (September 1999). http://www.cabinet-office.gov.uk/innovation/1999/ecomm.shtml.

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." *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* (28 November 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, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.
- Bush, George W. *Executive Order 13231. Critical Infrastructure Protection in the Information Age* (Washington, 16 October 2001). http://www.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 (Washington, 2000).
- Clinton, William J. *Executive Order 13010 on Critical Infrastructure Protection* (Washington, 15 July 1996). http://www.info-sec.com/pccip/web/eo13010.html.
- Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63* (Washington, 22 May 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.

- Clinton, William J. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities* (Washington, January 2001).
- *Cyber Security – Full Committee Hearing on Cyber Security – How Can We Protect American Computer Networks From Attack?* (Washington, 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, 22 May 2001). http://www.iwar.org.uk/cip/resources/gao/d01769t.pdf.
- Davis, John. *Research and Development for Critical Infrastructure Protection* (Washington, 5 September 1997). http://www.ciao.gov/resource/pccip/ac_randd.pdf.
- Erica B. Russell. "International and Interagency Critical Infrastructure Protection Coordination". Presentation at the *PfP Seminar on 'Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century* (Stockholm, 17–18 November 2003).
- 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, 17 October, 2001). http://www.iwar.org.uk/cip/resources/house-oct-17-01/.
- US Senate Committee on Governmental Affairs. *How Secure is Our Critical Infrastructure?* (Washington, 12 September, 2001). http://www.iwar.org.uk/cip/resources/senate-sep-12-01/.
- Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information. *Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center. (*Washington, 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.
- Marwick, Peat. *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, and Wayne A. Schroeder (eds.). *Use of Underground Facilities to Protect Critical Infrastructures, Summary of a Workshop* (National Academy Press: Washington, 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." *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).
- US Subcommittee on Oversight and Investigations Hearing. *Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?* (Washington, 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: 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: 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, October 1997).
- The White House. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.
- The White House. *The National Strategy to Secure Cyberspace* (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.
- 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, 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, 22 May 1998). http://www.cybercrime.gov/white_pr.htm.

Part II: CII Methods and Models

- Alberts, Christopher and Audrey Dorofee. *An Introduction to the OCTAVE Method.* http://www.cert.org/octave/methodintro.html.
- Alberts, Christopher and Audrey Dorofee. *OCTAVE Method Implementation Guide.* Version 2.0, Volumes 1–18 (Carnegie Mellon University, Juni 2001). http://www.cert.org/octave/pubs.html.
- Alberts, Christopher, Audrey Dorofee, James Stevens, and Carol Woody. *Introduction to the OCTAVE® Approach* (Carnegie Mellon University, August 2003). http://www.cert.org/octave/approach_intro.pdf.
- Barry, Ted. "Critical Information Infrastructure Protection in the United Kingdom". Paper presented at the *Critical Infrastructure Protection (CIP) Workshop* (Frankfurt a.M., 29–30 September 2003).
- Bellinger, Gene. *Modeling and Simulation: An Introduction.* Online at: http://www.systems-thinking.org/modsim/modsim.htm.
- Bundesamt für Sicherheit in der Informationstechnik. *IT Baseline Protection Manual. Standard Security Safeguards.* Updated July 2001. http://www.bsi.de/gshb/english/menue.htm.
- Center for Strategic Leadership, U.S. Army War College. *Issue Paper August 2003.* Volume 06-03. http://www.iwar.org.uk/cip/resources/csl-awc/nisac.pdf.
- 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.
- Commonwealth of Australia, Information Security Group. *Australian Communications-Electronic Security Instruction 33 (ACSI 33) Handbook 3, Risk Management.* Draft Version downloadable at: http://www.dsd.gov.au/_lib/pdf_doc/acsi33/HB3p.pdf.
- Emergency Management Australia. Critical Infrastructure Emergency Risk Management and Assurance Handbook (Mt Macedon, January 2003). http://www.disaster.qld.gov.au/publications/pdf/ Critical_Infrastructure_handbook.pdf.
- Gran, Bjørn Axel. *The CORAS Methodology for Model-Based Risk Assessment.* Version 1.0, WP2, Deliverable 2.4 (29 August 2003).
- 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 Defense Research Establishment (United Kingdom, 1–3 September 1999). http://www.isn.ethz.ch/crn/extended/workshop_zh/Norway_Tel.pdf.
- Haimes, Yacov Y. *Risk Modeling, Assessment, and Management* (New York: Wiley Publications, 1998).
- InfoSurance. *InfoSurance Fokus.* November 2002. http://www.infosurance.ch/de/pdf/fokus_2.pdf.
- InfoSurance, Wirtschaftliche Landesversorgung, Informatikstrategieorgan Bund. *Sektorspezifische Risikoanalysen: Methodischer Leitfaden* (no date, no place).

- KPMG / National Support Staff. *Predict Defence Infrastructure Core Requirements Tool (PreDICT)*. http://www.defence.gov.au/predict/general/predict_fs.htm.
- Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (eds.). *EICAR Conference Best Paper Proceedings 2003*. http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.
- 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.
- 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).
- 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).
- Marwick, Peat. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office* (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf.
- Ministry van Binnenlandse Zaken en Koniknrijksrelaties. *Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services*. April 2003.
- National Contingency Planning Group. *Canadian Infrastructures and their Dependencies* (March 2000).
- New South Wales Office of Information and Communications Technology's (OICT). *Information Security Guideline for NSW Government – Part 1 Information Security Risk Management*. Issue No: 3.2. (First published: September 1997, current version: June 2003).
- New South Wales Office of Information and Communications Technology's (OICT). *Information Security Guideline for NSW Government – Part 2 Examples of Threats and Vulnerabilities*. Issue No: 2.0. First published: September 1997, current version: June 2003).
- New South Wales Office of Information and Communications Technology's (OICT). *Information Security Guideline for NSW Government – Part 3 Information Security Baseline Controls*. Issue No: 3.0. (First published: September 1997, current version: June 2003).
- Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets*. DRAFT (19 December 2002).
- Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Threat Analysis*. Number: TA03-001, 12 March 2003. http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.
- Office of the Auditor General of Canada. *1999 Report of the Auditor General of Canada, September and November, Chapter 25: Preparedness for Year 2000, Final Preparation*. http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9925ce.html.
- Pfister, Ivo. "Round Tables InfoSurance: Sektorspezifische Risikoanalyse. Einführung und Methodische Grundlagen". *Luzerner Tage für Informationssicherheit LUTIS* (Juni 2003). www.infosurance.ch/lutis/vortraege/ methodische_grundlagen.pdf.
- Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*. Technical Guide – English Version, Version 1.02. February 1997.
- President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures (*Washington, D.C., October 1997).

- Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the *Critical Infrastructure Protection (CIP) Workshop* (Frankfurt a.M., 29–30 September 2003).
- Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. "Complex Networks. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control Systems Magazine* (Vol. 21, 6, December 2001): pp. 11–25.
- Schmitz, Walter. *ACIP D6.4 Comprehensive Roadmap – Analysis and Assessment for CIP*. Work Package 6, Deliverable D6.4, Version 1 (European Commission Information Society Technology Programme, May 2003).
- Standards Australia / Standards New Zealand. Risk Management AS/NZS 4360:1999 (Strathfield, 12 April 1999).
- 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.
- Stromquist, Walter R. *Uses and Limitations of Risk Analysis*. Prepared for the Royal Commission on the Ocean Ranger Marine Disaster Risk Analysis Seminar, 1 May 1984. http://www.chesco.com/~marys/ORanger.htm.
- US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology*. 28 September 2001. http://www.esisac.com/publicdocs/assessment_methods/OEA_VA_Methodology.pdf.
- US Department of Energy, Office of Energy Assurance. *Vulnerability Assessment Methodology. Electric Power Infrastructure*. DRAFT. September 2002. http://www.esisac.com/publicdocs/assessment_methods/VA.pdf.
- Varnado, Sam. "Modeling and Simulation for Critical Infrastructures – Status and Future Issues". Paper presented at the *Critical Infrastructure Protection (CIP) Workshop* (Frankfurt a.M., 29–30 September 2003).
- Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security*. Information & Security: An International Journal, Volume 7 (2001): pp. 67–79.
- Yates, Athol. *Engineering a Safer Australia: Securing Critical Infrastructure and the Built Environment (*Institution of Engineers, Australia, June 2003). http://www.ieaust.org.au/SafeAustralia/Engineering%20a%20Safer%20Aust.pdf.
- Zimmermann, D., *The Transformation of Terrorism. The "New Terrorism," Impact Scalability and the Dynamic of Reciprocal Threat Perception*, ed. Andreas Wenger, *Züricher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 67* (Center for Security Studies, Zurich: 2003).

Miscellaneous

- 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.fas.org/irp/offdocs/eo/eo-13231.htm.
- Buzan, Barry, Ole Wæver, and Jaap de Wilde. *Security: A New Framework for Analysis* (Boulder: Rienner, 1998).

- Clinton, William J. *Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue*. Version 1.0 (Washington, 2000).
- Clinton, William J. *Executive Order 13010 on Critical Infrastructure Protection* (Washington, 15 July 1996). http://www.info-sec.com/pccip/web/eo13010.html.
- Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63* (22 May 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.
- Dunn, Myriam. *Information Age Conflicts: A Study on the Information Revolution and a Changing Operating Environment.* Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung, No. 64 (Zurich: Center for Security Studies, 2002).
- Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (Eds.). *EICAR Conference Best Paper Proceedings 2003.*
- Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.). *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford University Press: Oxford, forthcoming 2004).
- Moteff, John, Claudia Copeland, and John Fischer. *Critical Infrastructures: What Makes an Infrastructure Critical?* CRS (Congressional Research Service) Report for Congress RL31556 (30 August 2002). http://www.fas.org/irp/crs/RL31556.pdf.
- Mussington, David. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development* (Santa Monica: RAND, 2002).
- Parsons, T.J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross-Sectoral Research in the UK." *Plenary Address at the Future of European Crisis Management* (Uppsala, Sweden, March 2001).
- President's Commission on Critical Infrastructure Protection (PCCIP). *Critical Foundations: Protecting America's Infrastructures* (Washington, D.C., October 1997).
- Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security.* Information & Security: An International Journal, Volume 7, 2001.
- Wenger, Andreas, Jan Metzger and Myriam Dunn (eds.). *The International CIIP Handbook: An Inventory of Protection Policies in Eight Countries* (Zurich: Center for Security Studies, 2002).
- Wenger, Andreas, Jan Metzger and Myriam Dunn. "Critical Information Infrastructure Protection: Eine sicherheitspolitische Herausforderung". In: Spillmann, Kurt R. and Andreas Wenger (eds.) *Bulletin zur Schweizerischen Sicherheitspolitik* (Zürich: Center for Security Studies, 2002): pp. 119–142.
- Westrin, Peter. "Critical Information Infrastructure Protection". In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security.* Information & Security: An International Journal, Volume 7 (2001): pp. 67–79.

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 High Tech Crime Centre (AHTCC) (http://www.ahtcc.gov.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)
- Predict Defence Infrastructure Core Requirements Tool (PreDICT) (http://www.defence.gov.au/predict/)
- Prime Minister of Australia (http://www.pm.gov.au)
- Stratwise Strategic Intelligence (www.stratwise.com)
- Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) (http://www.cript.gov.au/)

Austria

- Chief Information Office Austria (http://www.cio.gv.at)
- Bundesministerium für Inneres/Ministery of Internal Affairs (http://www.bmi.gv.at/)
- Computer Incident Response Co-ordination Austria (CIRCA) (http://www.circa.at/index.html)
- Bundeskanzleramt (http://www.bka.gv.at)
- Zentrum für sichere Informationstechnologie Austria (A-SIT) (http://www.a-sit.at)

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)

Finland

- National Emergency Supply Agency (NESA) (http://www.nesa.fi.)
- Finnish Communications Regulatory Authority (FICORA) (http://www.ficora.fi)

- CERT-FI (http://www.ficora.fi/englanti/tietoturva/certfi.htm)
- Finnish Information Society Development Center (http://www.tieke.fi)
- Finnish Government (http://www.valtioneuvosto.fi/vn/liston/base.lsp?k=en)
- eFinland (http://e.finland.fi/)
- Ministry of Defence (http://www.defmin.fi)

France

- Club de la Sécurite des Systèmes d'Information Français (CLUSIF) (https://www.clusif.asso.fr/en/clusif/present/)
- Computer Emergency Response Team (CERTA) (http://www.certa.ssi.gouv.fr/)
- Computer Emergency Response Team Industry, Services, and Trade (CERT-IST) (http://www.cert-ist.com)
- Direction for Security of Information Systems (DCSSI) (http://www.ssi.gouv.fr/fr/dcssi/index.html.)
- National Network of Telecommunications for Technology, Education, and Research (GIP RENATER) (http://www.renater.fr/)
- Security of Information Systems (SSI) (http://www.ssi.gouv.fr/fr/index.html.)
- Strategic Advisory Board on Information Technologies (CSTI) (http://www.csti.pm.gouv.fr)

Germany

- Arbeitskreis Schutz von Infrastrukturen/ German Group on Infrastructure Protection (AKSIS) (http://www.aksis.de)
- BKAonline – Bundeskriminalamt Wiesbaden/Federal Law Enforcement Agency (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 (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)
- German Emergency Preparedness Information System (deNIS) (http://www.denis.bund.de)
- German Ministry of the Interior (http://www.bmi.bund.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)
- Regulatory Agency for Telecommunications and Posts (http://www.regtp.de/en/index.html)
- 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)
- Technisches Hilfswerk (THW) (http://www.thw.de/english/)

International Organizations

- Analysis and Assessment for Critical Infrastructures Protection (ACIP) (http://www.iabg.de/acip/index.html)
- COevolution and Self-organisation In dynamical Networks (COSIN) (http://www.cosin.org/)
- Cyber Tools On-Line Search for Evidence (http://www.ctose.org)
- eEurope Standards (http://www.e-europestandards.org)
- EU Forum on Cybercrime (http://cybercrime-forum.jrc.it/default/)
- EU-funded CORAS project (http://coras.sourceforge.net/)
- European Commission Directorate-General's Joint Research Centre (JRC) (http://www.jrc.org)
- European Telecommunications Standards Institute (http://www.etsi.org/eeurope/home.htm)
- Information Society Website of the European Union (http://europa.eu.int/information_society/index_en.htm)
- Sixth Framework Programme of the European Commission (http://europa.eu.int/comm/research/fp6/index_en.html)

Italy

- Dipartimento di Informatica e Comunicazione/Department of Informatics and Communications (http://www.dico.unimi.it/)
- Incident Response Italy (www.iritaly.org.)
- Italian Association for Security in Informatics (http://www.clusit.it/indexe.htm)
- Minister for Innovation and Technologies (http://www.innovazione.gov.it/eng/)
- Ministry of Communication (http://www.comunicazioni.it/en)
- National Centre for Informatics in the Public Administration (CNIPA) (http://www.cnipa.gov.it)
- Polizia di Stato (http://www.poliziadistato.it/pds/english/)

The Netherlands

- Binnenlandse Veiligheidsdienst (BVD) (National Intelligence and Security Agency) (http://www.fas.org/irp/world/netherlands/bvd.htm)
- Branchevereniging van Nederlandse Internet Providers/Consortium of Dutch Internet Providers (NLIP) (http://www.nlip.nl)
- Directoraat-Generaal Telecommunicatie en Post (http://www.minvenw.nl/dgtp/home/)
- Government-wide Computer Emergency Response Team (GOVCERT.NL) (http://www.govcert.nl)
- INFODROME (http://www.infodrome.nl)
- KWINT (http://www.kwint.org)
- Ministerie van Verkeer en Waterstaat (http://www.minvenw.nl)
- Ministry of the Interior and Kingdom Relations (http://www.minbzk.nl)
- NLIP – Branchevereniging van Nederlandse Internet Providers (http://www.nlip.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)
- Waarschuwingsdienst (http://www.waarschuwingsdienst.nl)

New Zealand

- Security policy and guidance website (www.security.govt.nz)
- Standards New Zealand (www.standards.co.nz)
- Centre for Critical Infrastructure Protections (http://www.ccip.govt.nz)
- Ministry of Defence (http://www.defence.govt.nz)
- Cabinet (http://www.executive.govt.nz)
- Government Communications Security Bureau (http://www.gcsb.govt.nz)
- Department of the Prime Minister and Cabinet (http://www.dpmc.govt.nz)
- State Services Commission (http://www.ssc.govt)
- New Zealand Computer Society (http://www.nzcs.org.nz)
- Australian Computer Emergency Response Team (AusCERT) (http://www.auscert.org.au)
- Co-logic (http://www.cologic.co.nz)

Norway

- Center for Information Security (SIS) (http://www.norsis.no/indexe.php)
- Direktoratet for Sivilt Beredskap (DSB) (http://www.dsb.no)
- Ministry of Trade and Industry (http://odin.dep.no/nhd/engelsk/)
- National Telecommunications and Information Administration (http://www.ntia.doc.gov)
- Nasjonal sikkerhetsmyndighet (http://www.nsm.stat.no/index.html)
- 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 Defensce Material Administration (FMV) (http://www.fmv.se)
- Swedish Defense Research Agency (http://www.foi.se/english/)
- Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se/english/index.jsp)
- Swedish IT Incident Centre (SITIC) (http://www.sitic.se)
- Swedish National Defense College (http://www.fhs.se)
- Swedish National Defensce Radio Establishment (FRA) (http://www.fra.se/english.shtml)
- 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, ETH Zurich (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 (http://www.vbs.admin.ch/internet/GST/AIOS/e/index.htm)
- Federal Office for Communication (BAKOM) (http://www.bakom.ch/en/index.html)
- Federal Office for National Economic Supply (BWL) (http://www.bwl.admin.ch/)
- Federal Office for Police (FOP) (http://internet.bap.admin.ch)
- Federal Office of Information Technology, Systems and Telecommunication (BIT) (http://www.informatik.admin.ch)
- Federal Strategy Unit for Information Technology (ISB) (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)
- Swiss Coordination Unit for Cybercrime Control (CYCO) (http://www.cybercrime.admin.ch)
- Symposium on Privacy and Security (http://www.privacy-security.ch)

United Kingdom

- Cabinet Office (http://www.cabinet-office.gov.uk)
- Communications-Electronics Security Group (http://www.gchq.gov.uk/about/cesg.html)
- Communications-Electronics Security Group (http://www.gchq.gov.uk/about/cesg.html)
- Department of Trade and Industry (http://www.dti.gov.uk)
- Home Office (http://www.homeoffice.gov.uk)
- Information Assurance Advisory Council (IAAC) (http://www.iaac.org.uk/start.htm)
- MI5 The Security Service (http://www.mi5.gov.uk)
- National Infrastructure Security Co-ordination Centre (NISCC) (www.niscc.gov.uk)
- Office of the e-Envoy (http://www.e-envoy.gov.uk/Home/Homepage/fs/en)
- Strategy Unit (http://www.strategy.gov.uk)
- UK Online (http://www.ukonline.gov.uk/Home/Homepage/fs/en)
- Unified Incident Reporting and Alert Scheme (UNIRAS) (http://www.uniras.gov.uk)

United States

- Center for Democracy and Technology (http://www.cdt.org)
- Computer Emergency Response Team (CERT) (http://www.cert.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
- Office of Science and Technology Policy (http://www.ostp.gov/)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (http://www.cert.org/octave/)
- 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)
- US Department of Homeland Security (http://www.dhs.gov)
- White House (http://www.whitehouse.gov)

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 List of Experts*

Australia

- Adam Cobb, Director Stratwise Strategic Intelligence
- Ivan Timbs, National Office for the Information Economy (NOIE)

Austria

- Otto Hellwig, Former Official of the Federal Chancellery
- Thomas Pankratz, Austrian Federal Ministry of Defence, Bureau for Security Policy
- Gerald Trost, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic of Austria

Canada

- Louise Forgues, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
- Jacques L. Grenier, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
- Shannon Hiegel, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
- Colin Knight, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
- Dan Lambert, Solicitor General
- Paul Pagotto, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

Finland

- Markku Haranne, Ministry of the Interior, Rescue Services Unit
- Ilkka Kananen, National Emergency Supply Agency (NESA)
- Veli-Pekka Kuparinen, National Emergency Supply Agency (NESA)
- Mika Purhonen, National Emergency Supply Agency (NESA)

France

—

* This list includes experts involved in both the 2004 and the 2002 editions of the International CIIP Handbook.

Germany

- Thomas Beer, Industrieanlagen-Betriebsgesellschaft (IABG)
- Ralph Bendrath, Political Scientist
- Jörn Brömmelhörster, Consultant
- Susanne Jantsch, Consultant
- Dirk Reinermann, Federal Office for Information Security (BSI)
- Stefan Ritter, Federal Office for Information Security (BSI)
- Christine Scharz-Hemmert, Industrieanlagen-Betriebsgesellschaft (IABG)
- Willi Stein, Federal Office for Information Security (BSI)

Italy

- Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment (ENEA)
- Giovanna Dondossola, CESI
- Roberto Setola, Working Group for Critical Information Infrastructure Protection

The Netherlands

- Roland de Bruin, KWINT, ECP.nl
- Eric Luiijf, TNO Physics and Electronics Laboratory

New Zealand

- Mike Harmon, Centre for Critical Infrastructure Protection (CCIP)

Norway

- Cort Archer Dreyer, Ministry of Trade and Industry
- Havard Fridheim, Norwegian Defence Research Establishment (FFI)
- Arthur Gjengstö, Secretary to the Norwegian Commission on the Vulnerability of Society
- Stein Henriksen, Directorate for Civil Protection and Emergency Planning (DSB)
- Kjetil Sørli, Directorate for Civil Protection and Emergency Planning (DSB)
- Roger Steen, Directorate for Civil Protection and Emergency Planning (DSB)

Sweden

- Henrik Christiansson, Swedish Defence Research Agency (FOI)
- Georg Fischer, Swedish Defence Research Agency (FOI)
- Jan Lundberg, Swedish Emergency Management Agency (SEMA)
- Lars Nicander, Swedish National Defence College
- Sara Siri, Swedish Emergency Management Agency (SEMA)
- Peter Stern, Swedish Emergency Management Agency (SEMA)
- Peter Wallström, Cell Network
- Peter Westrin, FOI, Swedish Defence Research Agency
- Manuel W. Wik, Swedish National Defence College

Switzerland

- Michel Dufour, Dufour Consulting
- Kurt Haering, Former Managing Director InfoSurance Foundation
- Ueli Haudenschild, Federal Office for National Economic Supply
- Marc Henauer, Federal Office of Police/DAP
- Thomas Köppel, Former Official of the Federal Office of Police
- Anton Lagger, Federal Office for National Economic Supply
- Ruedi Rytz, Federal Strategy Unit for Information Technology (ISB)
- André Schmid, Managing Director InfoSurance Foundation

United Kingdom

- Ted Barry, National Infrastructure Security Coordination Centre (NISCC)
- Stephen Cummings, National Infrastructure Security Coordination Centre (NISCC)
- John Park, National Infrastructure Security Coordination Centre (NISCC)

United States

- Scott C. Algeier, US Chamber of Commerce
- John A. McCarthy, Critical Infrastructure Protection Project, George Mason University School of Law
- Emily Frye, Critical Infrastructure Protection Project, George Mason University School of Law

NATO

- Silla A. Jonsdottier, NATO Headquarters