Appendix

A1 Glossary of Key Terms

Categories

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

Causal Mapping

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

Cluster Analysis

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

Critical Information Infrastructure (CII)

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

Critical Information Infrastructure Protection (CIIP)

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

Critical Infrastructure (CI)

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

Critical Infrastructure Protection (CIP)

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

Cumulative Risk Assessment

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

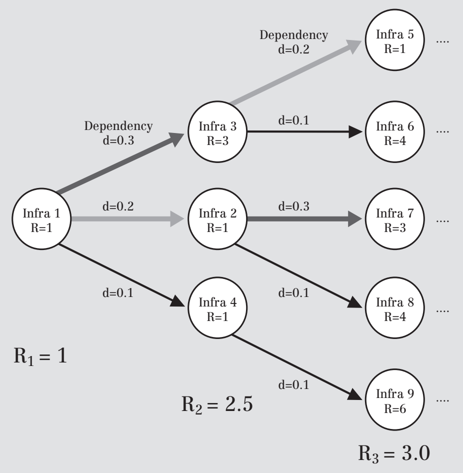


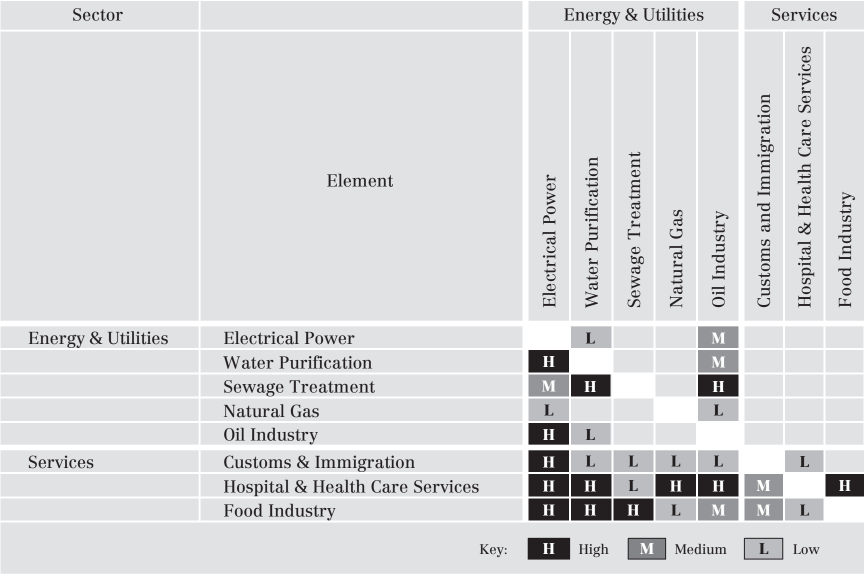
Figure 1: Cumulative Risk Tree (Source: Presentation by J. Grenier)

Dependency

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

Dependency/Interdependency Matrices

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



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

Key: H High M Medium L Low

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

Event Tree Analysis

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

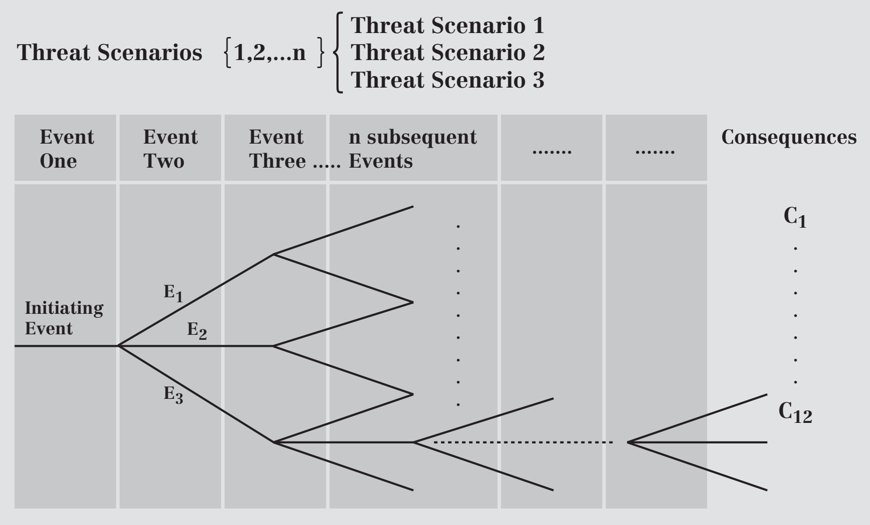


Figure 3: Event Tree (Source: Ezell, Farr, Wiese)

Expert Assessment/ Interviews

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

Factor Analysis

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

Fault Tree Analysis

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

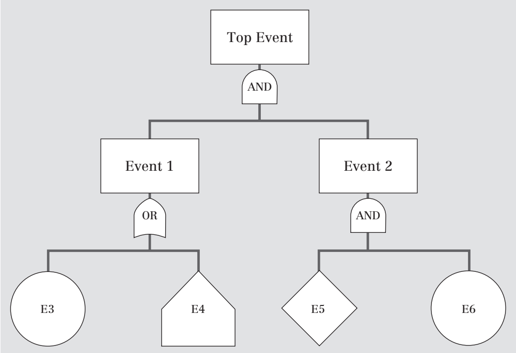


Figure 4: Example of a Simple Fault Tree

Hierarchical Holographic Modeling (HHM)

The HHM methodology takes into consideration the fact that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge. Each of these models may focus on a specific aspect, yet all may be regarded as acceptable representations of the infrastructure system. Therefore, HHM builds a family of models that address different identified aspects of the systems. Central to the HHM method is a particular form of diagram, as shown in Figure 5. The different columns in the diagram reflect different "perspectives" on the overall system.

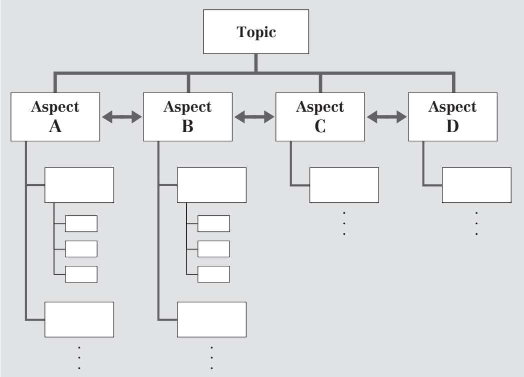


Figure 5: HHM Framework (Source: Y.Y. Haimes)

Information and Communication Technologies (ICT)

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

Infrastructure

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

Infrastructure Profiles (IPs)

Infrastructure profiles such as the one developed by the National Contingency Planning Group (Canada) include a number of characteristics of certain infrastructures, such as description of the infrastructure, statistics, maps, contacts, references, jurisdictions, and a detailed analysis of the interdependencies.

Interdependency

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

IT-Security Objectives

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

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

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

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

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

(3) Confidentiality of data and system information:

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

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

(4) Accountability (to the individual level):

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

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

Layer Model

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

Multi-Criteria Decision Approach

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

Multi-Criteria Model

See →*Multi-Criteria Decision Approach*; →"National Efforts for CII Analysis: Norway".

Multi-Objective Trade-off Analysis

The Multi-Objective Trade-off Analysis is closely linked to the →*Multi-Criteria Decision Approach* as it is based on the assumption that problems are characterized by multiple, non-commensurate, and often conflicting, objectives. It is used to identify this hierarchy of objectives and to avoid comparing and trading off objectives that belong to different levels. Ultimately, the goal is to present a number of alternatives. The decision-maker reviews the results and then makes a qualitative decision on system safety or security.

Partitioned Multi-objective Risk Method (PMRM)

The PMRM is a risk analysis method for solving multi-objective problems of a probabilistic nature. Instead of using the traditional expected value of risk, the PMRM generates a number of conditional expected-value functions, which represent the risk (given that the damage falls within specific damage ranges). It is therefore used to identify the risk of extreme and catastrophic events. This not only allows a decision-maker to see the expected value of damage, but adds understanding of low probability/ high-damage events.

Process and Technology Analysis

One of the methodological elements of the InfoSurance CIIP framework. It helps to identify critical infrastructure sectors dependencies on information infrastructure and across multiple sectors. (→"Models for CII Analysis: Process and Technology Analysis; →"National Efforts for CII Analysis: Switzerland").

Qualitative and Quantitative Risk Assessment

A *quantitative* risk assessment expresses threat likelihood, impact, and risk in terms of a numeric value, whereas a *qualitative* assessment uses ratings such as "high", "medium", or "low" to express the value. The major advantage of the quantitative approach is that it is precise and provides a measurement that can be fed directly into a cost-benefit analysis. Many approaches today start out by using qualitative rankings ("high", "medium", or "low") and attribute a range of values to each.

Risk

Risk is the net negative impact of an event/incident, considering both the probability and the impact of occurrence.

Risk/Impact Scattergram

When assessing impact of incidents, a scattergram plotting the relative rated criticality of the infrastructure elements (increasing from bottom to top) against their relative risk value (increasing from left to right) can be used (Figure 6).

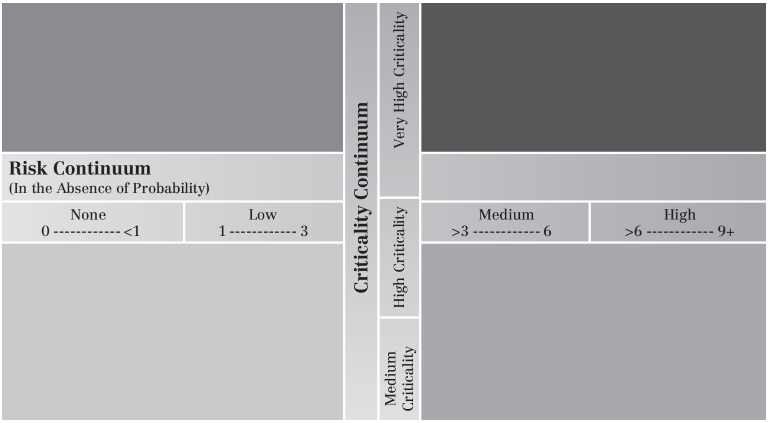
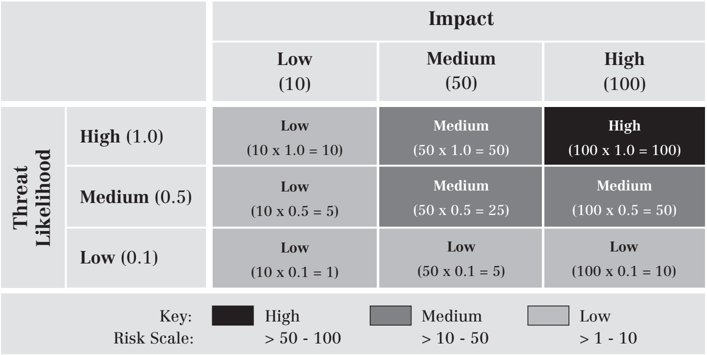


Figure 6: Risk/ Impact Scattergram (Source: Speech by J. Grenier)

This creates four quadrants in which crucial elements of a sector (e.g. communication satellites or telecom systems for the communications sector) can be positioned. This is a way to show which element needs special attention.

Risk Level Matrix

A risk level matrix is used in connection with a →*Risk Scale* to determine and describe the intensity of risk. It relates two categories (such as threat likelihood and impact) and multiplies assigned values to each category (Figure 7).



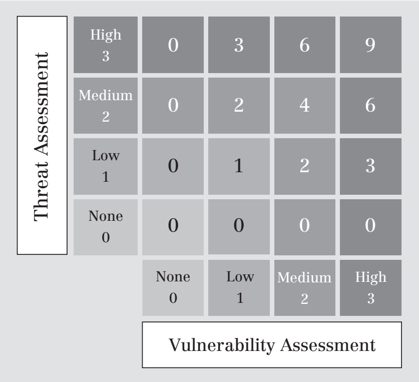
		Impact		
		Low (10)	**Medium** (50)	**High** (100)
Threat Likelihood	**High** (1.0)	**Low** (10 x 1.0 = 10)	**Medium** (50 x 1.0 = 50)	**High** (100 x 1.0 = 100)
	Medium (0.5)	**Low** (10 x 0.5 = 5)	**Medium** (50 x 0.5 = 25)	**Medium** (100 x 0.5 = 50)
	Low (0.1)	**Low** (10 x 0.1 = 1)	**Low** (50 x 0.1 = 5)	**Low** (100 x 0.1 = 10)

Key: Risk Scale:	■	High > 50 - 100	▨	Medium > 10 - 50	□	Low > 1 - 10

Figure 7: Typical Risk Level Matrix

Risk Rating Matrix

After the evaluation of threat and vulnerability for single components of an infrastructure element, risks can be determined based on a matrix that multiplies the assigned values for threat and vulnerability (Figure 8). This method allows for a comparison of relative risks between components of an infrastructure element, between layers in the infrastructure model, and between infrastructures.



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 8: Basic Risk Rating Matrix

Risk Scale

A risk scale assigns numeric values to → *Categories* of risk, such as “high”, “medium”, “low”. (See Figure 7).

Scenarios/ Scenario Technique

The scenario technique enables the generation of scenarios that serve to determine strategies in order to control or at least influence the unknown developments of complex systems as favorably as possible with regard to own objectives and interests. There are various techniques and even software tools to develop scenarios.[2]

Sector Analysis

Sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects of the sector. (→”Methods and Models to Analyze CII: Sector Analysis”).

[2] Cf. von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung.* (Wiesbaden, 1992).

Sector Model

Sector and layer models are mainly used as illustrations for how critical infrastructures are organized. They vary considerably from country to country (→”Methods and Models to Analyze CII: Sector and Layer Models”; →”National Efforts for CII Analysis: Switzerland”).

Seminar Games

Seminar gaming is an approach to understanding complex problems that capitalizes on the inherent expertise of groups of participants, which discuss complex topics by way of scenarios.[3]

Values

See →*Categories.*

Vulnerability

Vulnerability can be understood as the collective result of risks and the ability of a society, local municipal authority, company or organization to deal with and survive external and internal emergency situations. The vulnerability analysis covers a long-term perspective and gives focus to a sequence of events from the moment an emergency situation occurs until a new stabile situation has been reached (see also →*Vulnerability Assessment*).

Vulnerability Analysis

See →*Vulnerability Assessment.*

Vulnerability Assessment

There are two different understandings of vulnerability assessment:

1) Vulnerability assessment can be a step in risk analysis methodology. Its goal is to develop a list of vulnerabilities that could be

[3] Cf. Strategic Leadership Exercise “Informo 2001”, conducted by the Strategic Leadership Training in cooperation with Ernst Basler + Partner AG, http://www.admin.ch/ch/e/bk/sfa/sfa/rueckblick.html

exploited by a potential threat-source ("exposure analysis"). There are several sophisticated approaches to Vulnerability Assessment (→"National Efforts for CII Analysis: Australia"; →"National Efforts for CII Analysis: United States").

2) A second approach sees vulnerability as the collective result of risks and the ability of a society, local municipal authority, company, or organization to deal with and survive external and internal emergency situations. Vulnerability assessment is thus not part of risk analysis, but a combination of risk analysis and emergency management evaluation.[IV]

Vulnerability Profile Chart

A vulnerability profile chart visually represents vulnerability rankings, often with a focus on interdependencies. Each profile may represent a single sector. The vulnerability ranking is done in order to compare and contrast vulnerabilities between sectors. One possible approach is the definition of "risk areas" in order to group vulnerabilities into common areas for analysis. (→"National Efforts for CII Analysis: Australia"). (Example Figure 9)

Vulnerability Rating Table

Vulnerability is sometimes defined as a function of likelihood and consequences. Through the separate analysis of each, the vulnerabilities can be rated using the product of the "Consequence" and the "Likelihood" ratings, displayed as a rating table (Figure 10).

[IV] Cf. Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. Vulnerability Analysis and Auditing of Municipalities (Lund University Centre for Risk Assessment and Management (LUCRAM)): 15–17. http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

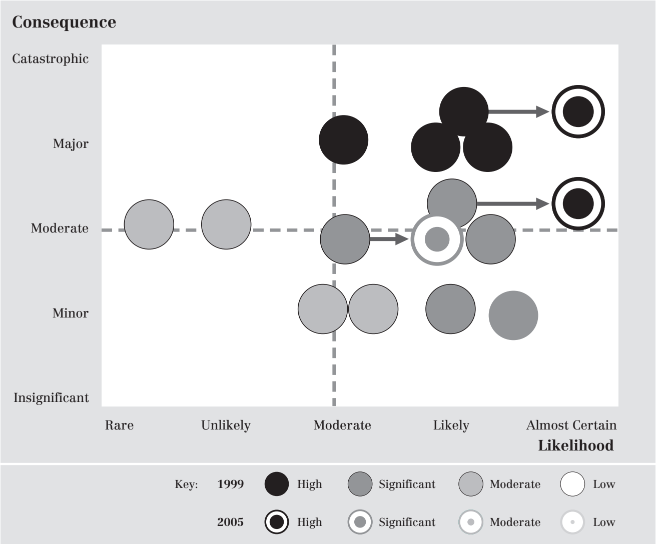


Figure 9: Vulnerability Profile Chart (Source: PreDICT)

		Consequences				
		Insignificant	Minor	Moderate	Maior	Catastrophic
Likelihood	Almost Certain	▩	▩	■	■	■
	Likely	▒	▩	▩	■	■
	Moderate	□	▒	▩	■	■
	Unlikely	□	□	▒	▩	■
	Rare	□	□	▒	▩	▩

Key: ■ High ▩ Significant ▒ Moderate □ Low

Figure 10: Vulnerability Rating Table

A2 Bibliography

Australia

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

Budget 2001–2002 (Fact Sheet): Protecting the National Information Infrastructure: Part of the Government's E-security Initiative. http://www.asio.gov.au/Media/Contents/protecting%20NII.htm

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

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). *E-Commerce beyond 2000*. (Canberra, 2000). http://www.iwar.org.uk/e-commerce/resources/au/beyond2k_final_report.pdf

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). *A Strategic Framework for the Information Economy. Identifying Priorities for Action*. (Canberra, December 1998).

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

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

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

Etter, Barbara. "The Australasian Policing Response to Electronic Crime". *Australasian Centre for Policing Research to the FBI Global Economic Threats Conference*. (FBI Academy, Quantico, Virginia (USA), July 9–13, 2001).

KPMG / National Support Staff. *Critical Infrastructure Project. Phase 2. Information Technology Report*. Predict Defence Infrastructure Core Requirements Tool (PreDICT). (April 2000). http://www.defence.gov.au/predict/segments/it/pdf/it_full.pdf

Rathmell, Andrew. *Trip Note*, *Australian Business-Government Task Force on Critical Infrastructure*, 26–27 March 2002.

Canada

Canadian Security Intelligence Service (CSIS). *Protection of the Canadian Critical Infrastructure*. (17 July, 2001).

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

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

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

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

"National Critical Infrastructure Protection Program". In: *Memo Quarterly Newsletter*. (Yukon Government and Emergency Preparedness Canada, vol. 7, Winter 2001).

ÖCB (ed.). *International CEP Handbook: Civil Emergency Planning in the NATO/EACP Countries 1999-2000*. (Stockholm, 2000).

Purdy, Margaret. *Cyber-Sabotage for Government. Speech at the Ottawa Congress Centre*. (Ottawa, 20 February, 2001). http://www.ocipep.gc.ca/pub_communi/speeches/cybersabotage_e.html

Germany

Act on the Protection of Personal Data Used in Teleservices. (Teleservices Data Protection Act – Teledienstedatenschutzgesetz, TDDSG) 22 July, 1997, amended last by Article 3 of the Bill on Legal Framework Conditions for Electronic Commerce.

Act on the Utilization of Teleservices. (Teleservices Act – Teledienstegesetz TDG) 22 July, 1997, amended last by Article 1 of the Bill on Legal Framework Conditions for Electronic Commerce.

Bewig, Frank. *Schutz kritischer Infrastrukturen in Deutschland: Kooperationen zwischen Staat und Privatwirtschaft*. (Semesterarbeit im Seminar "Militär- und Sicherheitspolitik im technologischen Wandel". (Berlin, September 2000). http://userpage.fu-berlin.de/~bendrath/hausarbeiten/kritis-D.rtf

Blattner-Zimmermann, Marit. “Kritische Infrastrukturen im Zeitalter der Informationstechnik”. *Seminar on Information Warfare.* (Lucerne, 22 November, 2001).

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

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

Bundesministerium für Bildung und Forschung. “Online – Offline: IT in Education”. *Innovationen Wissensgesellschaft.* (August 2000).

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

Ennen, Günther. “CERT-Bund – eine neue Aufgabe des BSI”. In: *KES Zeitschrift für Kommunikations- und EDV-Sicherheit*. Bundesamt für Sicherheit in der Informationstechnik (BSI). (Bonn, June 2001): 35–41.

Fischer, Wolfgang, Brigitta Krüger, Niels Lepperhoff, Regina Eich. *Was treibt die Entwicklung des Internet voran?* Programmgruppe Systemforschung und Technologische Entwicklung (STE). (Jülich, August 2001).

Hutter, Reinhard. “Cyber-Terror: Risiken im Informationszeitalter”. In: *Aus Politik und Zeitgeschichte* (vol. 10/11, 2002): 31–39.

Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS. (December 1999). http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html

Jantsch, Susanne. “Critical Infrastructure Protection in Germany”. *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/jantsch/sld001.htm

“Kritische Infrastrukturen in Staat und Gesellschaft”. In: *BSI-Kurzinformationen zu aktuellen Themen der IT-Sicherheit.* (January 2001). http:/www.bsi.bund.de/

Kühn, Klaus Dieter. “Katastrophenresistente Infrastrukturen”. In: *Bevölkerungsschutz.* (vol. 4, 2001): 46–47.

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations. Bundesgesetzblatt. (Part 1, 21 May, 2001: 876, Unofficial version for industry consultation).

Möhring, Michael. *Informationsgesellschaft.* (Universität Koblenz-Landau: Institut für Wirtschafts- und Verwaltungsinformatik, 2001).

Welzel, Carolin. “Vom Kalten Krieg zum Cyberwar: eBusiness, eGovernment – eWar?”. In: *politik-digital*. (19 April, 2001). http://www.politik-digital.de/text/netzpolitik/cyberwar/bundeswehr.shtml

Netherlands

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

Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs. *Internet Vulnerability*. (July 2001).

Evers, Joris. “The Netherlands adopts cybercrime pact”. In: *CNN.com*. (30 November, 2000). http://www.cnn.com/2000/TECH/computing/11/30/dutch.cybercrime.idg/

House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.

Infodrome. *De Overheid in de Informatiesamenleving: Mission September 1999*. (September, 1999). http://www.infodrome.nl/english/missie_eng.html

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

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

Luiijf, Eric. “Information Assurance and the Information Society”. In: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (Eds.). *EICAR 1999 Best Paper Proceedings*. (Aalborg, 1999).

Luiijf, Eric. “Information Assurance under Fire”. *Information Assurance and Data Security*, *SMI conference*. (London, 2–3 February, 2000).

Luiijf, Eric. “Netherlands Defense Information Operations Policy”. *Seminar on Information Warfare*. (Lucerne, 22 November, 2001).

Luiijf, Eric, M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet*. (The Hague, 2001).

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

Ministerie van Defensie, *Defensienota 2000*, (1999).

Stratix / TNO-FEL. *The Reliability of the Netherlands Internet: Consequences and Measures.* Report of Project Phase 3: Review of International Activities and Possible Actions. (English translation of "De Betrouwbaarheid van het Internet: Gevolgen en Maatregelen. Project KWINT – Rapportage Fase 3. (October 17, 2000, Version 2.2).

Norway

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

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

Hagen, Janne Merete, Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System.* Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defence Research Establishment. (United Kingdom, 1-3 September, 1999).

Henriksen, Stein. "National Approaches to CIP Norway". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Henriksen/sld001.htm

Hovden, Jan. *Public Policy and Administration in a Vulnerable Society.* Norwegian University of Science and Technology (NTNU). (Oslo).

Jervas, Gunnar, Ian Dennis, Richard Conroy (Eds.). *New Technology as a Threat and Risk Generator. Can Countermeasures Keep up with the Pace?* (Stockholm, March 2001).

Krohn Devold, Kristin. *The Government's Defence Challenges and Priorities. The Defence Minister's New Year Address to the Oslo Military Society, January 7, 2002. (Oslo, 2002).* http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010011-090053/index-dok000-b-n-a.html

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

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

Ministry of Justice and Police. *Statement on Safety and Security of Society.* Report No. 17 to the Storting (2000-2001).

Ministry of Trade and Industry. *Society's vulnerability due to its ICT-dependence.* (Abridged version of the main report, Oslo, October 2000).

Nicander, Lars. "The Swedish Initiative on Critical Infrastructure Protection" *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/nicander/sld001.htm

Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. *Vulnerability Analysis and Auditing of Municipalities.* (Lucram: Lund University). http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

Norges offentlige utredninger. (2000:24) *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Statens forvaltningstjeneste Informasjonsforvaltning. (Oslo, 2000).

Svendsen, Per-Kare. *Internet Rights Country Report – Norway.* (January 2000). http://www.apc.org/english/rights/europe/countries/norway.html

Sweden

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

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

The Swedish ICT Commission. *Basic Protection in Computer Hardware and Software. The Observatory for Information Security.* (2001).

The Swedish ICT Commission. *General Guide to a Future-Proof IT Infrastructure. Observatory for IT Infrastructure. Report 37/2001.* (Stockholm, 2001).

Wallstrom, Peter. "Methods for Infrastructure Protection". *MIS Training, InfowarCon '99.* (London, 1999).

Weissglass, Gösta (Ed.). "Planning a High-Resilience Society". *Papers and Proceedings from the Lövånger Symposium*, 18–20 August 1993. (Umeå, 1994).

Wik, Manuel W. "The Swedish Commission on Vulnerability and Security. Under Leadership of Special Investigator Åke Pettersson". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/Wik_135/sld001.htm

Switzerland

Bircher, Daniel. “Informationsinfrastruktur – Verletzliches Nervensystem unserer Gesellschaft”. In: *Neue Zürcher Zeitung*, 7 *July, 1999.*

Carrel, Laurent F. *Bericht des Projektleiters über die Strategische Führungsausbildung (SFU) 97.* (Bern, 1 July, 1998).

Generalsekretariat VBS (Ed.). *Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz.* (Draft, Bern, August 1999).

Groupe de Réflexion. *Für eine Informationsgesellschaft in der Schweiz. Zuhanden des Schweizerischen Bundesrates.* (Bern, June 1997).

Informatikstrategieorgan Bund. *Einsatzkonzept Information Assurance Schweiz. Melde- und Analysestelle Informationssicherheit (MELANI), Sonderstab Information Assurance (SONIA).* Schlussbericht vom 30. November 2001 (Zollikon: Ernst Basler + Partner AG, 2001).

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

Koordinationsgruppe Informationsgesellschaft (KIG). *Konzept “Information Assurance”.* (Bern, May 2000).

Rytz, Ruedi. *Sonderstab Information Assurance – ein paar Gedanken.* (Bern, 11 September, 2001).

Schweizerische Bundeskanzlei. *Information Assurance: Die Verletzlichkeit der schweizerischen Informationsgesellschaft.* (Bern, 19 May, 1998).

Schweizerische Bundeskanzlei. *INFORMO 2001: Strategische Führungsausbildung.* Dokumentation für Teilnehmende und Medienschaffende. (Bern, 2001).

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

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

Sibilia, Ricardo. “Informationskriegführung. Eine schweizerische Sicht”. *Institut für militärische Sicherheitstechnik (IMS).* (Nr. 97–6, Zurich, 1997).

Spillmann, Kurt R.; Libiszewski, Stefan; Wenger, Andreas; et al. “Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik”. In: *NFP 42 Synthesis, Nr. 11. Schweizerischer Nationalfonds*, Bern, 1999). http://www.snf.ch/nfp42/public/resume/rspillmanninfo_d.html

Strategy of the Federal Council for an Information Society in Switzerland. (Bern, 18 February, 1998).

Trappel, Josef. *Informationsgesellschaft Schweiz – Bestandesaufnahme und Perspektiven.* Europäisches Zentrum für Wirtschaftsforschung und Strategieberatung. (Prognos, Basel, May 1997).

United States

Belcher, Tim, Elad Yoran. *Internet Security Threat Report: Attack Trends for Q3 and Q4 2001.* (Alexandria, January 2002).

Bendrath, Ralf. "Critical Infrastructure Protection in the United States". *ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead.* (Zurich, 8–10 November, 2001). http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/bendrath/sld001.htm

Brown, Evelyn. "Energy Systems Expertise is Key to Critical Infrastructure Center." In: *Logos* (No 17, vol. 2, Fall 1999). http://www.anl.gov/OPA/logos17-2/infra2.htm

Buehring, Bill. *Natural Gas Security Issues Related to Electric Power Systems.* (November 28, 2001). http://wpweb2k.gsia.cmu.edu/ceic/presentations/Buehring.pdf

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

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

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

Clinton, William J. *Executive Order 13010 on Critical Infrastructure Protection.* (Washington, D.C., 15 July, 1996). http://www.info-sec.com/pccip/web/eo13010.html

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

Clinton, William J. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities.* (The White House, Washington, D.C., January 2001).

Cyber Security – Full Committee Hearing on Cyber Security – How Can We Protect American Computer Networks From Attack? (Washington, D.C., Wednesday, 10 October, 2001). http://www.iwar.org.uk/cip/resources/house-oct-10-01/

Dacey, Robert F. *Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities, before the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary.* GAO-01-769T (Washington, D.C., 22 May, 2001). http://www.iwar.org.uk/cip/resources/gao/d01769t.pdf

Davis, John (President's Commission on Infrastructure Protection). *Research and Development for Critical Infrastructure Protection*. (Washington, D.C., 5 September, 1997). http://www.ciao.gov/resource/pccip/ac_randd.pdf

Fisher, R., J. Peerenbaum. "Interdependencies: A DOE Perspective". *16th Annual Security Technology Symposium & Exhibition. Session IV: Infrastructure Interdependencies: The Long Pole in the Tent.* (Williamsburg, Virginia, 28 June, 2000).

Fisher, Ron, Jim Peerenbaum. "Lessons Learned from Industry Vulnerability Assessments and September 11th". *US Department of Energy Assurance Conference.* (Arlington, 12–13 December, 2001).

Government Electronics and Information Technology Association (GEIA). *Information Assurance and Critical Infrastructure Protection: A Federal Perspective.* (2001).

House Science Committee: *October 17, 2001 – Full Committee Hearing on Cyber Terrorism – A View From the Gilmore Commission.* (Washington, D.C., 17 October, 2001). http://www.iwar.org.uk/cip/resources/house-oct-17-01/

How Secure is Our Critical Infrastructure? U.S. Senate Committee on Governmental Affairs. (Washington, D.C., 12 September, 2001). http://www.iwar.org.uk/cip/resources/senate-sep-12-01/

Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center. Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information. (Washington, D.C., 25 July, 2001). http://www.iwar.org.uk/cip/resources/nipc-oversight/hr072501st.htm

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

KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office*. (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf

League, Sarah Jane. "Critical Infrastructure Assurance Office: Protecting America's Infrastructures". *InfowarCon '99.* (London, 1999).

Legal Information Institute. *Code Collection. Sec. 1001. – Statements or entries generally.* http://www4.law.cornell.edu/uscode/18/1001.html

Little, Richard G., Paul B. Pattak, Wayne A. Schroeder (Eds.). *Use of Underground Facilities to Protect Critical Infrastructures, Summary of a Workshop.* (National Academy Press: Washington, D.C., 1998).

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

Moteff, John D. *RL30153: Critical Infrastructures: Background and Early Implementation of PDD-63.* (Updated 12 September, 2000). http://www.cnie.org/nle/crsreports/science/st-46.cfm

National Information Infrastructure. Risk Assessment: A Nation's Information at Risk. (Executive Summary, January 1999). http://www.ncs.gov/n5_hp/N5_IA_HP/HTML/RVWG/niirisk.htm (no longer available)

Office of the Undersecretary for Defense. *Protecting the Homeland – Report of the Defense Science Board Task Force on Defensive Information Operations 2000 Summer Study.* (Executive Summary, vol. I, March 2001). http://www.acq.osd.mil/dsb/protecting.pdf

Oversight hearing on Information Technology – Essential Yet Vulnerable: How Prepared Are We for Attacks. Subcommittee on Governmental Efficiency, Financial Management and Intergovernmental Relations. (26 September, 2001). http://www.iwar.org.uk/cip/resources/house-sep-26-01/witnesses.htm

Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." In: *Computer Security Issues & Trends.* (vol. 1, 2001).

Proceedings of the Infrastructure Interdependencies Research and Development Workshop. Hosted by the Department of Energy, Office of Critical Infrastructure Protection, and the White House, Office of Science and Technology Policy. (Mc Lean, 12–13 June, 2000).

Protecting America‘s Critical Infrastructures: How Secure Are Government Computer Systems? US Subcommittee on Oversight and Investigations Hearing. (Washington, D.C., 5 April, 2001). http://energycommerce.house.gov/107/action/107-13.pdf

Ryan, Julie. *The Infrastructure of the Protection of the Critical Infrastructure.* (1998). http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm

Sandia National Laboratories. *Modeling of Interdependencies. Critical Infrastructure Surety.* http://www.sandia.gov/Surety/Facts/Modeling.htm

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

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

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

The Department of Homeland Security. *Information Analysis and Infrastructure Protection.* http://www.whitehouse.gov/deptofhomeland/sect6.html

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

United States General Accounting Office (GOA). *Critical Infrastructure Protection: Significant Challenges in Developing Analysis*, *Warning*, *and Response Capabilities.* (GAO-01-323, 25 April, 2001).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. (USA PATRIOT ACT) ACT OF 2001. http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf

US Critical Infrastructure Assurance Office. *Practices for Securing Critical Infrastructure Assets.* (Washington, D.C., January 2000). http://www.iwar.org.uk/cip/resources/prac.pdf

White Paper on PDD-63. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. (Washington, D.C., 22 May, 1998). http://www.cybercrime.gov/white_pr.htm

CII Methods and Models

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

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

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

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

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

Commonwealth of Australia. *Example of Risk Assessment*. http://www.dsd.gov.au/infosec/acsi33/HB3A.html

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

Ernst Basler + Partner AG. *Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb. Leitfaden* (on behalf of the German Federal Ministry of Transport) (Zollikon, 1996).

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

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

Fraser, B. (ed.) *RFC2196 Site Security Handbook. The Internet Engineering Task Force (IETF) Network Working Group*. (September 1997). http: //www.ietf.org/rfc/rfc2196.txt

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

Hagen, Janne Merete, Håvard Fridheim. *Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System*. Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defence Research Establishment. (United Kingdom, September 1–3, 1999).

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

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

Hutter, Reinhard. "Cyber-Terror: Risiken im Informationszeitalter". In: *Aus Politik und Zeitgeschichte*. (vol. 10/11, 2002): 31–39.

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

KPMG / National Support Staff. *Critical Infrastructure Project. Phase 2. Information Technology Report.* Predict Defence Infrastructure Core Requirements Tool (PreDICT). (April 2000). http://www.defence.gov.au/predict/segments/it/pdf/it_full.pdf

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

KPMG, Peat Marwick. *Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office*. (October 1998). http://www.ciao.gov/resource/vulassessframework.pdf

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

Luiijf, Eric, M. Klaver, J. Huizenga. *The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet*. (The Hague, 2001).

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

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

Masera, Marcelo, Wilikens, M. "Interdependencies with the Information Infrastructure: Dependability and Complexity Issues". *Conference Paper at the 5th International Conference on Technology, Policy, and Innovation.* (Ispra, 26-29 June, 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1168.doc.

Maurer, Daniel. *Evaluation of the Integrated Complexity Management Instrument (ICI) for Generating Global Scenarios*. (Bern, June 2001). http://www.isn.ethz.ch/crn/basics/process/documents/ici_rapport_e.pdf

Merz, Hans, Thomas Schneider, and Hans Bohnenblust. *Bewertung von technischen Risiken. Beiträge zur Strukturierung und zum Stand der Kenntnisse. Modelle zur Bewertung von Todesfallrisiken* (Zürich: vdf Verlag der Fachvereine Zürich, 1995).

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

Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin, Bo Lenntorp. *Vulnerability Analysis and Auditing of Municipalities*. (Lucram: Lund University). http://www.isn.ethz.ch/crn/basics/process/documents/vulnerability.pdf

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

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

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

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

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

Stratix / TNO-FEL. *The Reliability of the Netherlands Internet: Consequences and Measures. Report of Project Phase 3: Review of International Activities and Possible Actions*. (English Translation of "De Betrouwbaarheid van het Internet: Gevolgen en Maatregelen. Project KWINT – Rapportage Fase 3. (October 17, 2000, Version 2.2). http://www.tno.nl/instit/fel/refs/pub2001/kwint_paper1048.pdf

von Reibnitz, Ute. *Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung*. (Wiesbaden, 1992).

A3 Important Links

Australia

Attorney-General's Department (http://www.ag.gov.au)

Australian Computer Emergency Response Team (AusCERT) (http://www.auscert.org.au)

Australian Security Intelligence Organization (ASIO) (http://www.asio.gov.au)

Defense Science and Technology Organization (DSTO) (http://www.dsto.defence.gov.au)

National Office for the Information Economy (NOIE) (http://www.noie.gov.au)

Prime Minister of Australia (http://www.pm.gov.au)

Canada

Canada's National Computer Emergency Response Team (http://www.cancert.ca)

Canadian National Research Council (NRC) (http://www.nrc.ca)

Communication Research Centre (CRC) (http://www.crc.ca)

D-Net (http://www.dnd.ca)

Federal Association of Security Officials (http://www.faso-afrs.ca)

Government-on-Line (GoL) (http://www.gol-ged.gc.ca)

Institute for Information Technology (IIT) (http://www.iit.nrc.ca)

Networks of Centres of Excellence (NCE) (http://www.nce.gc.ca)

Office of Critical Infrastructure Protection and Emergency Preparedness (OCI-PEP) (http://www.ocipep-bpiepc.gc.ca)

Treasury Board Secretariat (http://www.tbs-sct.gc.ca)

Germany

Arbeitskreis Schutz von Infrastrukturen (AKSIS) (http://www.aksis.de)

BKAonline – Bundeskriminalamt Wiesbaden (http://www.bka.de)

Bundesamt für Sicherheit in der Informationstechnik (BSI) (http://www.bsi.de)

Bundesministerium für Bildung und Forschung (BMBF) (http://www.bmbf.de)

Bundesnachrichtendienst (BND) (http://www.bundesnachrichtendienst.de)

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (http://www.bitkom.org)

CERT-Bund (http://www.bsi.bund.de/certbund/index.htm)

DCERT (http://www.dcert.de)

Deutsche Telekom AG (http://www.telekom.de)

Deutscher Bundestag (http://www.bundestag.de)

DFN-CERT (http://www.cert.dfn.de)

Europäisches Institut für IT-Sicherheit (http://www.eurubits.de)

Informations- und Kommunikationsdienste-Gesetz (http://www.iid.de/iukdg/)

Initiative D21 (http://www.initiatived21.de)

Initiative Informationsgesellschaft Deutschland (http://www.iid.de)

juris GmbH (http://www.juris.de)

secunet Security Networks AG (http://www.secunet.de)

Sicherheit im Internet (http://www.sicherheit-im-internet.de)

SIZ – Informatikzentrum der Sparkassenorganisation GmbH (http://www.s-cert.de)

The Netherlands

Binnenlandse Veiligheidsdienst (BVD) (National Intelligence and Security Agency) (http://www.fas.org/irp/world/netherlands/bvd.htm)

Directoraat-Generaal Telecommunicatie en Post (http://www.minvenw.nl/dgtp/home/)

INFODROME (http://www.infodrome.nl)

Ministerie van Verkeer en Waterstaat (http://www.minvenw.nl)

Ministry of the Interior and Kingdom Relations (http://www.minbzk.nl)

NLIP – Branchevereniging van Nederlandse Internet Providers (http://www.nlip.nl)

Rathenau Instituut (http://www.rathenau.nl)

SURFnet Computer Security Incident Response Team (http://cert-nl.surfnet.nl/home-eng.html)

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) (http://www.aivd.nl)

The Platform for Electronic Business in the Netherlands (ECP.nl) (http://www.ecp.nl/ENGLISH/index.html)

TNO Web (http://www.tno.nl)

Norway

Direktoratet for Sivilt Beredskap (DSB) (http://www.dsb.no)

Ministry of Trade and Industry (http://odin.dep.no/nhd/engelsk/)

Okokrim (http://www.okokrim.no)

The Norwegian Network for Research & Education – Computer Emergency Response Team (http://cert.uninett.no)

Sweden

Försvars Departementet (http://forsvar.regeringen.se)

KTH Royal Institute of Technology (http://www.kth.se/eng/)

Överstyrelsen för Civil Beredskap (http://www.ocb.se)

Swedish Alliance for Electronic Commerce (GEA) (http://www.gea.nu)

Swedish Defense Research Agency (http://www.foi.se/english/)

Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se/english/index.jsp)

Swedish National Defense College (http://www.fhs.mil.se)

The National Board of Psychological Defence (http://www.psycdef.se/english/)

Switzerland

Bundesamt für Berufsbildung und Technologie BBT (http://www.bbt.admin.ch)

CERT SWITCH (http://www.switch.ch/cert/)

Center for Security Studies and Conflict Research (FSK) (http.//www.fsk.ethz.ch)

Commission for Technology and Innovation (CTI) (http://www.snhta.ch/www-support/institutions/cti_fopet.htm)

Comprehensive Risk Analysis and Management Network (CRN) (http://www.isn.ethz.ch/crn/)

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

Federal Office for Communication (OFCOM) (http://www.bakom.ch/en/index.html)

Federal Office for National Economic Supply (NES) (http://www.bwl.admin.ch/)

Federal Office for Police (FOP) (http://internet.bap.admin.ch)

Federal Office of Information Technology, Systems and Telecommunication (FOITT) (http://www.informatik.admin.ch)

Federal Strategy Unit for Information Technology (FSUIT) (http://www.isb.admin.ch)

Foundation InfoSurance (http://www.infosurance.org)

IBM Zurich Research Laboratory (http://www.zurich.ibm.com)

Information and Communication Management Research Group (http://www.ifi.unizh.ch/ikm/research.html)

Information Society Coordination Group (http://www.isps.ch)

International Relations and Security Network (ISN) (http://www.isn.ethz.ch)

National Emergency Operations Center Agency (NAZ) (http://www.naz.ch)

Security and Cryptography Laboratory (LASEC) (http://lasecwww.epfl.ch)

Softnet (http://www.softnet.ch)

Strategische Führungsausbildung (http://www.sfa.admin.ch)

Symposium on Privacy and Security (http://www.privacy-security.ch)

United States

Center for Democracy and Technology (http://www.cdt.org)

Critical Infrastructure Assurance Office (CIAO) (http://www.ciao.gov)

Department of Homeland Security (http://www.whitehouse.gov/deptofhomeland)

Energy Information Sharing and Analysis Center (ENERGY-ISAC) (http://www.energyisac.com)

Federal Bureau of Investigation (FBI) (http://www.fbi.gov)

Federal Computer Incident Response Center (http://www.fedcirc.gov)

Federation of American Scientists (http://www.fas.org)

Financial Services Information Sharing and Analysis Center (FS-ISAC) (http://www.fsisac.com)

Information Technology Information Sharing and Analysis Center (IT-ISAC) (https://www.it-isac.org)

National Coordinating Center for Telecommunications (http://www.ncs.gov/ncc/)

National Infrastructure Protection Center (NIPC) (http://www.nipc.gov)

North American Electric Reliability Council (NERC) http://www.nerc.com

Partnership for Critical Infrastructure Security (PCIS) (http://www.pcis.org)

Stay Safe Online (http://www.staysafeonline.info)

Surface Transportation Information Sharing and Analysis Center (ST-ISAC) (http://www.surfacetransportationisac.org)

Miscellaneous

Cryptome (http://cryptome.org)

Dependability Development Support Initiative (DDSI) (http://www.ddsi.org)

European Warning and Information System Forum (EWIS) (http://ewis.jrc.it)

Global Business Dialogue on Electronic Commerce (http://www.gbde.org)

A4 Experts Involved

Australia

Ivan Timbs, National Office for the Information Economy (NOIE), E-Security Policy Section (http://www.noie.gov.au)

Canada

Jacques L. Grenier, Office of Critical Infrastructure Protection and Emergency Preparedness (http://www.ocipep-bpiepc.gc.ca)

Colin Knight, Office of Critical Infrastructure Protection and Emergency Preparedness (http://www.ocipep-bpiepc.gc.ca)

Germany

Ralf Bendrath, Scientist

Dr. Jörn Brömmelhörster, Consultant

Dr. Susanne Jantsch, Industrieanlagen-Betriebsgesellschaft (IABG) (http://www.iabg.de)

Dr. Christine Scharz-Hemmert, Industrieanlagen-Betriebsgesellschaft (IABG) (http://www.iabg.de)

Netherlands

Ronald de Bruin, KWINT, ECP.nl (http://www.ecp.nl)

Eric Luiijf, TNO Physics and Electronics, Laboratory (http://www.tno.nl)

Norway

Cort Arch Dreyer, Ministry of Trade and Industry (http://odin.dep.no)

Havard Fridheim, Norwegian Defence Research Establishment (http://www.mil.no/felles/ffi/start)

Arthur Gjengstö, Secretary to the Norwegian Commission on the Vulnerability of Society

Stein Henriksen, Directorate for Civil Defence and Emergency Planning (http://www.dsb.no)

Sweden

Lars Nicander, Director National Office of IO/CIP Studies, Swedish National Defence College (http://www.fhs.mil.se)

Jan Lundberg, Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se), former ÖCB

Manuel W. Wik, Swedish National Defence College (http://www.fhs.mil.se)

Peter Westrin, PH.D., FOI, Swedish Defence Research Agency (http://www.foi.se)

Dr. Peter Stern, Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se), former ÖCB

Peter Wallström, Cell Network (http://www.cellnetwork.se)

Switzerland

Dr. Michel Dufour, Dufour Consulting

Thomas Köppel, Federal Office for Police (http://internet.bap.admin.ch)

Kurt Haering, Director Foundation InfoSurance (http://www.infosurance.ch)

Dr. Ruedi Rytz, Federal Strategy Unit for Information Technology (FSUIT) (http://www.isb.admin.ch)

Dr. Ueli Haudenschild, Federal Office for National Economic Supply (http://www.bwl.admin.ch)

United States

Scott C. Algeier, U.S. Chamber of Commerce (http://www.uschamber.com)

A5 Abbreviations

ACSI 33:	Australian Communications-Electronic Security Instruction 33, (Australia)
AG KRITIS:	Interministerielle Arbeitsgruppe Kritische Infrastrukturen, (Germany)
AgIO:	Cabinet Office Workgroup on Information Operations, (Sweden)
AIOS:	Bureau for Security of Information and Objects, (Switzerland)
AKSIS:	Arbeitskreis Schutz Kritischer Infrastrukturen, (Germany)
ASIO:	Australian Security Intelligence Organisation, (Australia)
AusCERT:	Australian Computer Emergency Response Team, (Australia)
BIT:	Federal Office of Information Technology, Systems and Telecommunication, (Switzerland)
BITKOM:	Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien, (Germany)
BKA:	Bundeskriminalamt, (Germany)
BMBF:	Bundesministerium für Bildung und Forschung (Federal Ministry for Education and Research), (Germany)
BMWi:	Bundesministerium für Wirtschaft and Technologie, (Germany)
BND:	Bundesnachrichtendienst, (Germany)
BSI:	Bundesamt für Sicherheit in der Informationstechnik, (Germany)
BZK:	Ministry of the Interior and Kingdom Relations, (The Netherlands)
CanCERT:	Canadian Computer Emergency Response Team, (Canada)
CART:	Computer Analysis and Response Team, (United States)
CERT:	Computer Emergency Response Team
CERT SWITCH:	Computer Emergency Response Team of the Swiss Academic & Research Network, (Switzerland)
CERT-Bund:	German Computer Emergency Response Team für Bundesbehörden, (Germany)
CERT-NL:	Computer Emergency Response Team of the Netherlands, (The Netherlands)
CERT-RO:	Computer Emergency Response Team – Central Government, (The Netherlands)
CFAA:	Computer Fraud and Abuse Act, (United States)
CHO:	Chief Headquarter of Defense, (Norway)

CI:	Critical Infrastructure
CIAO:	Critical Infrastructure Assurance Office, (United States)
CIF:	Consultative Industry Forum, (Australia)
CIIP:	Critical Information Infrastructure Protection
CIP:	Critical Infrastructure Protection
CIPG:	Critical Infrastructure Protection Group, (Australia)
CIPTF:	Critical Infrastructure Protection Task Force, (United States)
CIS:	Center for International Studies, (Switzerland)
CRC:	Communications Research Centre, (Canada)
CRN:	Comprehensive Risk Analysis and Management Network, (Switzerland)
CTI:	Commission for Technology and Innovation, (Switzerland)
CWIG:	Critical Infrastructure Working Group, (United States)
CYTEX:	Cyber Terror Exercise, (Germany)
DDPS:	Swiss Federal Department of Defense, Civil Protection and Sports, (Switzerland)
DISFP:	Division for Information Security and Facility Protection, (Switzerland)
DJP:	Federal Department of Justice and Police, (Switzerland)
DoD:	Department of Defense, (United States)
DoE:	Department of Energy, (United States)
DSB:	Directorate for Civil Defense and Emergency Planning, (Norway)
DSD:	Defence Signals Directorate, (Australia)
DSTO:	Defence Science and Technology Organisation, (Australia)
EO:	Executive Order, (United States)
ECP-NL:	Platform Electronic Commerce in the Netherlands, (The Netherlands)
ESCG:	E-Security Coordination Group, (Australia)
ETH:	Swiss Federal Institute of Technology (ETH Zurich), (Switzerland)
FBI:	Federal Bureau of Investigation, (United States)
FDEA:	Federal Department of Economic Affairs, (Switzerland)
FDF:	Swiss Federal Department of Finance, (Switzerland)
FedCIRC:	Federal Computer Incident Response Center, (United States)
FFI:	Norwegian Defense Research Establishment, (Norway)
FIRST:	Forum of Incident and Security Response Team, (Canada)
FOI:	Swedish Defense Research Agency, (Sweden)

FOITT:	Federal Office of Information Technology, Systems and Telecommunication, (Switzerland)
FOP:	Federal Office for Police, (Switzerland)
FS/ISAC:	Financial Services Information Sharing and Analysis Center, (United States)
FSUIT:	Federal Strategy Unit for Information Technology, (Switzerland)
FSK:	Forschungsstelle für Sicherheitspolitik und Konfliktanalyse (Center for Security Studies and Conflict Research), (Switzerland)
GEA:	Swedish Alliance for Electronic Commerce, (Sweden)
GoL:	Government-on-line, (Canada)
HERT:	Hacking Emergency Response Team, (The Netherlands)
HHM:	Hierarchical Holographic Modeling
I&C:	Information and Communications
IAG:	Infrastructure Analysis Group
ICT:	Information and Communication Technologies
IDC:	Interdepartmental Committee on the Protection of the National Information Infrastructure, (Australia)
IIT:	Institute for Information Technology, (Canada)
IMS:	Institute for Microstructural Sciences, (Canada)
IOWG:	The Information Operations Working Group
IPs:	Infrastructure Profiles
IRAM:	Infrastructure Risk Analysis Model
ISACs:	Information Sharing and Analysis Centers
ISN:	International Relations and Security Network (Switzerland)
ISP:	Internet Service Provider
IT:	Information Technology
ITM:	Institut für Informations-, Telekommunikations- und Medienrecht, (Germany)
IWG:	CIP R&D Inter-Agency Working Group, (United States)
KLPD:	Korps Landelijke Politiediensten, (Dutch Police), (The Netherlands)
KTH:	Royal Institute of Technology, (Sweden)
LKA:	Landeskriminalamt, (Germany)
MCDA:	Multi Criteria Decision Approach
MIE:	Minimum Essential Infrastructure
MISA:	Municipal Information Systems Association, (Canada)

NAZ:	National Emergency Operations Center Agency, (Switzerland)
NCC:	National Coordinating Center
NCE:	Networks of Centres of Excellence, (Canada)
NCIPP:	National Critical Infrastructure Protection Program, (Canada)
NCPG:	National Contingency Planning Group, (Canada)
NCSA:	National Cyber Security Alliance, (United States)
NCSIP:	National CIO Sub-Committee on Information Protection, (Canada)
NERC:	North American Electricity Reliability Council, (United States)
NES:	Federal Office for National Economic Supply, (Switzerland)
NII:	National Information Infrastructure
NIPC:	National Infrastructure Protection Center, (United States)
NIRA:	National Infrastructure Risk Assessment, (Canada)
NIST:	National Institute of Standards and Technology, (United States)
NLIP:	Consortium of Dutch Internet Providers, (The Netherlands)
NOIE:	National Office for the Information Economy, (Australia)
NRC:	Canadian National Research Council, (Canada)
NSD:	Industry Security Delegation, (Sweden)
ÖCB:	Swedish Agency for Civil Emergency Planning, (Överstyrelsen för Civil Beredskam), now KBM (Sweden)
OCIIP:	Office of Computer Investigations and Infrastructure Protection, (United States)
OCIPEP:	Office of Critical Infrastructure Protection and Emergency Preparedness, (Canada)
OFCOM:	Federal Office For Communication, (Switzerland)
OGIT:	Office of Government Information Technology, (Australia)
OGO:	Office for Government On-line, (Australia)
OPET:	Office for Professional Education and Training, (Switzerland)
OSTP:	Office of Science and Technology Policy, (United States)
PCCIP:	Presidential Commission on Critical Infrastructure Protection, (United States)
PCIS:	Partnership for Critical Infrastructure Security, (United States)
PDD:	Presidential Decision Directives, (United States)
PEST:	Political, Economic, Social, Technological (Analysis)
PMRM:	Partitioned Multi-objective Risk Method

PreDICT:	Predict Defence Infrastructure Core Requirements Tool, (Australia)
PSCIOC:	Public Sector Chief Information Officer's Council, (Canada)
PSM:	Protective Security Manual, (Australia)
R&D:	Research and Development
RAFLS:	Relational Analysis For Linked Systems, (Canada)
SAVI:	Säkring Av Viktig Infrastructure, (Sweden)
SCNS:	Secretaries' Committee on National Security, (Australia)
SEMA:	Swedish Emergency Management Agency, (Sweden)
SFU:	Strategic Leadership Exercise, (Switzerland)
Sigint:	Signals Intelligence
SII:	Strategic Infrastructure Initiative, (Canada)
SIS:	Ministry of Trade and Industry Initiative, (Norway)
SLT:	Strategic Leadership Training, (Switzerland)
SWOT:	Strength, Weakness, Opportunities, Threats (Analysis)
USA PATRIOT:	(Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (United States)
V&W:	Ministry of Transport, Public Works and Water Management, (The Netherlands)
VAF:	Vulnerability Assessment Framework, (United States)
ZES:	Zentrum für Strategische Studien, (Germany)