Models for CII Analysis

Introduction

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

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

For each approach, four elements are considered:

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

Technical IT-Security Models

Application Area

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

Objective

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

Reference Material

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

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

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

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

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

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

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

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

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

Risk Analysis Methodology (for IT Systems)

Application Area

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

Objective

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

Work Process

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

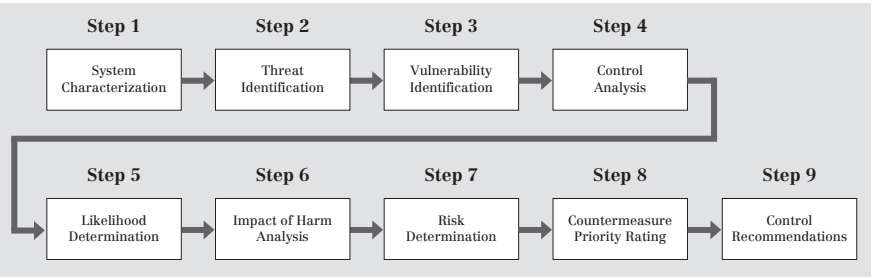

Figure 21: Steps in Risk Assessment Methodology

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

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

Step 1: System Characterization

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

Step 2: Threat Identification

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

Step 3: Vulnerability Identification

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

Step 4: Control Analysis

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

Step 5: Likelihood Determination

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

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

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

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

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

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

Step 6: Impact or Harm Analysis

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

Step 7: Risk Determination

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

Step 8: Countermeasure Priority Rating

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

Step 9: Control Recommendations

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

Reference Material

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

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

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

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

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

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

Column 1 Asset Identification	C 2 Threat to the Asset	C 3 Threat Likelihood	C 4 Harm	C 5 Resultant Risk	C 6 Required Risk	C 7 Countermeasure(s) Priority Rating
Row 1: Reliability of e-commerce-related 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[10]

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

Infrastructure Risk Analysis Model (IRAM)[11]

Application Area

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

Objective

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

Work Process

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

Phase I: Identify Threats and Vulnerabilities

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

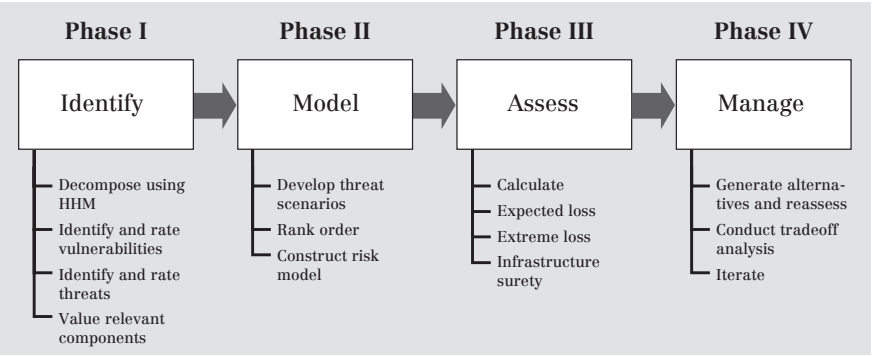

Figure 22: The four Phases of the Infrastructure Risk Analysis Model

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

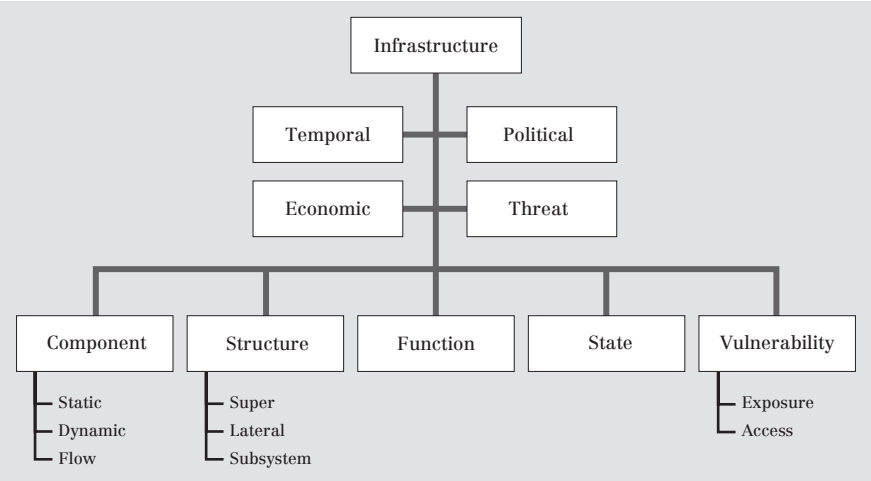

Figure 23: Generic Systems Decomposition (Source: Ezell, Farr, Wiese) [12]

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

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

Phase II: Model Risks

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

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

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

Phase III: Assess Loss

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

Phase IV: Manage

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

Reference Material

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

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

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

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

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

Leontief-Based Model of Risk in Complex Interconnected Infrastructures

Application Area

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

Objective

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

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

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

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

Work Process

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

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

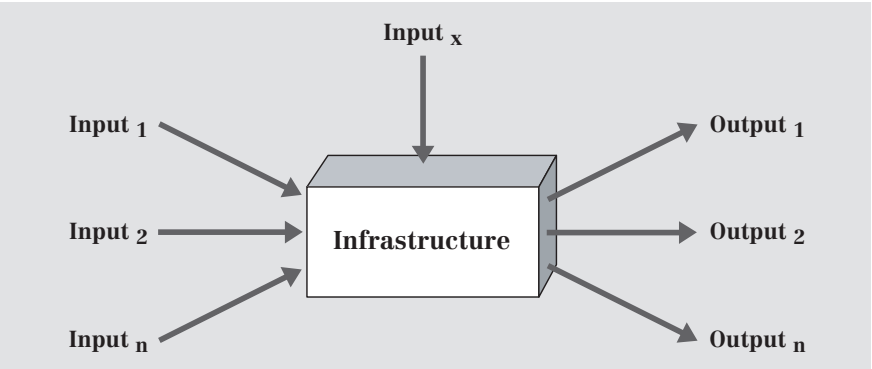

Figure 24: Input-Output Relationship

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

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

Reference Material

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

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

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

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

Sector and Layer Models

Application Area

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

Objective

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

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

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

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

Reference Material

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

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

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

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

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

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

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

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

Sector Analysis

Application Area

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

Objective

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

PEST (Political, Economic, Social, Technological) Analysis

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

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

Table 4: PEST Example

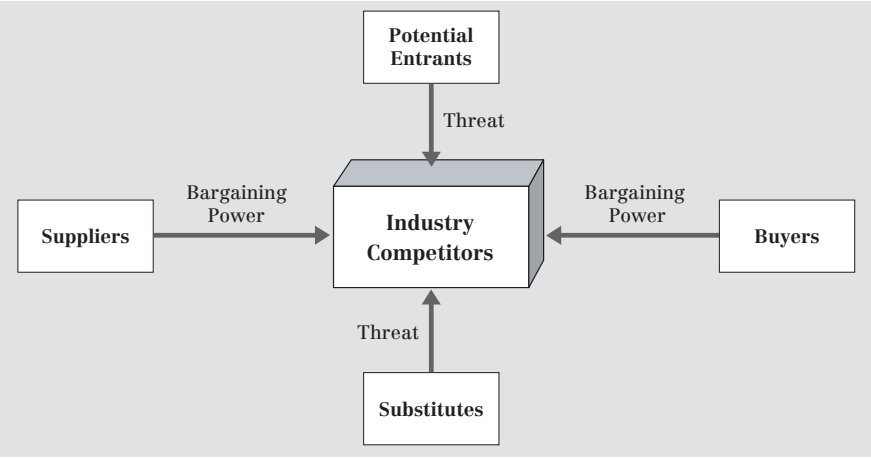

Figure 25: Michael Porter's Five Forces Model

Porter's Analysis

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

SWOT (Strength, Weakness, Opportunities, Threats)

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

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

Table 5: Typical SWOT Worksheet

Reference Material

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

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

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

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

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

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

Process and Technology Analysis

Application Area

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

Objective

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

Work Process

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

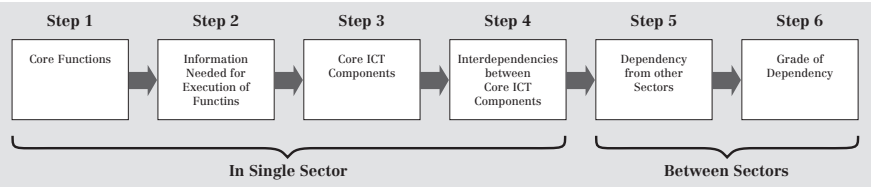

Figure 26: Steps of the Process and Technology Analysis

Step 1: Identify Core Functions of a Sector

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

Step 2: Identify Information Needed for Execution of Function

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

Step 3: Identify Core ICT Components

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

Step 4: Show Interdependencies Between Core ICT Components

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

Step 5: Define Dependency from Other Sectors

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

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

Step 6: Establish Grade of Dependencies

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

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

Reference Material

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

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

Dimensional Interdependency Analysis

Application

This descriptive approach portrays six dimensions of infrastructure interdependencies.

Objective

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

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

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

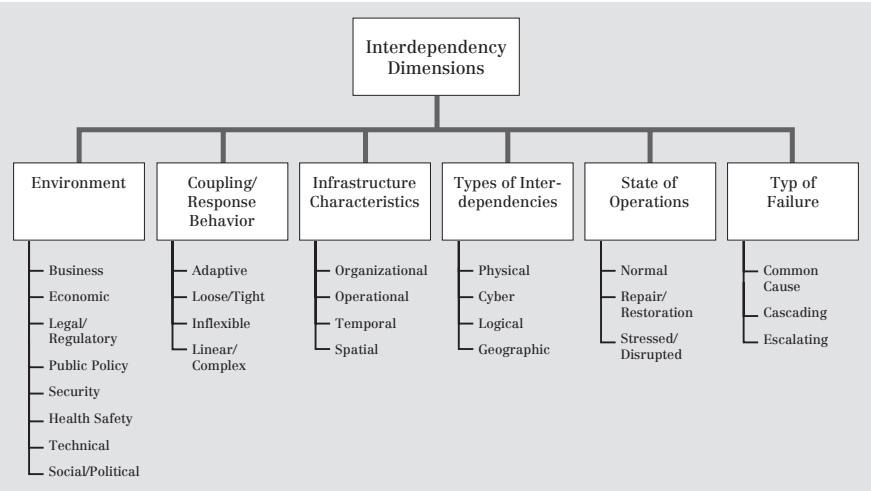

Figure 27: Interdependency Dimensions

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

Reference Material

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

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

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