1 Sector Analysis

A →*Sector* can be defined as a group of industries or infrastructures that perform a similar function. In general, critical sectors are sectors whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social well-being of a nation. However, the definition of critical sectors varies among countries (→see *Part I: CIIP Country Studies*). Each country uses different standards of what is critical. The definitions also vary over time. Furthermore, some of these infrastructures are always critical, some are occasionally critical, while others only become critical in the case of failures in other vital infrastructures.

What is Sector Analysis?

There are many aspects that might be analyzed in connection with individual sectors, such as how and why they are critical, or what parts of it are particularly vulnerable, etc. In general, sector analysis adds to an understanding of the functioning of single sectors by highlighting various important aspects such as underlying processes, stakeholders, or resources needed for crucial functions. Sector analysis is a basis for better understanding the larger, complex infrastructure systems. However, sector analysis on its own remains insufficient for a holistic understanding of the larger infrastructures system at hand.

Even more, the division of the whole system into sectors is rather artificial and serves a more practical purpose. It is a need stemming from the fact that infrastructures are mainly owned and operated by private actors, so that the only sure path to protected infrastructures in the years ahead is through a real partnership between infrastructure owners and operators and the government. It is therefore necessary for a meaningful analysis to evolve beyond the conventional 'sector'-based focus, since, for example in the case of a terrorist attack, key elements within an infrastructure are more likely targets than entire sectors. It makes more sense to categorize targets in terms of their inherent function – e.g., the supply of raw material, distribution nodes, or command and control centers.

How to Determine Which Sectors Are Critical

In sector analysis, the question of "what is critical" is a key problem. The subject of what infrastructures and sectors are to be included in the list of critical assets requires input from private sector experts as well as experts and officials at various levels of government. More often than not, the issue is addressed by expert groups, either in larger or smaller groups, but might also be determined by lead agencies within government. It must be kept in mind that therefore results often depend on the subjective impressions of experts.

Since different people from different communities are involved in the process, a common understanding and definition of the term "critical" is of the essence: Without standardization of the assets to be considered, prior to any attempted assessment, owners and operators of potentially critical assets might not all choose a common level of granularity. For example, a representative of the electric power generation business might identify generating stations or dams as critical, while others might extend that assessment to the level of turbines or bearings.[2]

Usually, a component or a whole infrastructure is defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to the interdependency between the component or the infrastructure and other infrastructures. In a broader view, infrastructures or components of infrastructures have come to be seen as critical due to their inherent symbolic meaning.[3]

2 Cf. Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Tool to Assist Owners and Operators to Identify Critical Infrastructure Assets* (Draft, 19 December 2002): p. 2.

3 For more details, see Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Frommelt, I. (eds.). Stockholm International Peace Research Institute (SIPRI), *Business and Security: Public-Private Sector Relationships in a New Security Environment* (Oxford, forthcoming 2004) and *Part I: Country Surveys* , e.g. Country Surveys on Canada and the US.

Examples of How to Determine Which Sectors Are Critical

In the following, two examples are given of how to identify critical sectors:

- Example 1 (Canada) – The National Contingency Planning Group's Approach to Criticality (NCPG)
- Example 2 (the Netherlands) – Quick Scan on Critical Products and Services (Quick Scan)

Example 1 (Canada) – The National Contingency Planning Group's Approach to Criticality (NCPG)

When the *National Contingency Planning Group* (NCPG) was formed in October 1998, part of its mandate was the production of a *National Infrastructure Risk Assessment* (NIRA). The NIRA's objective was to better position the country for the transition to the year 2000 by finding out which infrastructures were most at risk. It set out to examine important Canadian infrastructure elements, determine their criticality, and assess the probability of their failure.[4] Two criteria were used to determine the criticality:

- The possible impact on four tenets (direct impact on individual Canadians):
  - No loss of life;
  - Basic community needs are met;
  - Business continues as usual;
  - Confidence in government is maintained.
- The degree of dependency (direct impact on Canadian government, industry, and business).[5]

In February 1999, the group finished identifying and defining elements of Canada's critical infrastructure. The assessment of criticality was based on information that the NCPG had collected from a broad group of stakeholders, including key industries, and other government departments. It assessed the likelihood of Year 2000 failure on the basis of the state of preparedness for the Year 2000 changeover and progress in developing contingency plans. The

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

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

interdependencies identified in those plans were used to assess the potential impact of failure of critical infrastructure elements.[6]

Example 2 (The Netherlands) – Quick Scan on Critical Products and Services (Quick Scan)

In early 2002, the Dutch government initiated the critical infrastructure protection project *Bescherming Vitale Infrastructuur*, with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT.[7] The project includes four steps: 1) a *quick-scan analysis* of the Dutch critical infrastructure, 2) stimulation of a public-private partnership, 3) threat and vulnerability analysis, and 4) a gap analysis of protection measures. The analysis undertaken under step 1 identifies products and services vital to the nation's critical infrastructure, the (inter-) dependencies of these products and services, and underlying essential processes.

To identify sectors, products, and services comprising the national critical infrastructure, a quick-scan →*Questionnaire* was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were then augmented and refined in seventeen workshops with the vital public and private sectors. In parallel, damage experts evaluated the potential damage impact of loss or disruption of vital products and services on five →*Indicators*: (1) people, (2) animals, (3) the economy, (4) the environment, and (5) immaterial complacency.[8]

To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are 'merely' very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution

6 Office of the Auditor General of Canada. *1999 Report of the Auditor General of Canada, September and November, Chapter 25: Preparedness for Year 2000, Final Preparation.* http://www.oag-bvg.gc.ca/domino/reports.nsf/html/9925ce.html.

7 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. *Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services* (April 2003).

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

to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale or endangers the minimum quality level." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society.

According to this model, a sector is deemed "critical" if its breakdown or serious disruption could lead to damage on a national scale, or in other words, if the impact of a disruption was severe enough. The definition of vitality was sharpened by making a distinction between direct and indirect vitality: →*Indirect Vitality* is the extent to which other vital products and services contribute to the dependability of the vital service or product, while →*Direct Vitality* is the contribution that a product or service makes to the continuity of the society, which is equivalent to the amount of direct (first-order) damage caused by a loss or serious disruption of the product or service.

In order to assess the first-order direct vitality, all product and services were plotted in a graph, where the relative value of their direct vitality is assigned to the x-axis and the relative value of their indirect vitality to the y-axis (see Figure 1). Products and services marked in the upper right-hand corner of the graph are the most vital and critical ones.

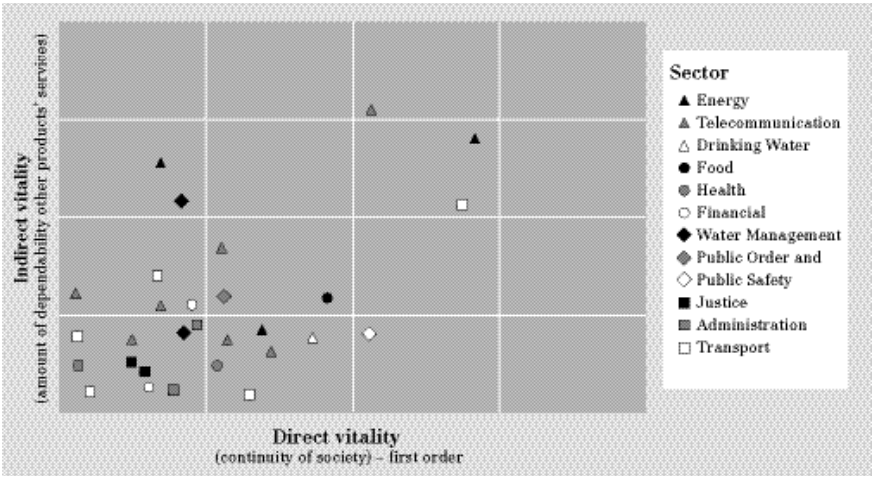

Figure 1: Quick Scan: Vital Products and Services

How to Specify Characteristics of Critical Sectors

The determination of how critical sectors function, what the influencing parameters are in particular sectors, how important specific sectors are to the economy, and who the major players are, including the identification of core functions, value chains, and dependency on information and communication technology in each critical sector, is a prerequisite for subsequent →*Interdependency Analysis* (→see also Chapter 2 on *Interdependency Analysis*).

Most critical sectors have different structures and requirements, so that the appropriate level of detail might vary considerably from sector to sector. They can, for example, be subdivided into industries, into services, into products, or combinations of the various subdivisions.[9] Different industries require different approaches to consulting experts. In some industries, workshops can produce rapid and valuable results, while in other, personal interviews might be necessary.

Often, →*Sector Models* and/or →*Layer Models* are used to illustrate parts of infrastructure systems and their relationship to each other. Usually, they are used as mere illustrations of how critical infrastructures are organized, or serve as the basis for additional steps in the determination of interdependencies. Additionally, simulation systems employ different kind of sector or layer models for visualization. Plain sector models are simple two-dimensional representations of critical sectors. Interdependencies between the sectors might be shown with one or two-way arrows, which might also be rendered with different degrees of intensity. Layer models, on the other hand, come in all variations and sizes (see examples below).

Examples of How to Specify Characteristics of Critical Sectors

In the following, we will consider seven examples of how to specify the characteristics of critical sectors:

- Example 1 (Australia) – PreDict Industry Profiles (PreDict);
- Example 2 (Canada) – Critical Infrastructure Protection Task Force Layer Model (CIPTF);
- Example 3 (Germany) – BSI Methodology for the Analysis of Critical Infrastructural Sectors (ACIS);
- Example 4 (Netherlands) – Bitbreuk Layer Model (Bitbreuk);

9 Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

- Example 5 (Netherlands) – The Four Models of the KWINT-Report (KWINT);
- Example 6 (Switzerland) – Sector Roundtables, Methodological Steps 1–4 (Roundtables);
- Example 7 (United States) – Department of Energy Layer Models (DoE).

Example 1 (Australia) – PreDict Industry Profiles (PreDict)

♦ The PreDict approach also appears in *Chapter 2: Interdependency Analysis*, and in *Chapter 5: Vulnerability Assessment.*

In 1998, government officials decided to analyze the Australian national defense-related infrastructure in order to develop strategies to remove, ameliorate, or avoid identified vulnerabilities.[10] Ten industries (Transport, Fuel, IT, Utilities, Health, Third Party Logistics (3PL) Providers, Education and Training, Communications, Defense-Related Manufacturing, and Financial Services)[11] were described in detail in terms of:

- Key Statistics;
- Key Market Segments;
- Regulatory Framework;
- Sector Environment;
- Industry Performance;
- Industry Trends.

The analysis section of the reports offers a summary representation of the sectors focusing mainly on the economic environment. It highlights industry-sector information such as trends, points of strength and weakness, the impact of the external environment, and the role of competitive forces in a bid to understand the sector under investigation.

The methodological approaches used were →*PEST Analysis* (to identify at political, economic, social, technological factors), →*Porter's Analysis* (to assess intensity of rivalry; competitors, barriers to entry, threat of substitutes; supplier power, and buyer power), and →*SWOT Analysis* (to assess

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

11 The term *industry* is used interchangeably with the term *sector* in the PreDict approach.

strength, weakness, opportunities, and threats). Additionally, a lifecycle view was drawn from the material gathered during interviews with industry representatives.

The approaches to the applied analyses were initially developed as a starting point for the determination of draft →*Vulnerabilities* for discussion and confirmation by industry and defense representatives during industry interviews and workshops. The results of the initial analysis were refined during the following project phases. The identified vulnerabilities were grouped into twelve →*Broad Risk Areas*. The twelve →*Broad Risk Areas* are: Political, Economic, Social/Environmental/Cultural, Technological, Supplier, Customer, Substitutes, Competitor, Barriers to Entry, Operations (Human Resources), Operations (Training), and Flexibility/Adaptability.[12] This was done in order to compare and contrast the vulnerabilities between industry sectors and the defense sector and to group the identified vulnerabilities into common areas for analysis. The majority of the Broad Risk Area titles were drawn from the analytical perspective drawn upon in the PEST and Porter's analysis[13] (→see also Chapter 5 on *Vulnerability Assessment*).

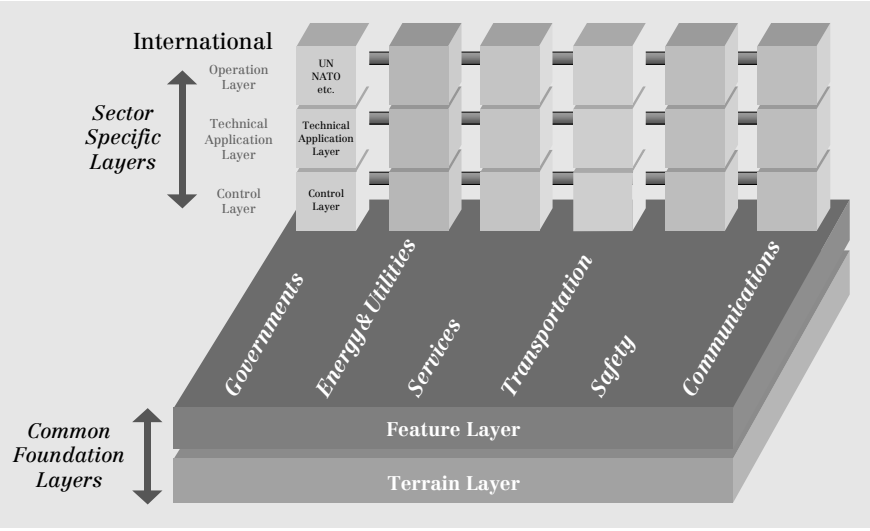

Figure 2: Canadian Layer Model

Example 2 (Canada) – Critical Infrastructure Protection Task Force Layer Model (CIPTF)

♦ The CIPTF approach also appears in *Chapter 2: Interdependency Analysis*, and in *Chapter 3: Risk Analysis*.

In the spring of 2000, the *Critical Infrastructure Protection Task Force* (CIPTF) was established within the *Canadian Department of National Defence*. The CIPTF developed an extensive review process for critical infrastructures in Canada. Based on six sectors identified as critical (Governments, Energy and Utilities; Services; Transportation; Safety; Communications),[14] the CIPTF developed a multi-dimensional →*Layer Model* that takes into consideration the responsibilities of sectors at various levels, namely at the international, federal, provincial, municipal, and the private levels.

Each of these areas of responsibility consists of three vertical sector-specific layers (operations layer, technical application layer, and control layer), which in turn rest on two "common foundation layers":

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

Figure 2 shows the layer model in an initial phase. At this point, only the specific layer of the international sector has been added onto the common foundation layers. With each additional step, the federal, provincial, municipal, and private-sector layers are added.[15] This model was used for subsequent interdependency analysis (see →*Chapter 2: Interdependency Analysis*, *Example 2*).

12 See analysis section of industry reports. http://www.defence.gov.au/predict.

13 Ibid.

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

15 Ibid.

Example 3 (Germany) – BSI Methodology for the Analysis of Critical Infrastructural Sectors (ACIS)

The *German Office for Information Security* (BSI) has developed a methodology for the *Analysis of Critical Infrastructural Sectors* (ACIS) to identify the political and economic processes critical for the society as a whole.[16]

The BSI uses a step-by-step approach. First, the sector under examination is described. Then the business processes that are relevant to the functioning of the sector are identified. They are assessed with a criticality analysis, which considers the outcomes in the case of one component of the process breaking down. The probability of the breakdown occurring is assessed. Since historical or statistical data is rarely available for incidents, the involvement of experts is of prime importance for this kind of analysis. Five →*Categories* (insignificant, minor, moderate, major, and catastrophic) are used to describe

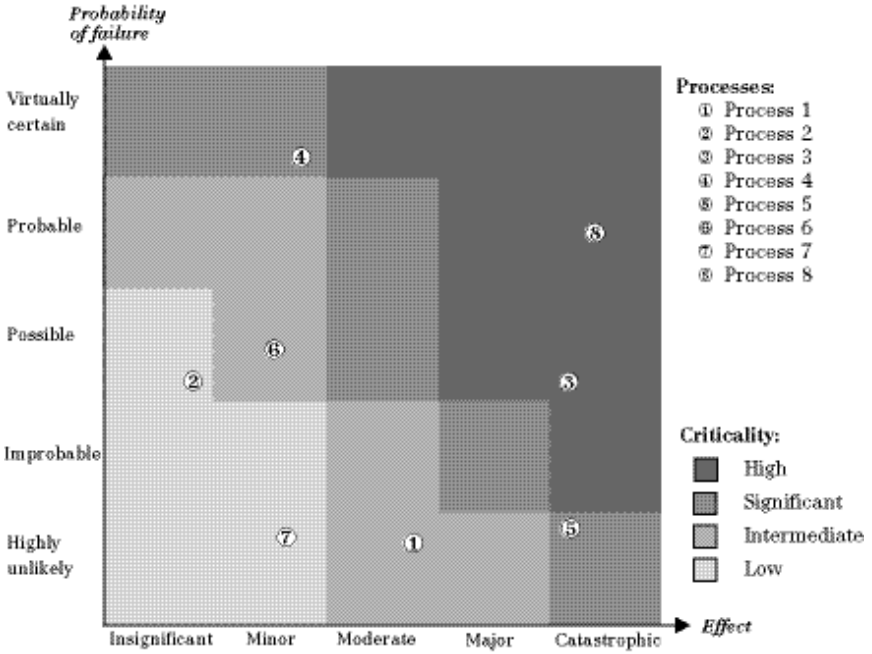

Figure 3: Criticality Matrix for Processes[17]

16 Reinermann, Dirk and Joachim Weber. "Analysis of Critical Infrastructures: The ACIS Methodology (Analysis of Critical Infrastructural Sectors)". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

17 Ibid.

the effects or the possible degree of damage, and another five →*Categories* (highly unlikely, improbable, possible, probable, virtually certain) are used to describe the probability of failure. The overall criticality of the process is derived from the combination of effects and failure probability.

The individual processes can then be plotted in a →*Criticality Matrix* (Figure 3).

Only the few business-critical processes that are also critical for a whole sector (those considered highly and significantly critical are in the top right corner in the figure) are taken to the next abstraction level in the analysis ("sector analysis level"). These samples of processes are analyzed in terms of their criticality. A second criticality matrix for sector processes helps to identify those that are also critical for the next level, namely at the abstraction level of "society". In the next step, only those processes that are deemed significantly or highly critical for the whole of society are assessed in terms of their dependence on IT. In this way, the methodology elaborated by the BSI serves as a filtering and cost-effectiveness tool, since it helps to significantly reduce the amount of work that is required for the analysis.[18]

Example 4 (Netherlands) – Bitbreuk Layer Model (Bitbreuk)

The model proposed by the *BITBREUK* report,[19] which focuses on the ICT infrastructure, is a →*Layer Model* with vertically stacked elements of CII and a focus on the IT sector (Figure 4).

Electrical power supply is considered to be the single factor underlying all ICT. Above this first layer are four more layers. The infrastructure's middle layer is located at the fourth level. This layer provides added-value services such as domain name registration or Internet servers between different underlying national and international infrastructures. This middle layer is the basis for the provision of more advanced

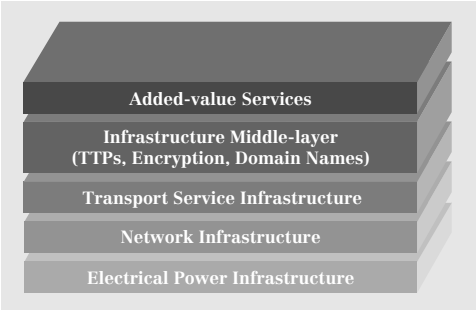

Figure 4: Bitbreuk Layer Model

18 Ibid.

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

services chains for government and for public and commercial organizations. These added-value services are dependent on the availability and integrity of the underlying layers of infrastructure. This indicates vertical dependence on the one hand, and, on the other hand, also involves horizontal information flows and information service chains between the different public and private actors, individuals, and society as a whole.[20]

Example 5 (Netherlands) – The Four Models of the KWINT Report (KWINT)

♦ The KWINT approach also appears in *Chapter 5: Vulnerability Assessment.*

The *Stratix Consulting Group/ TNO FEL* completed the so-called *KWINT-Report* (from the Dutch working title "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid") in 2001.[21] The overall aim of the project was to analyze the current vulnerabilities of the Dutch section of the Internet,[22] to identify possible consequences of threats, and to determine appropriate measures to reduce the vulnerabilities.[23] In order to clarify the roles of various actors and address the diversity, interdependencies, and vulnerabilities, four models with different orthogonal points of view were proposed (Figure 5).

- The *social level model* was used to discuss the motives and economics behind developments in the Internet;
- The *functional level model* was used as an intermediate between the functions experienced by the user of ICT and the more abstract and technical processes that form the basis for the functioning of the Internet (Figure 6).

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

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

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

23 Luiijf, Klaver, and Huizenga, The Vulnerable Internet.

- The *structural level model* was used to investigate the market environment of service providers and of product suppliers;
- The *physical level model* takes into account the importance of the physical location of the operational facilities when analyzing vulnerabilities.[24]

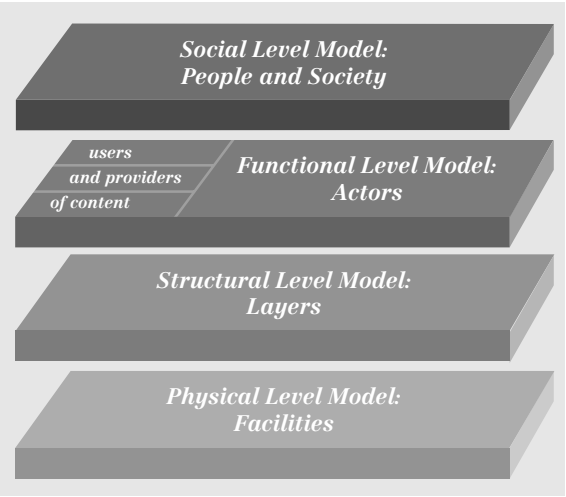

Figure 5:
Four Levels of Models

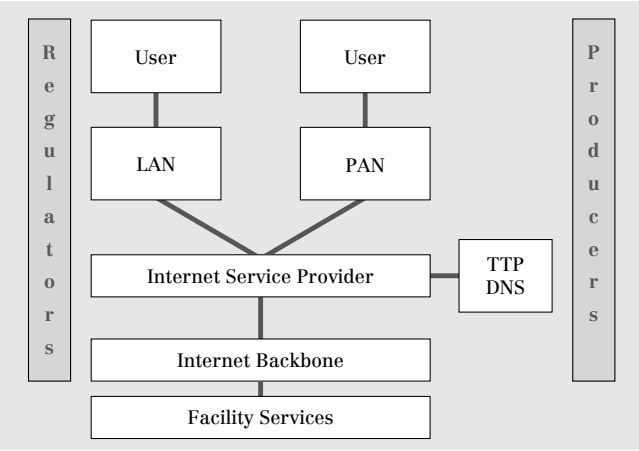

Figure 6:
Functional Model with Types of Actors

24 Luiijf, Klaver, and Huizenga, The Vulnerable Internet, pp. 3–5.

Example 6 (Switzerland) – Sector Roundtables, Methodological Steps 1–4 (Roundtables)

♦ The Sector Roundtables approach is also described in *Chapter 3: Risk Analysis.*

Under the auspices of the *Swiss InfoSurance Foundation*, sector-specific risk analysis roundtables are conducted for ten sectors, using a common methodology[25] (→see also Chapter 3 on *Risk Analysis*). The methodology used for each of the sectors is a ten-step risk analysis approach (see Table 2):

System Analysis		
Step		*Aim*
1	Sectors	Risk estimate for the 10 sectors
2	Sub-Sectors	Structure sector in organisational units
3	Core Functions	Structure sub-sectors according to functional core functions
4	Resources	Identify resources necessary for execution of core functions
5	Dependencies	Identify dependencies between sub-sectors <> core functions <> resources
6	Vulnerabilities	Identify possible weak points in resources, core functions, or sub-sectors
Risk Analysis		
7	Scenarios	Create representative scenarios for the identified vulnerabilities for each sector
8	Risk Estimation	Evaluate qualitatively for each scenario the extent of damage and frequency of damage occurrence
9	Risk Matrix	Create survey of the relevant scenarios; structure according to magnitude and frequency
10	Measures	Create ideas for measures

Table 2: Swiss Roundtables

Steps 1–4 are presented in this section since they are the core elements of sector analysis. The four steps aim to 1) gain an overview of critical sectors, 2) identify sub-sectors for each sector on the basis of organizational criteria, 3) identify core functions of the sub-sectors, and 4) assess the resources necessary for the functioning of the sub-sectors.

First the ten sectors for which the risk analysis is to be conducted were defined:[26] On this basis, sub-sectors for each of the ten sectors will be identified

25 Pfister, Ivo. *Round Tables InfoSurance: Sektorspezifische Risikoanalyse. Einführung und Methodische Grundlagen* (Luzerner Tage für Informationssicherheit LUTIS, June 2003). www.infosurance.ch/lutis/vortraege/ methodische_grundlagen.pdf. InfoSurance Fokus (November 2002): http://www.infosurance.ch/de/pdf/fokus_2.pdf.

26 These ten sectors are: (Public) Administration, Civil Defense and Emergency Services, (Tele-) Communication, Energy, Finance, Industry/ Manufacturing, Media, Public Health, Transport (and Logistics), Water (see →Part I for more details).

according to organizational standpoints. This step will also help to identify the main stakeholders and key players for each sector and sub-sector. Core functions of the sub-sectors are understood as the most important services provided by the sub-sector. Hence, in the third step these core functions have to be identified. The following information has to be gathered for each core function:

- What is required in terms of availability of service or function?
- What processes are executed for the delivery of the core function?
- Who delivers the core process?
- Which internal and external resources are needed for the normal delivery of the core process?

The sub-sectors depend on certain resources to fulfill their core function. These resources are identified in the fourth step by using a pre-fixed checklist as guidance. The list contains the following categories (of resources):

- Hardware
- Applications
- Data and Information
- Structural Infrastructure
- Technical Infrastructure
- Persons

Figure 7 shows an example of a process and technology analysis for the telecommunication sector.

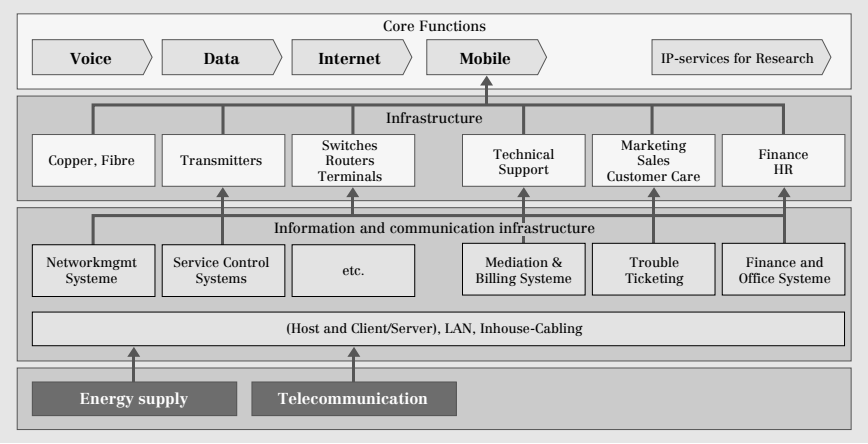

Figure 7: Core Functions, Infrastructure, and Components of the Swiss Telecommunication Sector

Example 7 (United States) – Department of Energy (DoE) Layer Models

The *Department of Energy* (DoE) uses →*Layer Models* to show interdependencies of the energy sector with other sectors and sector components (Figure 8):

Each sector is pictured as a grid on which the individual critical system components are located. Each component must be mapped in detail. The aim is to define critical system components and attendant vulnerabilities; interdependence propagation pathways and the degree of coupling; spatial and temporal system behavior; and the evaluation of protection, mitigation, response, and recovery options.[27] This information can be used for the *Interdependent Energy Infrastructure Simulation System* (IEISS), which gives users a unified view of physical interdependencies.[28]

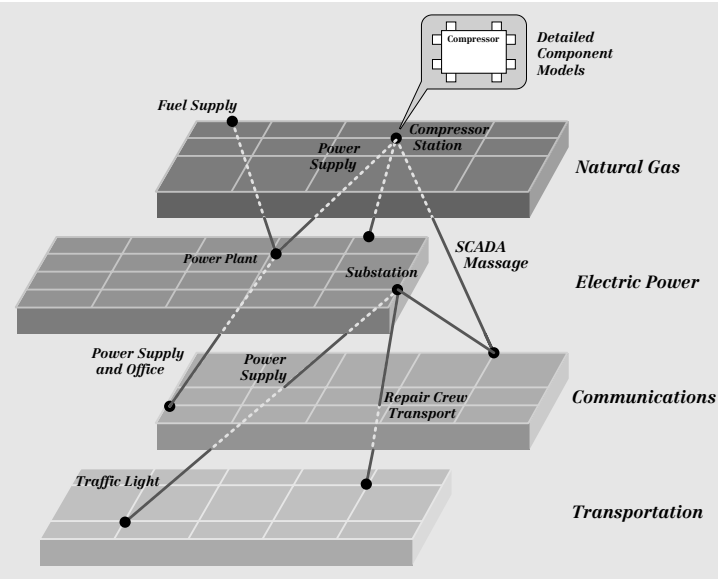

Figure 8: Interdependencies between Critical Infrastructures[29]

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

28 Varnado, Sam. "Modeling and Simulation for Critical Infrastructures – Status and Future Issues". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003).

29 Center for Strategic Leadership, US Army War College. *Issue Paper August 2003*, vol. 06–03. http://www.iwar.org.uk/cip/resources/csl-awc/nisac.pdf.