Critical Infrastructure Protection in The Netherlands: A Quick-scan

Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. Klaver
TNO Physics and Electronics Laboratory (TNO-FEL), The Netherlands

About the Authors

Eric Luiijf M.Sc.Eng. works as principal consultant in the Telecommunications and Security division of the TNO Physics and Electronics Laboratory (TNO-FEL) in the Netherlands. He graduated at the Mathematical Department of the Technical University of Delft in 1975. Since 1995, his research includes information security, information operations and critical infrastructure protection. Eric was the leading author of the essay 'Bitbreuk' ('In Bits and Pieces'). Eric was one of the main researchers behind the study KWINT, which looked at the vulnerability of the Dutch part of the Internet.
Eric has published many articles and papers on the topics information operations, information assurance, and critical infrastructure protection. He has been interviewed many times by Dutch press, TV and radio on these topics.

Helen Burger graduated (M.Sc.) in Applied Mathematics in 1989 at the University of Leiden and then started working at TNO Physics and Electronics Laboratory within the division Operations Research and Business Management. She has carried out many projects on system performance analysis and optimisation using qualitative and quantitative methods. Currently the emphasis of her work lies on topics within the TNO program on Public Safety, including critical infrastructure protection.

Marieke Klaver studied Mathematics at the University of Leiden. After her PhD in 1990, she joined the TNO Physics and Electronics Laboratory. Since 1997, Marieke takes part in TNO's R&D efforts in the area of "information warfare" and the protection of vulnerable information infrastructures. She contributed to the study KWINT, which looked at the vulnerability of the Dutch part of the Internet. In 2002, she contributed to the studies on the critical infrastructure commissioned by the Ministry of the Interior and Kingdom Relations. She is acting R&D programme manager Information Operations.

Mailing address: TNO Physics and Electronics Laboratory (TNO-FEL), P.O. Box 96864, 2509 JG The Hague, The Netherlands; Phone: +31 70 3740312; Fax: +31 70 3740651; Email addresses: luiijf@fel.tno.nl, burger@fel.tno.nl, klaver@fel.tno.nl.

Continued on page 2

Descriptors

Critical Infrastructure, Information Infrastructure, protection, policy, analysis, dependency, interdependency, damage, society, public-private partnership

Reference to this paper should be made as follows
Luiijf, E.; Burger, H. & Klaver, M. (2003). Critical Infrastructure Protection in the Netherlands: A Quick-scan. In U.E. Gattiker (Ed.), EICAR Conference Best Paper Proceedings (ISBN: 87-987271-2-5) 19 pages. Copenhagen: EICAR.

Critical Infrastructure Protection in The Netherlands: A Quick-Scan

Abstract

Some sectors and parts of the Dutch national infrastructure are that essential to the Netherlands that serious disruption or even loss of service could lead to a severe impact to the Dutch society, government and industry as well as to neighbouring countries. Early 2002, the Dutch government started the critical infrastructure protection project 'Bescherming Vitale Infrastructuur' with the objective: 'The development of an integrated set of measures to protect the infrastructure of government and industry (including Information and Communication Technology)'.
This paper describes the first steps of this project: a quick-scan determination of what vital products and services the nations' critical infrastructure is comprised of, the (inter)dependencies of these products and services, and underlying essential processes. The paper outlines the project context and execution, and describes the methodologies, results, and lessons learned.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Introduction

As described by Luiijf in 1999 (a, b), a number of countries started reconsidering the vulnerability of their infrastructures in the last decade of the previous century. The protection of strategic infrastructures and objects, vital for the continuation of the society, was an important topic during the days of the cold war. Towards the end of the cold war and certainly thereafter, the attention to infrastructure discontinuity caused by attacks or other major causes of disruption became more lax. However, a major shift has occurred in the mean time in both the technologies used and the threat spectrum. The upcoming millennium event with the Y2K-problem highlighted this around 1995-1996 when people discovered that no one could predict whether infrastructures could survive the shift from (19)99 to (20)00 without fatal failures of infrastructures with cascading effects.

The United States (US) and Australia (Cobb, 1997, 1999) were amongst the leading nations that sensed a potential, even larger problem. They started discussing the vulnerability of the vital infrastructures at large. New risks in all sectors like telecommunications, energy, health, administration, transport and so on, were identified by the presidential commission on critical infrastructure protection in the USA (PCCIP 1997). The sectors that are considered vital to society are at risk due to the increasing complex dependencies and interdependencies of the critical infrastructures. A critical infrastructure is defined as an infrastructure that is essential to the economic security, the smooth functioning of the government at all levels, and society as a whole. Moreover, most of these critical infrastructures are either build upon or monitored and controlled by vulnerable information and communication technology (ICT) systems. Disruption or even loss of the vital services, which are critically depending on other, often ICT-based or ICT-controlled, infrastructures could have serious impact on society. If occurring frequently, this could seriously harm public confidence as well. It was already stated in (Luiijf, 1999a) that our security and safety, economy, and ways of life are now highly dependent on the interrelated trio electricity, communications, and computer systems.

The PCCIP concluded already in 1997 that infrastructures have always been attractive targets to adversaries, activists, and terrorists. In the past, national borders and friendly neighbours provided some protection. However, today, the evolution of cyber threats has changed the situation drastically. In cyberspace, national borders are no longer relevant for conveying information and mounting attacks. Even worse, potentially serious cyber attacks on a critical infrastructure can be conceived and planned without easy detectable logistic preparation.
For that reason, it became clear to the Clinton administration that government, society, organisations and critical industries needed to prepare jointly for defending their assets. Subsequently, President Clinton took an initial set of actions to increase the protection of the critical infrastructures in the USA (Clinton, 1998). The events on September 11, 2001 increased the awareness of vulnerabilities and the sense-of-urgency to protect the critical infrastructures in many countries all over the world. For that reason, many

other countries started or intensified their critical infrastructure protection (CIP) programs after that date. As an example, the new Department for Homeland Security (DHS) in the USA has recently been established to carry out the co-ordination role for critical infrastructure protection in the USA as well as the responsibility for critical information-infrastructure protection (CIIP)-activities for all federal systems.

Earlier Work

The high-level analysis and discussion on CIP and CIIP in the USA is a well-documented and relatively transparent process. Apart from the US, Wenger, Metzger & Dunn (2002) documented the critical information infrastructure protection activities in seven other countries: Australia, Canada, Germany, Norway, Sweden, Switzerland, and The Netherlands. Their work describes different CIP- and CIIP-analysis methodologies used by these countries.

In The Netherlands, the Infodrome project by the government in the period 2000 – 2002 looked at policy issues stemming from the deep penetration of ICT into all aspects of society. The essay 'In Bits and Pieces' (Luiijf, 2000) has been written to stimulate the public discussion on the increasing ICT-dependency of the society and the risks involved. Partly as a result from that discussion, the Dutch Ministry of Transport, Public Works and Water Management commissioned the study KWINT that investigated the vulnerability of the Dutch Internet (van Till et al., 2001). The Dutch Cabinet endorsed the recommendations of that study on July 6, 2001. This led to a number of public-private partnership actions co-ordinated by the Platform for electronic business in the Netherlands (ECP.NL; www.ecp.nl). One of the completed actions is the establishment of a Computer Emergency Response Team for the Dutch government administration (originally called CERT-RO; since February 2003 GOVCERT.NL) and a malware alerting and information service for the public and small and medium enterprises (SMEs). Another action concerns the development of a set of transparent performance indicators, including those for security, for the Dutch Internet service provision community. Enhancing the security posture of the Dutch internet, however, covers only a small part of the Dutch critical infrastructure. To address the protection of the total of the nations' vital infrastructure, a much wider CIP-approach is required.

The Dutch CIP Approach from a Process Perspective

Some sectors and parts of the infrastructures are so vital for the Dutch society that serious disruption or even loss of service could lead to severe damages. The Dutch industry sectors and government have been aware for quite a while that their essential processes underpinning the essential services are depending upon essential services delivered by other sectors. The millennium problem increased this awareness. This caused the industry sectors to ask government and politics for increased protection of the essential products and services for industry and society. Early 2001, the Dutch Parliament asked the government for an integrated approach of the problem. The events on 11th of September 2001 increased the need and urgency to start such an integrated CIP-approach in the Netherlands. Action line 10 of the Dutch counter-

terrorism plan (Tweede Kamer, 2001) started the project Bescherming Vitale Infrastructuur (Protection of the Dutch Critical Infrastructure) with the objective: '*The development of an integrated set of measures to protect the infrastructure of government and industry (including ICT)*'. The project plan for this action line consists of several steps: a quick-scan analysis of the Dutch critical infrastructure, stimulation of a public-private partnership, threat and vulnerability analysis, and a gap analysis of protection measures.

This paper discusses the first two of these steps, the methodologies used, and relevant study results. The study started with the aim to obtain answers to the following three main questions:

(1) what are the sectors, products and services comprising the nations' critical infrastructure of government and industry?
(2) what are the underlying processes?, and
(3) what are the (inter)dependencies?

A quick-scan questionnaire was developed. That questionnaire has been used early 2002 by the Dutch government departments to make an inventory of all products and services they regarded vital, including the underlying processes and dependencies. In June 2002, the outcome of the analysis of the collected information was presented in a working conference with key representatives of both the public and private sectors. The initial results were then augmented and refined in seventeen workshops with the public and private vital sectors. Over 130 organisations, industries, government departments and agencies took part in the workshops. In parallel, damage experts valued the potential damage impact of loss or disruption of vital products and services to people, animals, economy, environment, and immaterial complacency.
All the materials from the questionnaires, the work sessions, and desk research were combined and analysed resulting in a report describing the end results of the first two steps of project Protection of the Dutch Critical Infrastructure. Additionally, a short comparative analysis was undertaken on the international CIP developments. It was concluded that the European Union does not play a co-ordinating or leading role (yet) in this topic area. Several international organisations (e.g. IATA, IMO, SWIFT) are, however, actively organising cross-border critical infrastructure assurance efforts.
The report has been presented to the Dutch Cabinet on February 14th. In the following week, the report including a set of recommendations was sent to the Dutch Parliament.

Determining the Dutch Critical Infrastructure

To determine what the Dutch national critical infrastructure is comprised of, it is necessary to determine the boundary between what products and services are vital to the nation and which are 'just' very important. This is not exact science, as political sensitivities play a certain role as well.
In the days of the cold war, determining this boundary seemed easy. Strategic physical objects and infrastructures (like e.g. harbours, bridges, and telephone exchanges) were placed on a so-called key point list. That determined the nations' critical infrastructure.

Nowadays, however, taking only isolated objects into account is no longer valid, since many infrastructures have dependencies and interdependencies with other critical infrastructures. Therefore, a more process-oriented analysis is required. ICT is an important factor of influence in this analysis since many of these (inter)dependencies are largely driven by ICT.

Moreover, this determination process is not easy since The Netherlands lacks a crisp deterministic definition of what is 'vital' to the society. Neither does an internationally accepted definition exist. In order not to loose valuable time, we followed a pragmatic approach using the following working definition:

'*A product or service is vital when it either:*

- *provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law & order, (2) public safety, (3) economy, (4) public health, (5) ecological environment,*
- *or when loss or disruption impacts citizens or government administration at a national scale or endangers the minimum quality level.'*

This shifts the problem of what is vital or just very important to the political level which needs to determine what is the acceptable damage impact to society, i.e. what is the minimum acceptable quality level of the vital services to society.

When determining the nations' critical infrastructure in this way, a top-down approach is required to identify the chains of essential processes supporting the delivery of the vital products and services to the nation. In this process the neighbouring countries and structures (both in the classical physical way and in cyberspace) should not be neglected. Starting with the Dutch millennium list of vital sectors, an initial list with over 40 potential vital products and services was created. Later on, an additional set of ten other products and services was identified and added to this list.

The government departments that are responsible for one of these products or services were tasked to fill in a questionnaire, which we developed, per potential vital product or service. The questionnaire asked for (1) a short description of the product or service; (2) existing legal requirements for the dependability of the product or service; (3) a split of the underlying processes in input, value-addition, and distribution processes; (4) per underlying process the none/ low/ medium/ high/ total level of dependency on each of the other products and services; (5) failure and recovery characteristics; (6) importance in terms of the aspects people, animals, economy, environment, and immaterial complacency; and (7) the none existing/ low/ medium of high level in which other products or services are dependent upon the product or service.
It should be mentioned that the dependability we looked after is not based on the availability aspect alone. Dependability as described in the questionnaire, is based on the aspects of availability and integrity. For example, drinking water running from the tap is hardly useful for people and animals in case of chemical or biological contamination.

The analysis of the over fifty questionnaires gave a good initial view on highly dependent and interdependent products and services. Dependency is a linkage or a connection between two products or services, through which the state of one influences or is correlated to the state of the other. Interdependency is a mutual dependency of products or services. The analysis showed some weaknesses in the process, e.g. a limited involvement of industry sectors (which are responsible for providing over half of the vital services) - due to the quick-scan nature of the process - and a stunning lack of knowledge about ones' clients.

Refinement phase

At a working conference with key representatives of both the public and private sectors, the attendees agreed that a refinement of the earlier results was necessary to create a solid base for the next steps of the project Protection of the Dutch Critical Infrastructure. Analysing the base types of the underlying processes of all the vital products and services lead to the findings shown in Table 1. It was obvious that some clustering of government products and services could take place as they generally are based upon the same type of underlying processes. Using these results, the Dutch industry sectors and the government settled the nations' critical infrastructure to enclose 11 vital sectors with 31 vital products and services (Table 2).

In the questionnaire we asked the producers and providers of the products and services about the level of dependency of their clients to themselves, as well as their own dependency on the other named vital products and services. The intention of this question was to determine the possible differences between the views of the client and the producer/ provider of a vital product or service. Rather than a limited number of small differences, many large positive and negative discrepancies were noted. This led to the conclusion that the producers and providers of potential vital products and services may have a good balanced view with respect to their internal processes and external dependencies, but have only a limited and a very unbalanced view on their own importance for others.

In order to stimulate public awareness, to increase the applicability of the results and to remove inconsistencies, the group of participants was expanded with private parties and a refinement phase was organised. In this phase, we also sharpened the definition of vitality.

Firstly, we defined *indirect vitality* as the amount in which other vital products and services contribute to the dependability of the vital service or product. Basically, this (backward) dependency information was already collected with the quick-scan questionnaire and only required validation and minor changes due to the amendments in the set of vital products and services. Note that we asked for the dependencies without any protection measures, meaning no back up, no redundancy, no alternate buffers or supplies. Then, it is relatively easy to determine for each product or service the (forward) dependent products and services and the levels of these dependencies.

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Secondly, we defined *direct vitality* as the contribution that a product or service delivers to the continuity of the society. This is equivalent to the amount of direct (first-order) damage caused by a loss or serious disruption of the product or service. As damage aspects we consider (life of) people, animals, economy, environment, and immaterial complacency. A group of damage-experts covering these fields scored all 31 products and services on these aspects. Due to time constraints, only a limited set of products and services were scored in a plenary session using electronic boardroom services and plenary discussions. Attention was required to make sure that only the direct first order impact was considered. Due to cascading effects via the dependency chain (indirect vitality) loss of a vital product or service may result in many subsequent damages. E.g. disruption of the natural gas provision causes problems with heating and cooking, but is affecting animal life only in a limited way. At the same time, electricity generation is hampered causing problems with ventilation of stables, thus may cause death of pigs and chicken due to overheating. Rather than directly counted as damage due to failure of the natural gas service provision, these effects are first-only effects of disruption of electricity services. Using the dependency matrix, all second, and higher order effects multiplied by the amount of dependencies, can be added to the first order effects to determine the total effect of loss or disruption of services upon society.

Study results

In order to assess the first-order direct vitality, all product and services were placed in a figure with on one axis the relative value of their direct vitality and on the other axis the relative value of their indirect vitality. Figure 1 illustratively shows the method used. The higher and/or more to the right, the more vital the product or service is to the society. The resulting list for the Netherlands is not very different from those found in the studies mentioned by Wenger, Metzger & Dunn (2002) where the energy sector, the human-oriented services like drinking water, food, and health services, and the telecommunication and transport sectors score high. It needs to be noted that most of the vital services are nowadays vitally supported by information and communication technology.

In the same way, the input from other vital products and services (amount of backward dependency) versus the level of delivered services (forward dependencies) were analysed using a figure like the illustrative figure shown in Figure 2. The higher, the more vital products and services are directly dependent. The more to the right, the more the production / delivery of the product or service is dependent upon other vital products and services. As example, air traffic is dependent upon many other vital services, but is not used much by other vital product and services. A product like electricity, on the other hand, mainly depends for its generation on another source of energy as well as upon the power distribution system. Electricity, however, is a vital source of energy for most other products and services and society at large as was already reported by Steetskamp and Van Wijk in 1994.
When looking more closely to Figure 2, the products and services placed in this figure belong to one of four quadrants: contributing (the top and left quadrant), loosely connected (bottom, left), entangled (top, right), and dependent (bottom, right).

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

The R&D team noted that the dependency of products and services on the Global Positioning System or GPS (Carrol, 2002; van Willigen, 2002), which itself is vulnerable for electronic disturbances, has probably been underrated by a number of vital products and services, e.g. mobile telecommunications, Internet and electricity provision. GPS is wired in a lot of these essential processes at a pretty low technical level providing time services.

The most public and private awareness raising result of the study is the simple web-like diagram of total and high interdependencies of the vital products and services as has been depicted in Figure 3.

The idea to look at the failure and recovery processes stems from earlier Swiss studies by Ernst Basler and Partner AG (Wenger, Metzger & Dunn, 2002). Figure 4 illustratively shows the combined failure (horizontally) and recovery (vertically) process characteristics for vital products and services. Here we determined how long it takes to reach the minimum quality level of the service after a service is disrupted, the moment the impact really hits society. The right hand side of the line starting at that point shows the moment that the impact is steady state. For instance, on the one hand failure of electricity supply may have an almost immediate impact, but after about eight hours irreversible damages occur (Steetskamp and Van Wijk, 1994). On the other hand, disruption of shipping will have effects upon society only after two to three months due to the large buffers in the harbours.
In the same way, the figure shows how long it takes after restarting the delivery of the product or service to the society before the minimum quality level is restored and the moment the recovery is complete. When electricity generation and distribution are restored, the actual recovery process for the consumers still may take a number of hours as reconnection can only be done in small steps. Second-order effects are for instance that train schedules will be disturbed for at least a day. Note that it will take years for certain products and services to fully recover either due to long-term environmental damage effects or due to a shift in modality or diversion of transport flows to other countries.

Looking at these failure and recovery aspects, we can split the products and services in five groups: (I) fast impact with slow recovery, e.g. water quality, (II) slow impact with slow recovery, e.g. shipping, (III) fast impact and fast recovery, e.g. telecommunications, (IV) slow impact with fast recovery, and (V) very fast impact and very fast recovery, e.g. emergency communications.
These differences between the products and services need to be taken into account when considering crisis management procedures for vital products and services. Some require almost split-minute reaction, blueprint procedures, and much training and exercises, while others allow a much slower decision process taking psychological (e.g. hoarding of goods) and long-term effects into account.

Summary and Conclusion

In a public-private effort, the Dutch nations' critical infrastructure has been determined. It consists of 11 vital sectors with 31 vital products and services.

In a structured way, we have obtained a good insight in all types of damage at a major scale that may occur when a product or service is disrupted or lost. In the same way, contributions to other vital products and services as well as dependencies on other vital products and services have been mapped.

The steps taken in the project largely raised the awareness of (inter)dependencies of vital products and services. Cascading effects due to failure of one infrastructure may occur due to the dependency chains. Figure 3 helped representatives of the vital public and private sectors to understand that efforts required to protect ones' own essential production and delivery processes, requires full understanding of and co-operation with other sectors. This wider infrastructure protection problem is much more complex, than the protection required by the millennium approach.

When regarding the protection of the critical infrastructure, most of the time one concentrates on the availability of the product or service. However, we put emphasis on not forgetting to protect integrity of the products and services as well.

Information and communication technology (ICT) is either as information transport medium or as a means for measure and control underpinning the essential processes of the vital products and services. ICT is however, by its supporting nature, not a separate vital product or service on its own. Thus, ICT needs to be covered by risk analysis efforts in each vital sector for each vital product or service.

Differences in failure and recovery process characteristics should be taken into account, both in nation-wide crisis management plans as well as in determining which vital products and services require priority in recovery processes.

International co-operation is required when vital infrastructures cross physical or virtual borders. The study found that the European Union does not play a co-ordinating or leading role (yet) in this topic area. Several international organisations are, however, actively organising cross-border assurance efforts.

Recommendations

Recommendations for governments and politicians

Organising public-private co-operation on critical infrastructure protection requires a strong vision and leadership by the government. Otherwise, certain sectors or products and services may fall behind. Given the complex, interwoven dependencies, the weakest link may jeopardise all other efforts.

For the same reason, co-ordination is required when dealing with sector-specific protective measures and action. Sector-specific sub-optimisation should be avoided to reduce the total costs. International co-operation and harmonisation should be stimulated as critical infrastructures extend cross-border, both in the physical sense as in cyberspace.

Our study noticed that only a few vital products and services have a quality management system monitoring a set of cross-sector agreed performance indicators and using that as a feedback for improving the quality. It is recommended to all vital products and services to start measuring key indicators right away if not in effect yet. Trend analysis, even when based upon some initial indicators, can be helpful to monitor the availability and integrity of the vital product or service. Unavailability of measurement data means no long-term insight based upon facts.

Recommendations and issues for R&D

As noted before, many vital products and services lack a cross-sector agreed system of performance indicators. Rather than developing them on a national basis, international standards shall be developed.

Further international study is required into the differences in failure and recovery processes. A broad and deep understanding of these figures is required in order to understand on the one hand the probability of cascading effects, and on the other hand the impact that a vital product or service may have via the dependency-chain.

An international comparative study on damage impact by disruption or loss of a vital product or service could give insight in which vital products/services may have the most impact when disrupted and need an international (e.g. EU) base-level of protection.

Acknowledgements

The project 'Quick-scan Bescherming Vitale Infrastructuur' was commissioned by the Dutch Ministry of Interior and supervised by the Interdepartmental Commission Critical Infrastructure (IWVI).
The authors are grateful for the support to the study by A.H. Nieuwenhuijs (MSc.), A.C. Kernkamp (MSc.), Mrs. K.Y. de Jong (MSc.), A.L.L.C.M. Bik (MSc.), J.M. Hoogstraten, and Mrs. E. Martis (MSc.).

References

Carroll, J. (2002); GPS Vulnerability Assessment. US Department of Transport. Cambridge, Massachusetts. [On-line] http://www.volpe.dot.gov/gps/pubs.html

Clinton, W.J. (1998), Presidential Directive 1998, number 63 (PDD 63): critical Infrastructure protection directive. Washington, D.C., USA. [On-line] Available: http://www.ciao.org

Cobb, A. (1997). Australia's vulnerability to information attacks. Australian Strategic and Defence Studies Centre, Australia. ISBN 07315 27232.

Cobb, A. (1999). Critical infrastructure attack: An investigation of the vulnerability of an OECD country. In Bosch, J.M.J., Luiijf, H.A.M., Mollema, A.M. (Eds.) NL ARMS – Netherlands Annual Review of Military Studies 1999: Information Operations. (pp. 201-.222). Tilburg University Press, Tilburg, The Netherlands. ISSN 0166-9982.

Luiijf, H.A.M. (1999a). Information assurance and the information society, In Gattiker, U.E., Pedersen, P., Petersen, K. (Eds.), EICAR 1999 Best paper proceedings, Aalborg, Denmark. ISBN: 87-987271-0-9.

Luiijf, H.A.M. (1999b). Information assurance: A long way to go. In Bosch, J.M.J., Luiijf, H.A.M., Mollema, A.M. (Eds.) NL ARMS – Netherlands annual review of military studies 1999: Information Operations. (pp. 137-.154). Tilburg University Press, Tilburg, The Netherlands. ISSN 0166-9982.

Luiijf, H.A.M., Klaver, M.H.A. (2000). Bitbreuk: Kwetsbaarheid van de Nederlandse ICT infrastructuur en de gevolgen voor de informatiemaatschappij. [In bits and pieces: Vulnerability of the Dutch ICT-infrastructure and the consequences for the information society]. Infodrome, Amsterdam. [On-line] Available: http://www.tno.nl.

PCCIP (1997). Critical foundations: Protecting America's infrastructures. Report 040-000-00699-1, United States Government Printing Office (GPO), Washington, D.C., USA. [On-line] Available: http://www.pccip.gov

Steetskamp, I., Van Wijk, A. (1994). Stroomloos, kwetsbaarheid van de samenleving: gevolgen van verstoringen van de elektriciteitsvoorziening [No power, vulnerability of the society: consequences of disturbances in electrical power delivery]. Rathenau Instituut, The Hague, The Netherlands.

Tweede Kamer (2001). Eerste voortgangsrapportage m.b.t. actieplan Terrorismebestrijding en veiligheid van 5 oktober 2001 [First progress report w.r.t. the action plan counter-terrorism and safety dated 5 October 2001]. Tweede Kamer der Staten-Generaal vergaderjaar 2001-2002, 27925(21), The Hague, The Netherlands.

Van Till, J., Luiijf, H.A.M., de Boer, Klaver, M.H.A., Huizenga, J.R., van de Sandt, C. (2001). KWINT: Samen werken voor veilig Internet verkeer, een e-deltaplan. [KWINT: Working together for a secure Internet, an electronic deltaplan]. Ministry of Transport, Public Work and Water Management, The Hague, The Netherlands. [On-line] Available: http://www.tno.nl.

Van Willigen, D. (2002). Radio Navigation: Perspectives and Challenges. Reelelektronika BV/ Gauss Research Foundation, The Netherlands.

Wenger, A., Metzger, J., Dunn, M. (eds.) (2002). International critical information infrastructure protection (CIIP) handbook: An inventory of protection policies in eight countries. Center for security studies and conflict research ETH, Zurich, Switzerland. [On-line] Available: http://www.isn.ethz.ch/crn

Table 1: Base types of underlying processes.

Input process	Value-addition process	Distribution process	Sample sectors / products and services
Incoming of raw materials	Production	Distribution	Energy, drinking water; food
Construction & maintenance of infrastructure	Development and delivery of service	Dispatch/ trans-shipment	Telecommunication, transport
Collect information	Analyse / process/ action-taking	Supply / communicate	Justice, broadcasting, civil governance, water management, private financial infrastructure
Deduct and collect money	Execute rules/ determination of payment amount to collect or to pay	Money transfer	Financial transfers by the Administration (e.g. tax, social services)
Be ready / dispatch centre	Information collection/ co-ordination/ dispatch	Turn out and incident management	Emergency services (e.g. ambulances and police)
Acquire material; recruitment and selection of personnel	Training	Operational deployment	Armed Forces

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS

Table 2: The 11 vital sectors and 31 vital products and services.

No.	Sector	Vital Product or Service
1	**Energy**	Electricity
2		Natural gas
3		Oil
4	**Telecommunications**	Permanent telecom infrastructure (e.g. POTS, leased lines, microwave links)
5		Mobile telecommunications
6		Radio communication and navigation
7		Satellite communication
8		Broadcasting
9		Internet-infrastructure and -access
10		Mail and courier services
11	**Drinking water**	Drinking water provision
12	**Food**	Food provision and food safety
13	**Health**	Health services
14	**Financial**	Private financial infrastructure (e.g. banks, financial services)
15		Financial transfers by the Administration (e.g. tax, social services)
16	**Management of**	Management of water quality
17	**surface water**	Management of water quantity (e.g. dike system, pumps, sluices)
18	**Public Order and**	Maintain public order (e.g. police)
19	**Public Safety**	Maintain public safety (e.g. fire fighting)
20	**Justice**	Jurisdiction and detention
21		Maintenance of justice
22	**Administration**	Diplomacy
23		Public information services
24		Armed Forces / Defence
25		Civil governance
26	**Transport**	Road transport
27		Rail transport
28		Air transport
29		Inland navigation
30		Shipping
31		Pipelines

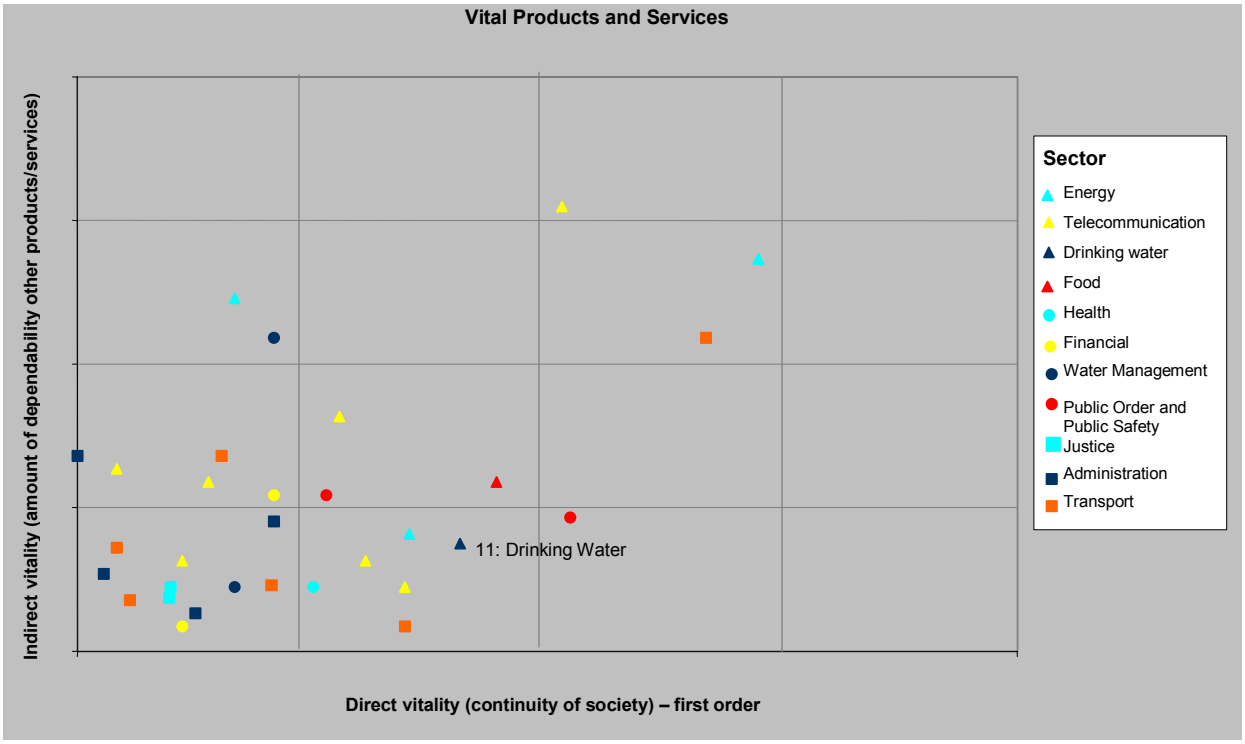

Figure 1: The direct vitality versus indirect vitality. The higher up and/or more to the right, the more vital the product or service is to society. (artificial example).

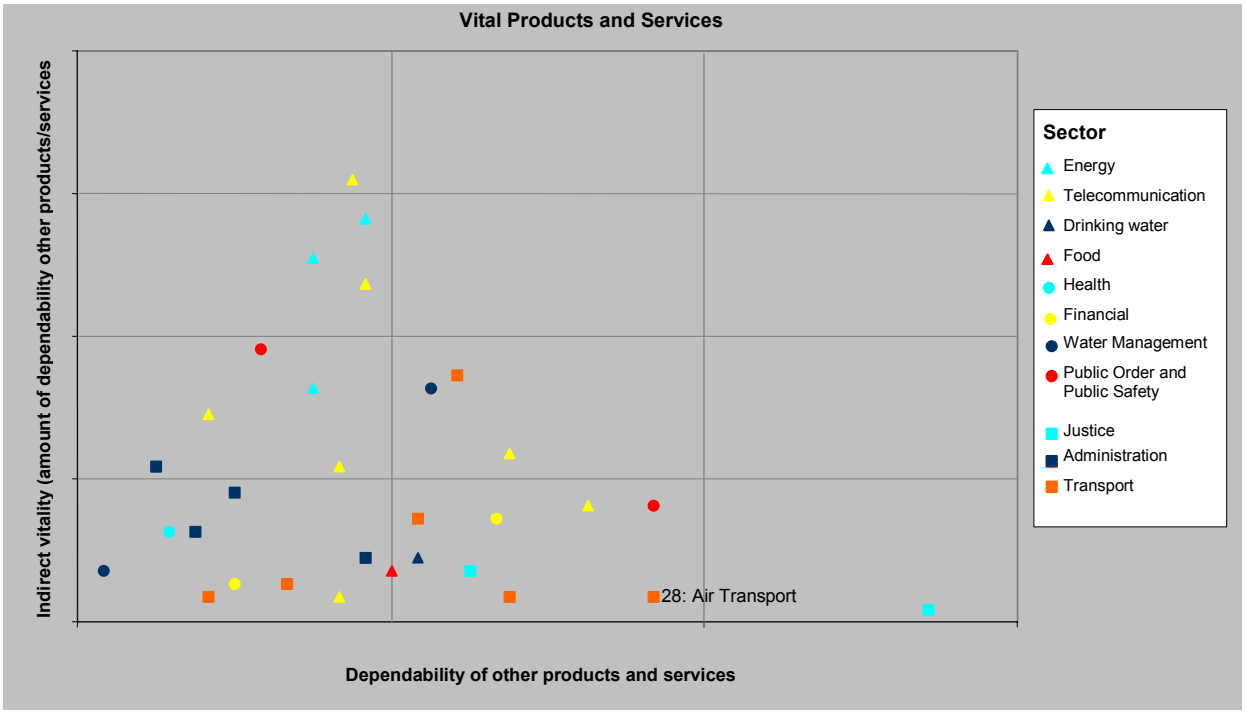

Figure 2: The own dependency (amount of backward dependency) versus the level of delivered services (forward dependencies). The higher, the more vital products and services are directly providing to other vital products and services. The more to the right, the more the production / delivery of the product or service is dependent upon other vital products and services (artificial example).

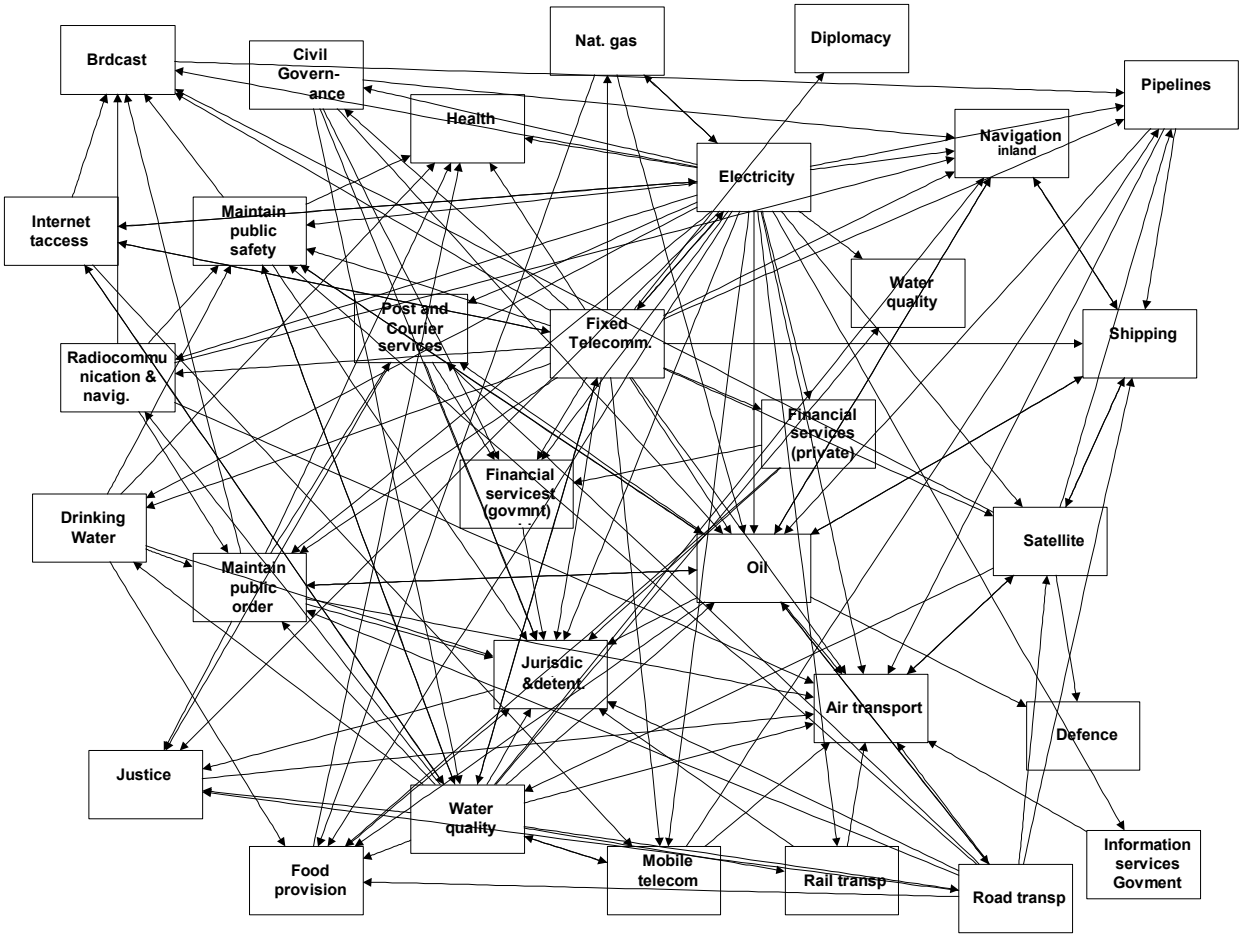

Figure 3: The complex web of (high and total) dependencies and interdependencies.

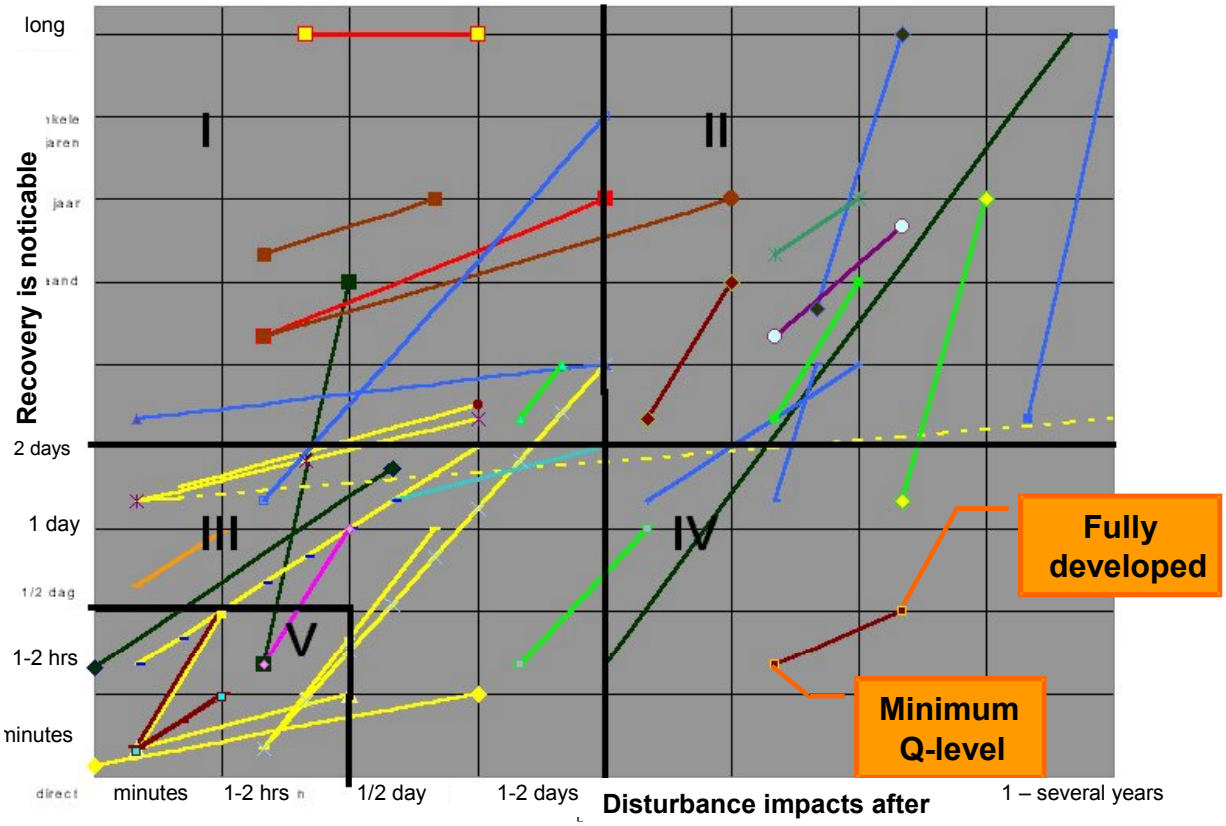

Figure 4: Failure (horizontally) and recovery (vertically) process characteristics (artificial example).

ISBN: 87-987271-2-5 EICAR Denmark c/o TIM-World ApS