Critical (information) Infrastructure Protection in The Netherlands

Eric A.M. Luiijf, Helen H. Burger, Marieke H.A. Klaver

TNO Physics and Electronics Laboratory (TNO-FEL)
P.O. Box 96864
2509 JG The Hague, The Netherlands
luiijf@fel.tno.nl
burger@fel.tno.nl
klaver@fel.tno.nl

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 those of neighbouring countries. Early 2002, the Dutch government started the Critical Infrastructure Protection (CIP) 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 phases of this project: a quick-scan determination of what critical products and services the nations' critical infrastructure is comprised of, the (inter)dependencies of these products and services, and the underlying essential processes. The paper outlines the project context and describes used methodologies, the results, and lessons learned.

1 Introduction to Critical (Information) Infrastructure Protection

As described in [Lui99a] and [Lui99b], several countries started reconsidering the vulnerability of their infrastructures in the last decade of the previous century. During the cold war, the protection of strategic infrastructures and objects was considered crucial for the survivability of a country. After the cold war, countries approached the possibility of disruption or disturbance of the critical infrastructure more lax as the fear for the red threat disappeared. They neglected the fact that both at the technology side and the threat spectrum paradigm shifts occurred. The millennium problem highlighted one of them: governments and industry were unable to predict whether information and communication technology (ICT)-based infrastructures could survive the millennium transition without failures of the critical infrastructure with cascading effects.

The United States and Australia were amongst the leading nations that sensed quite early an even larger problem [Cob97, Cob99]. The US Presidential Commission on Critical Infrastructure Protection (PCCIP) [PCC97] highlighted the vulnerability of the critical infrastructure (CI) at large and the ICT-dependent sectors in particular. The critical infrastructure is defined as „those facilities, services and information systems which are

so vital to a nation that their disruption or destruction would have a national and/or international debilitating impact on the security, economy, public health and safety, and the effective and smooth functioning of government at all levels, and society as a whole".

The first paradigm shift is that most of the critical infrastructure (CI) is monitored and controlled by ICT-systems with their inherent vulnerabilities. Our security and safety, health, economy, and way of life are highly dependent on the interrelated trio electricity, communications, and computer systems ([Lui99a]). The increasing complexity, (inter)-dependencies, and convergence of infrastructures increased the vulnerability of modern societies. This is amplified by common ground for failure due to the use the same type of commercial-off-the-shelf systems and software. The second paradigm shift occurred in the threat spectrum. Although, infrastructures have always been attractive targets, national borders provided some form of protection. Cyberspace changes this completely. Now, only a limited amount of resources is required to plan and execute serious attacks on our ICT-based critical infrastructure. This asymmetric threat by activists, irregular adversaries and terrorists replaced the well-known 'red' enemy threat. The events on September 11, 2001 globally increased the awareness and sense-of-urgency for this problem. For that reason, many countries started or intensified their on-going Critical (Information) Infrastructure Protection (C(I)IP)-activities.

2 C(I)IP programs in The Netherlands

Triggered by the millennium transition in The Netherlands, a sequence of projects on the vulnerability and protection of the Critical (Information) Infrastructure was started. Firstly, the Infodrome project looked at policy issues stemming from the deep penetration of ICT into all aspects of society. The Infodrome essay 'In Bits and Pieces' [Lui00] stimulated the public and political discussion on the increasing ICT-dependency of the Dutch society and the risk involved. The KWINT study [Til01] investigated the vulnerability of the Dutch part of the Internet. As a result, the Computer Emergency Response Team for the Dutch Administration (GOVCERT.NL), a malware alerting service for the public and Small and Medium Enterprises (SMEs), and a website on information security (www.SurfopSafe.nl) were established. On-going KWINT actions by the Dutch Platform for Electronic Business (ECP.NL) include the development of transparent performance indicators, the improvement of the reliability and continuity of the Dutch Internet, and SME-sector specific introductions to ISO/IEC 17799 standard.

Early 2001, the Dutch industry sectors asked the government for an integrated C(I)IP approach. The government reaction was accelerated by the occurrences on 11/09: the Dutch Security and Combating International Terrorism action plan [TK01] comprises the Dutch C(I)IP project 'Protection of the Dutch Critical Infrastructure (Bescherming Vitale Infrastructuur)'. Its objective is: „The development of an integrated set of measures to protect the infrastructure of government and industry (including ICT)". Phase 1 of the project is a quick-scan dependency study. The next sections discuss the first results of this quick-scan, the methodologies used, and lessons-learned.

3 Project „Protection of the Dutch Critical Infrastructure“

3.1 The CIP Quick-scan process

The quick-scan project aimed to obtain answers to the following three main questions:

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

Early 2002, we developed a questionnaire that was used to create an initial inventory of all products and services the Ministries regarded as critical, including their underlying processes and dependencies. After analysis, our findings were presented during a work session with over 70 key stakeholders representing the Dutch public and private critical infrastructure. In seventeen sector-specific workshops, experts broadly representing industry and government augmented and refined the information about their dependent key business processes. In this way, the gamut and interdependencies[1] of their critical products and services were coherently investigated with over 130 organisations, industries, government departments and agencies. In parallel, we organised an expert meeting with national experts on risk and damage assessment who assessed the direct consequences of the breakdown or disruption of critical infrastructure processes. An estimation of potential national and international damage was made in terms of casualty of people and animals, economic consequences, environmental consequences, and immaterial complacency including sociological and psychological effects on citizens.

All material from the questionnaires, work sessions, and desk research were then combined and analysed. Additionally, a short comparative analysis was undertaken on the international C(I)IP developments. From that 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, and SWIFT) are, however, actively organising cross-border critical infrastructure assurance efforts. Our reports [Lui03a, Lui03b] were completed early 2003 and delivered to the Dutch Cabinet and the Dutch Parliament. Both concurred with the findings in the report and agreed on starting the next phase of the C(I)IP project ‘Bescherming Vitale Infrastructuur’, the risk analysis and investigation which precautions and vulnerability-reducing measures are in place.

3.2 Determining the Dutch Critical Infrastructure

To determine what the Dutch national critical infrastructure is comprised of, it was necessary to determine what is ‚critical‘. Addressing this issue posed a problem as The Netherlands lacks a crisp deterministic definition of what is ‘critical’ to the society.

[1] 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.

Neither does an internationally accepted definition seem to exist. In order not to loose valuable time, a pragmatic approach was taken using the following working definition:

> *A product or service is critical 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, and (5) ecological environment, or when loss or disruption impacts citizens or government administration at an international or national scale or endangers the minimum quality level.*

This shifted the problem of the split between what is critical and what is essential towards agreeing upon the minimum quality level. This, however, is a political issue. It are the politicians who understand the political sensitivities and priorities (which in turn are highly influenced by the public) and determine the politically acceptable impact of a critical infrastructure disruption to society.

To investigate what comprises the Dutch critical infrastructure, we used a process-oriented approach. In the cold war days the critical infrastructure was determined by drafting long lists of so-called vital objects (e.g. harbour cranes, bridges, power plants). This approach is no longer valid since many infrastructures are interdependent with other critical infrastructures as their critical processes are chained. Moreover, ICT is the main interconnecting driver jeopardising the physical objects-only approach. For that reason, we identified the dependency chains of critical processes first. This, however, requires a top-down analysis of the processes that support the delivery of the critical products and services to the nation and of neighbouring nations in the classical physical sense and in cyberspace. An example that shows the difference in approach is that when a telecommunications company is asked to determine their critical infrastructure using the old-style object-oriented approach, they will table their most valuable assets first. However, the process-oriented approach makes an inventory of the dependent critical processes of the clients from the critical sectors. Other assets may then stand out as vital. For instance, a telephone switch with only a couple of hundreds of lines near a nuclear power plant could turn out to be one of the most critical assets of the nation.

Our investigation started with a questionnaire per potential critical product or service asking for (1) a short description of the product/service; (2) existing legal dependability requirements[2]; (3) a critical process view by splitting the provision of the service or product into underlying input, value-addition, and distribution processes; (4) per underlying process an assessment of the level of dependency of each of the other critical products and services (none/ low/ medium/ high/ total); (5) failure and recovery characteristics; (6) importance in terms of the aspects people, animals, economy, environment, and immaterial complacency; and (7) the assessment of how other products or services depend upon ones' own product or service. The analysis gave a good initial view on highly dependent and interdependent products and services. Weaknesses in this view stemmed from the limited involvement of industry sectors - which are responsible

[2] It should be noted here that the dependability as studied comprises both availability and integrity. For example, access to a database of a hospital can be working, thus available, but when the database delivers garbled output or mixed patient data, the system is not of use.

for providing over half of the critical services - and due to a stunning lack of understanding of ones' dependent clients. The latter was found because we compared the answers to the question sets (4) and (7). Instead of a limited number of small mismatches, many large positive and negative discrepancies were noted. This led to the conclusion that the producers and providers of critical products and services have a very unbalanced and limited understanding of their own importance for others, with the risk of wrong contingency priorities.

Table 1: The 11 Dutch critical sectors and their 31 critical products and services

No.	Sector	Product or service
1	**Energy**	Electricity
2		Natural gas
3		Oil
4	**Telecommunications**	Fixed telecommunication networks services [3]
5		Mobile telecommunication services
6		Radio communication and navigation
7		Satellite communication and General Positioning System
8		Broadcast services (radio and TV)
9		Internet access
10		Postal and courier services
11	**Drinking water**	Drinking water supply
12	**Food**	Food supply and food safety
13	**Health**	Health care
14	**Financial**	Financial services and financial infrastructure (private)
15		Financial transfer services (government)
16	**Retaining and managing**	Management of water quality
17	**surface water**	Retaining and managing water quantity
18	**Public Order and Safety**	Maintaining public order
19		Maintaining public safety
20	**Legal order**	Administration of justice and detention
21		Law enforcement
22	**Public administration**	Diplomacy
23		Information provision by the government [4]
24		Armed Forces / Defence (emergency support tasks)
25		Public administration
26	**Transport**	Road transport
27		Rail transport
28		Air transport
29		Inland navigation
30		Ocean shipping
31		Pipelines

[3] This includes POTS, microwave links, cable and leased lines.

[4] This comprises weather service, citizenship registries and other public information services, etceteras.

During the refinement phase, the project team intended to stimulate public awareness, to increase the applicability of the results and to remove inconsistencies. One of the first activities was to agree upon the set of sectors, products and services that compose the critical infrastructure. This was accomplished by analysing of the underlying processes of the initial set of products and services. Some clustering of products and services could take place as those services are generally based upon the same type of underlying processes (e.g. collecting money, calculate according to rules, redistribute money for tax, social security, schools etc.). In principle, the protection of these critical services requires the same base set of protection measures. Based on this analysis, the Dutch industry sectors and the government settled the nations' critical infrastructure to enclose 11 critical sectors with 31 critical products and services (Table 1).

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

In the same way *direct vitality* was defined as the contribution that a product or service delivers to the continuity and wellbeing of society. This is equivalent to the amount of direct (first-order) damage caused by loss or serious disruption of a critical product or service. A group of damage-experts covering these fields scored for all 31 critical products and services the impact of disruption of a critical product or service on (life of) people, animals, economy, environment, and immaterial complacency. Attention was required to make sure that only the direct first order impact was considered, in order to obtain a clear understanding of (inter)dependencies.

3.3 Study results

In order to assess the first-order direct vitality, Figure 1 shows all critical products and services with the relative value of their direct vitality on the x-axis and the relative value of their indirect vitality on the y-axis. As simple mapping from total, high, medium, and low to a numeric value was used to determine the relative position. The higher and/or more to the right, the more critical the product or service is to the Dutch society. The results are not very different from those found in studies by other nations (see [Wen02]), where the energy sector, the human-oriented services like drinking water, food, and health services, and the telecommunication and transport sectors turn out to be the most critical. Our study, however, made an independent assessment of the relative measure of criticality rather than using a rule of thumb list. Moreover, it is easy to see that the Netherlands is highly ICT-dependent as the information-infrastructure products and services stand-out.

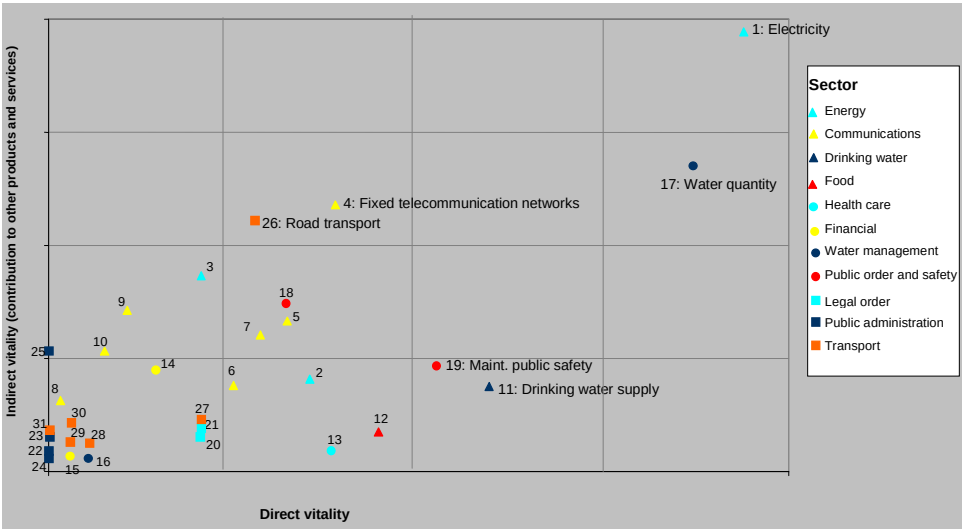

Figure 1: The direct vitality versus indirect vitality. The higher and/or more to the right, the more critical the product or service is to society.

The R&D team noted that the dependency of products and services on the Global Positioning System or GPS [Ca02] and [Wil02], which itself is vulnerable for electronic disturbances, is probably underrated by a number of the critical sectors including mobile telecommunications, Internet and electrical power provision. GPS providing time services is wired in a lot of these critical processes at a pretty low technical level and for that reason probably overlooked.

In the same way, the input from other critical products and services (amount of backward dependency) versus the level of delivered services (forward dependency) are depicted by Figure 2. The higher, the more critical products and services are directly dependent. The more to the right, the more the production or delivery of the product or service is dependent upon other critical products and services. As example, air traffic is heavily dependent upon many critical services, but is not used much by any of the other critical product and services. On the other hand, a product like electrical power mainly depends for its generation on a source of energy as well as on the power distribution grid. Electrical power, by the way, is critical to the provision of most other critical products and services as well as to the society at large, something that was already reported in [Ste94].

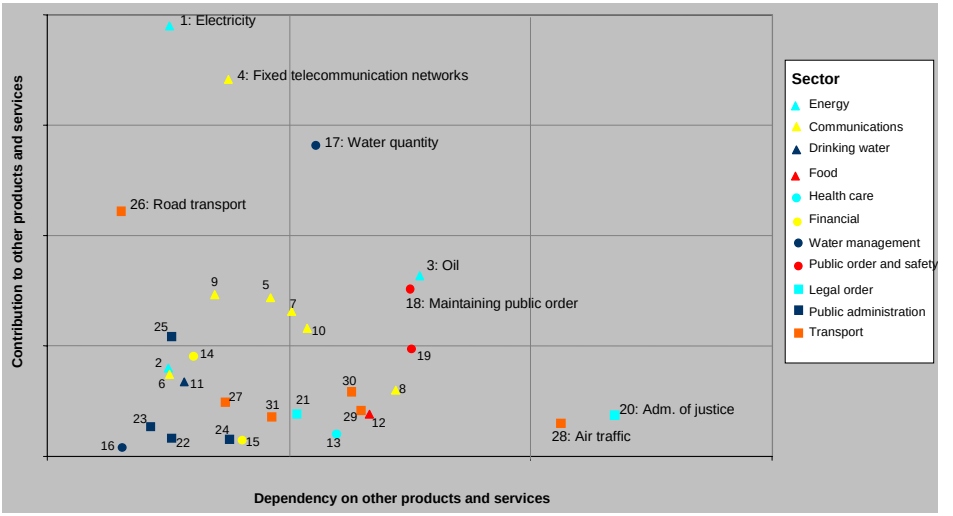

Figure 2: The own dependability (amount of backward dependency) versus the delivered services to other critical sectors. The higher, the more a critical product/service is vital to other critical products/services. The more to the right, the more dependent a critical product/service is to other critical products/services. The main ICT-based products and services stand out.

Both Figure 1 and Figure 2 show that the main ICT-based telecommunications and financial sectors stand out in their vital importance for other sectors. The Internet is surprisingly already a vital resource to many other critical products and services. As example, 15% of the Dutch power market is traded via the Internet at the Amsterdam Power Exchange where European-wide the power consumption and generation markets meet and settle MWh prices.

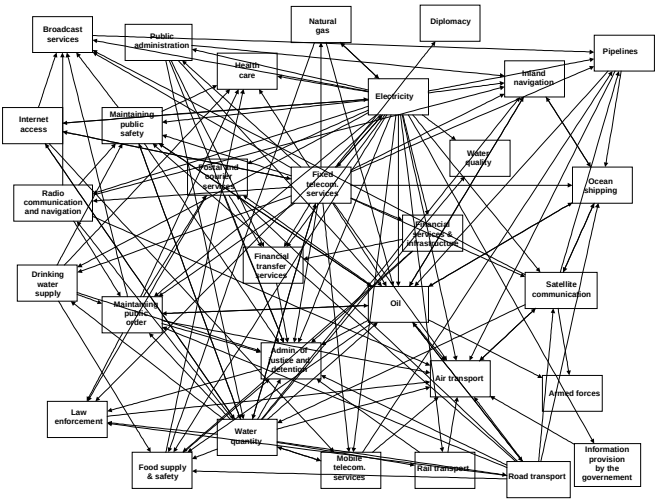

Figure 3: The complex webcob of (high and total) dependencies and interdependencies.

For that reason, the Dutch government and the private industry collaborate to increase the assurance of these infrastructures. CIIP-projects like the aforementioned KWINT and NACOTEL (National platform for the Continuity of Telecommunications) are case in point. Of help with that is Figure 3. This is the most public and private awareness raising result of the study, the simple but complex cobweb of total and high level dependencies between the critical products and services.

4 Conclusion and future

In a public-private effort, the Dutch nations' critical infrastructure has been determined. It is composed of 11 critical sectors with 31 critical products and services (Table 1). In a structured way, a good insight in all types of damage at a major scale that may occur when a product or service is disrupted (integrity and/or availability) or lost is obtained. In the same way, contributions to other critical products and services as well as dependencies on other critical products and services have been mapped. Uniquely, the relative vitality of the various critical products and services have been determined, both for indirect vitality and direct vitality.

The project thus far largely raised the awareness of all the Dutch critical infrastructure stake-holders about their (inter)dependencies and the importance of their products and services for other critical sectors. Simple figures like Figure 3 helped in understanding that efforts required to protect ones' own critical production and delivery processes requires the full understanding of and co-operation with other critical sectors. It was concluded that cascading effects due to failure of one infrastructure via the dependency chains can not be excluded. As result, the wider infrastructure protection problem is much more complex than most stakeholders expected as they are just one node in a web of dependencies. Securing the availability and integrity of a critical product or service also requires sufficient availability and integrity of the critical business processes' supply chains.

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 critical products and services. ICT is, however, by its supporting nature, in the Dutch opinion not a separate critical product or service on its own. Thus, ICT dependency and vulnerability need to be covered by risk analysis efforts in each critical sector for each critical product or service.

Public-private co-operation to tackle the critical infrastructure protection problem requires a strong vision and leadership by the government. A stick and carrot approach is required. Otherwise, the protection of certain critical sectors may fall behind. Given the complex, interwoven dependencies, the weakest link may jeopardise most 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 critical 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 service quality. It was recommended to all critical sectors to start measuring key performance indicators right away if not in effect yet. These key performance indicators shall preferably be based on – in a number of cases to be developed - international standards. Trend analysis, even when based upon some initial indicators, can be helpful to monitor the availability and integrity of the critical product or service. Unavailability of measurement data means no long-term insight based upon facts.[5]

Further international study is required into the differences of failure and recovery processes of the various critical sectors. 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 critical product or service may have via the dependency-chain.

International co-operation is required when critical infrastructures cross physical or cyberspace borders. Especially, critical information infrastructures and information-based infrastructures tend to have international impact in case of disruption or loss. Our 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.

5 Acknowledgements

The project 'Quick-scan Bescherming Vitale Infrastructuur' was commissioned by the Dutch Ministry of the Interior and Kingdom Relations. 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

[Ca02] Carroll, J. (2002); GPS Vulnerability Assessment. US Department of Transport. Cambridge, Massachusetts. [On-line] http://www.volpe.dot.gov/gps/pubs.html

[Cli02] 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

[Cob97] Cobb, A. (1997). Australia's vulnerability to information attacks. Australian Strategic and Defence Studies Centre, Australia. ISBN 07315 27232.

[5] In effect, the Dutch Ministry of Economic Affairs announced regulations ordering the electrical power distribution industry to register all performance problems and disturbances with an independent registry organisation which is transparent to the public.

[Cob99] 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.

[Lui99a] 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.

[Lui99b] 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.

[Lui00] 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.

[Lui03a] Luiijf, H.A.M., Burger, H.H., Klaver, M.H.A. (2003). Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten (managementdeel). [Critical Infrastructure Protection: Quick-scan of critical products and services – management report]. TNO-report FEL-03-C001, The Hague, The Netherlands.

[Lui03b] Luiijf, H.A.M., Nieuwenhuijs, A.H., Kernkamp, A.C., de Jong, K.Y., Burger, H.H., Bik, A.L.L.C.M., Hoogstraten, J.M. (2003). Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten. [Critical Infrastructure Protection: Quick-scan of critical products and services]. TNO-report FEL-03-C002, The Hague, The Netherlands.

[PCC97] 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

[Ste94] 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.

[TK01] 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.

[Til01] 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.

[Wil02] Van Willigen, D. (2002). Radio Navigation: Perspectives and Challenges. Reelelektronika BV/ Gauss Research Foundation, The Netherlands.

[Wen02] 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