ICT IN BITS AND PIECES ON THE VULNERABILITY OF INFORMATION-INFRASTRUCTURES

H.A.M. Luiijf
TNO Physics and Electronics Laboratory
P.O. Box 96864, 2509 JG The Hague, The Netherlands
phone +31 70 374 0312, fax +31 70 374 0651, luiijf@fel.tno.nl

Abstract
Information Operations studies in the Netherlands made the Dutch Ministry of Defence (MoD) aware that both military and public information-infrastructures can be target for hostile information operations. As a result, MoD stimulated discussions within the Dutch government on the threat to and vulnerability of Dutch critical infrastructures. This paper describes critical infrastructures protection studies that the Dutch government initiated in the last 2 years in order to address the threats, vulnerabilities, and the possible urgency to resolve them.

The paper highlights Information Operations, risks and threats to the information age society, and the need for public-private partnership to address Critical information-Infrastructure Protection (CIP). Issues covered are: prevention of incidents, reduction of critical infrastructure vulnerabilities to an acceptable level for society, and ensuring that control of the critical infrastructure is restored as quickly as possible. The latter in case a high-impact disturbance affects the information infrastructure.

Some of the processes, models and analysis techniques that we used in the vulnerability analysis of the Dutch Internet are described. The development of a set of related models was required to clarify the roles, diversity and inter-dependencies between the government, users, and market actors. Infrastructure protection initiatives and activities in other countries were investigated in order to understand the lessons learned and to avoid pitfalls. Classifying these international initiatives resulted in a number of interesting observations. The action lines stemming from the studies are discussed shortly.

Keywords: information operations, critical infrastructure protection, modelling, vulnerability, quality of service

1. Introduction

In 1999, the Dutch and German Ministries of Defence (MoD) completed a joint study on the prerequisites and implications of the new phenomena Information Operations (Info Ops) within Multinational Operations of Armed Forces (InfoOps1999). After this study, the MoD established a Defence working group on Information Operations, the WGIOD. The WGIOD completed the Netherlands Info Ops policy early 2001, which was endorsed by the Dutch Minister of Defence on April 2, 2001. Info Ops are defined as "actions taken to influence decision-makers in support of political and military objectives by affecting the opponents' information, decision-making processes, C2-means, and supporting communication and information systems, while exploiting and protecting one's own information and/or information and communication systems."

This definition follows the NATO MC422(1999) Info Ops definition. Info Ops encompasses the co-ordination and harmonisation of number of military and non-military focus areas like for instance C2-warfare, political and diplomatic activities.

Both the joint German-Dutch study Information Operations and the recent Dutch Info Ops policy document identify the issue of asymmetrical threats. This made the Dutch Ministry of Defence aware that the Dutch civil information-infrastructures can be a target for hostile information operations. It became clear that, when looking at the thriving information and communication technology developments, especially those of the Internet, a downside for our society might occur when the vulnerabilities of critical information infrastructures are not properly addressed. Not only in the military cyberspace – cyber warfare realm (Luiijf, 1999) - but also in our everyday information-age society, people, organisations, agencies and governments are confronted with threats against, and vulnerabilities of, our information infrastructure and information systems. At the same time, our economy and even our safety rely increasingly on the integrity, availability, and reliability of information and communication systems and infrastructures.

Government decision-making units, organisations, society, and critical industries have become increasingly inter-networked, interdependent and entangled. They rely heavily, if not totally, on essential, global and converging infrastructures. These infrastructures are managed using the same complex information and communication technology and infrastructures. And the information infrastructures increasingly depend on Internet Protocol (IP) based subsystems, from end-user screen to end-user screen, including private and corporate networks. Due to these factors, society is now facing new global threats with causes that can vary from (simple) unintentional, technical, natural and intentional causes to acts-of-God. Non-military organisations (NMO's), terrorist and action groups and other adversaries can pose many threats for the new information age society. Since September 11th, society understands that hypothetical threats may become reality. It is not anymore the question whether but when an incident or attack will occur.

The outcome of the US Presidential Commission on Critical Infrastructure Protection study (PCCIP, 1997) triggered the attention of several governments. Critical infrastructure studies were commissioned in a number of countries. The Dutch government, however, at that time concentrated its efforts at controlling the millennium problem. At the start of 2000, several Dutch ministries with the MoD in the lead put the critical infrastructure topic on the agenda of the Infodrome project. Infodrome is a strategic project exploring the role that the Dutch government has to play in the information society of the future.
Early 2000, Infodrome commissioned the writing of an essay on critical information infrastructures. The goal of this essay was to validate the notion of emerging risks and to stimulate a broad public and political discussion. The essay (Luiijf, 2000) with the title BITBREUK ("In Bits and Pieces") highlighted the increasing vulnerability of the ICT-based Dutch society.

In parallel, the Dutch Ministry for Transport, Public Works and Water Management (MoT for short) is responsible for policy development with respect to infrastructures. The MoT commissioned Stratix Consulting BV and TNO in June 2000 to undertake

an in-depth 'KWetsbaarheden INTernet' (KWINT) study on the vulnerability of the (Netherlands section of the) Internet.

Below, the outline of both studies is presented. The threats to critical information-infrastructures at large are discussed in sections 2 to 4. In the succeeding sections, the KWINT-study on the vulnerability of the Internet, is described as an example on how complex problem with many public and private actors can be addressed. The results of the studies are briefly described.

2. Paradoxes

One of the vulnerabilities for society, as highlighted in many international studies, is the vulnerability of (critical) infrastructures. These vulnerabilities were well understood by our civil defences. However, the fast up-rise of the inter-networked, dependable, intertwined, and converged ICT-based infrastructures created a new problem for information-based societies. If the availability, integrity or even the confidentiality of the information systems is compromised in any way, whether deliberately or inadvertently, this could produce devastating scenarios not only for sections of our national society but also for sections of international society. At the end of the day, the information society owes its continued existence to the reliable functioning of a highly complex entity of interconnected networks and network-based services.

According to the "Stroomloos"-report[1], the vulnerability of society to undesirable (technical) malfunctions, undesirable human behaviour and undesirable natural phenomena such as natural disasters and 'acts of God' may give rise to serious social disruption (Steetskamp and van Wijk, 1994:10). The sources used by these authors serve to highlight the vulnerability paradox:

> *"The less vulnerable a country becomes in terms of public utilities, the harder it is hit by any disruption in the production, distribution and consumption of those utilities".*

The Dutch Millennium Platform, too, worked from the assumption that an electrical power failure lasting more than eight hours would give rise to serious disruption of society, and drew up its emergency plans accordingly. The "Stroomloos"-report claims that, compared to the situation abroad, the risk of disruption to electricity supplies is low (meaning a high degree of availability). However, according to Steetskamp and van Wijk (1994: 10), this stability, coupled with a heavy increase in consumption in society, even goes so far as to create a *double* vulnerability paradox:

> *"At the same time, society will increasingly use such an infrastructure service because it seems to be so reliable".*

The latter is a human perception issue, as the conclusion is not necessarily based on any measurable reality!

Recent incidents involving electrical power supply and communication infrastructures suggest that that this double paradox with respect to the availability also applies to ICT-infrastructures. If, on top of this, we include the vulnerability of integrity,

[1] Stroomloos = disruption of the electrical power distribution

confidentiality, and privacy (e.g., doubts in public confidence in financial transactions via public networks), then it is clear that the vulnerability of critical ICT-infrastructures may well become, or already is, the Achilles heel of any ICT-based society.

Social resilience declines sharply as a function of increased perception of the reliability of infrastructure services. The "Stroomloos"-report points out (Steetskamp and van Wijk, 1994:20): "*In addition, social resilience is not high because risk-awareness among citizens, companies, institutions, public services and government is not particularly high. People are unaware of the potential social consequences and do not view the situation as threatening*" and "*after eight hours, disruption of society as a whole can assume disastrous proportions. This is especially the case when the disruption affects a large area and there are signs that it will last for more than 24 hours.*"
Serious disruptions to the ICT-based infrastructures could lead to a similar situation after a couple of hours, given that our society is becoming increasingly dependent on chain processes such as electronic payment, logistical just-in-time systems, etc.

3. About Theats and Intentions.

Caused by the increased connectivity, the threats to ICT have shifted from some malicious person who needed to be physically near the system to someone who attacks you via Cyberspace from some place on our globe. In fact, an attacker in the Sahara dessert using a laptop and satellite up-link might be nearer to you in Cyberspace than the bakery-around-the-corner.
When looking at the Cybercrime threat, the most visible are the web-defacements. Script-kiddies (the one's that use scripts to repeatedly use well-known vulnerabilities to break into systems) and hackers that collect "hack-miles" show the penetration of the system by modifying or replacing a web page from for instance a Ministry. This so-called Cyber graffiti is relatively harmless, although it causes 90% to 95% of the "knocks on the ICT-doors" and thus a certain performance loss and management attention.
A second class of threats is caused by viruses, worms and Trojan Horses. To cause harm, they most of the time require co-operation of a human in the organisation itself which unconsciously starts a program attached to an email from unknown source or just likes the email with the subject "I Love You"...
With proper system and security management controls as well as user security training, the threats mentioned above can be considerably lowered as well as the impact to an organisation. One should not forget that the attack tools are becoming increasingly sophisticated and require less basic knowledge over time.

Another class of threats is criminal organisations and intelligence brokers that use hackers to obtain money or valuable proprietary information of companies and organisations. They seldom make news headlines as companies take their losses and not the blame, if the Cyber crime is detected at all. Unless the trust in financial institutions is lost, this type of crime does not impact society and economics yet.

Activists in Cyber space are supporting a cause, e.g. are supporting a freedom-fighting movement or are against the killing of animals for the humans food-chain. They can organise a temporary denial-of-service of systems and networks, the electronic equivalent of a sit-in protest, or deface home pages of high-profile organisations. A democratic society can tolerate such e-sit-in outages as long as the harmful effect is proportional and not causing casualties. Examples are the actions of

the Electronic Disturbance Theatre (EDT) in support of the Mexican Zapatistas, the East Timor independence hacker movement, and the supporting tools development for e-actions by the electrohippies collective.

For political-military freedom to decide, society as a whole, and the economy, the largest Cyber threats with high impact can be caused by hacktivists, Cyber terrorists, and offensive Cyber Information Operations by state actors.
Activists that pass the line of violence and irreversible damage are called hacktivists. They may try to damage systems and functions of the organisations and their supporting environment they disagree with. Examples are hacktivists that tried to block and damage WTO systems, email bombs and viruses targeted to NATO (member) information systems during the Kosovo-conflict, a clean-wiped database of a hospital during the e-fights between Azerbaijan and Armenia, and a system of the High-Count in Japan that had all its files removed.
The next threats are those against critical information-infrastructures with the intend to cause irreversible direct or indirect damage to people, society and economy. Cyber terrorists might, for various reasons, attack either the hardware and connections (physical damage, HERF-devices) or by other methods attack vital information systems to attack their integrity (e.g. changed blood types or changed medical treatment records in a hospital system), their availability or exclusivity.

Apart from these external threats we never should forget the 60-80% of insider threats that may cause damage, the technical and natural causes, and just acts-of-God.

4. In Bits and Pieces.

In our critical information-infrastructure studies for the Dutch government, we identified different layers at which disruption of or damage to critical information-infrastructures may have a disastrous high-level impact upon individual people, our society, and our (globally inter-networked, interdependent and entangled) economy. In our Bitbreuk-study (in English: In Bits and Pieces), such "breakages" may occur at the layers of: electrical power distribution, the communication link infrastructure (e.g., dig through of fibre cables), failure of electronic services, and loss of confidence in the information society by the society (e.g., electronic banking is distrusted). For these reasons, it is very important that it is not all about availability, but factors of integrity, privacy, and confidentiality are equal Important when considering critical information-infrastructure protection.

Relatively simple software or hardware failures at the various layers make news at either the front or the third page almost on a daily basis. Although this shows the impact of ICT on society, these outages are most of the time regarded as bad luck rather than as an warning call. People with the intention to harm groups of people, the society and/or the economy, can easily deduct from the newspapers where the Single Points of Failure (SPoFs) in information-infrastructures are. They can estimate the impact in case of deliberate actions against such an infrastructure, knowing that contingency plans are often lacking or partially implemented.

Some examples: 1700 Post offices in the Netherlands stay closed as a computer download could not occur due to a system failure; a computer failures causes 70% of all trains in The Netherlands to be halted for several hours and a couple of 100.000 people stranded at the platforms; a steal beam cuts four glass fibre cables and causes all telephony, data traffic and alarm communication in three provinces of the Netherlands to be disrupted for almost 10 hours; outage of the Galaxy IV satellite troubled the organisation in US hospitals as doctors and other personnel could not be addressed anymore by beepers.

5. The KWINT-project and the methodology used

The 'KWetsbaarheden INTernet' (KWINT) study on the vulnerability of the (Netherlands section of the) Internet took place from July 2000 till December 2000. It can be regarded as an example of how we addressed the vulnerable information society and its underlying vulnerable information-infrastructures. The KWINT objectives for study were to answer the following questions: (1) what are the current vulnerabilities of the (Dutch section of the) Internet?; (2) what are the developments that can be foreseen in the next three years?; (3) what are the possible consequences in case an identified threat becomes reality?; (4) which actors play a role?; (5) which measures need to be taken to reduce the vulnerabilities, if any?. 'Internet' was defined end-to-end in this study, including workstations, private- and public IP-networks and information systems on servers.
These intermediate results were the basis for getting the answers to the two crucial questions: (1) is there a need to increase the security and trustworthiness of the Internet and, if so, how and by which actor(s)?; (2) what are the policy recommendations for the Dutch government?

As government departments and a number of market actors did have neither a clear understanding of the risks nor the sense of urgency to act expediently, considerable time was devoted in the KWINT project to reach a common understanding. After all, the development of policy requires broad support from all actors for the proposed policy direction and the initial measures that need to be taken.

As the KWINT-project had to be completed within six months, several activities were undertaken in parallel. Firstly, a common set of definitions based upon the information security regulations for the Dutch government as defined in (VIR, 1994) were selected. Subsequently, a number of related models were developed in order to make the complexity of the problem manageable in further studies. These were used for a high-level vulnerability-analysis by experts. A survey of international CIP and Internet security initiatives took place. Intermediate results of the vulnerability analysis were put forward for validation in a workshops with representatives of market actors (e.g. service and telecom providers, banks), employer and consumer organisations, and government departments. The consultation was used to determine the level of urgency and support for addressing the vulnerabilities of the Internet. With the input of these actors, a number of recommendations and measures were drafted. In two workshops, one with the same actors and another with government policy-makers from various ministries involved in ICT-policies, these drafts were discussed. The final KWINT-report (Stratix/TNO, 2001) was completed and released on 12th January, 2001.

6. The Models

The issues in the "vulnerabilities of the Internet" are numerous, complex and multi-facetted. The information infrastructure can deteriorate in many ways. Power outages, cable cuts, failures in network switches, problems in the national DNS (domain name service) infrastructure, confidentiality problems of a TTP (trusted third party service), failure of a critical chain of financial transactions, to name but a few.

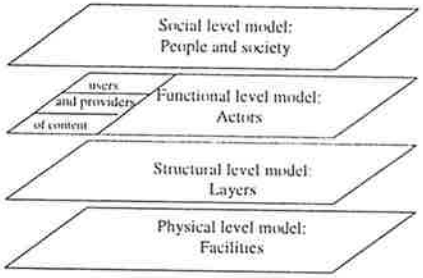

Figure 1: Four levels of models.

There are a multitude of market-driven actors involved at many different layers: infrastructure providers, service providers, application services, business-to-business users as well as customers, and, last but by no means least, the Dutch government as both user, provider and possibly regulator.
In the available literature, not many usable models were found to access the complex dependability and other vulnerabilities, their impact to society, and the many actors involved in the provision of Internet services. Only recently, a dependability model was described in (Kyriakopoulos and Wilikens, 2001). It became necessary to develop four levels of models (Figure 1) with different orthogonal points of view, in order to address and clarify the various actor roles, the diversity, inter-dependencies and vulnerabilities. The society level model was used to discuss the motives and economics behind the Internet developments. This model was used to explain the dynamics of the Internet developments: the current chaining of services by multiple organisations in all sectors of society and the strong bottom-up streams of new ideas that influence all facets of the Internet.

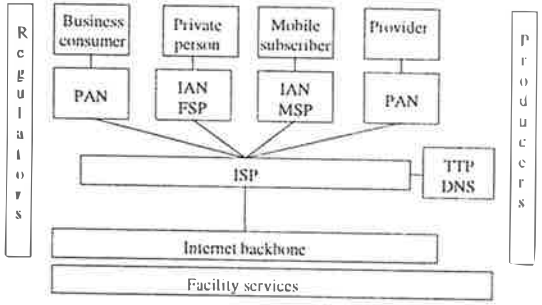

Figure 2: Functional model with types of actors.

The functional level model (Figure 2) was used as an intermediate between the functions the user (individual, groups, SMEs, organisations) experience and the more abstract level of models underneath, as described in Figure 1. In brief: various types of users connected by way of private access networks (PAN), Internet access networks (IAN) and fixed or mobile access service providers (FSP/MSP) are recognised. Users may be both consumers and providers of information. Market actors may fulfil more of these roles. The Internet types of actors are: (1) users/consumers of services; (2) providers of information and transaction services; (3) access network providers; (4) Internet service providers (ISPs); (5) basic

application service providers (DNSs, ASPs, TTPs); (6) backbone transmission-capacity providers; (7) regulators (IETF, ITU, ETSI; governments); (8) software and hardware producers enabling Internet functionality; (9) facility services (buildings, power, security, added-value services, etc.).

The Stratix basic layer model (Figure 3), based on the so-called 'Tillevision Model' (van Till, 1993), was used to investigate the market areas of service providers and of product suppliers. All private and enterprise user information and transaction facilities can be found in the information layer. Generic application layer functions like domain name services, protocol converters (e.g. Email to SMS), Trusted Third Party services, e-mail post offices can be found on the application layer. At the network layer in this model, IP-data is exchanged between end-user systems and ISP's and between ISP's. The transmission layer takes care of the physical transport of the digital information. Horizontally, the geographical reach is depicted as not all actors aim to play in the same geographical area., e.g. the .nl- top-level domain has a national scope while the .com domain name service provider has a global customer base.

Besides the placement of actors and functions in the structural level model, the physical location of the operational facilities is of importance when analysing vulnerabilities. For the actors (including the users), a geographical or horizontal chain dependency often exists, e.g. many countries peer (inter-connect) their Internet in the US. Peering and co-location centres, concentrations of points-of-presence, and web hosting in 'data hotels' can be a potential single-point-of-failure if redundancy is not taken into account.

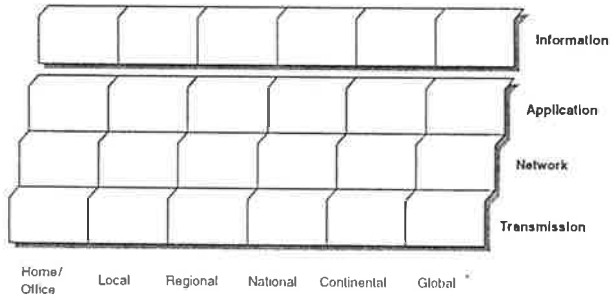

Figure 3: Basic layer model.

7. Reliability indicators

How reliable is the (Netherlands) Internet as critical information infrastructure? To answer that question, a systematic collection of incidents and relevant indicators for confidentiality, integrity, availability and performance (quality of service) is required. This information is required for transparency of service provision and to obtain an objective view on the information assurance of the Dutch Internet. It was found that only a limited number of aspects are measured by service providers in a non-uniform way. We identified a number of international research activities in this area, e.g. (CAIDA, 2000; IPPM, 2000; OESO, 1998), but there is not yet a transparent internationally accepted set of reliability indicators. However, the Union of Netherlands Internet Service Providers is working on a quality label approach, which states a number of reliability requirements (NLIP, 2001). KWINT concludes that the development of internationally accepted set of reliability indicators is required for a

government that wants to protect the rights of its citizens by stimulating a liberated but transparent market.

8. Vulnerability analysis of (the Netherlands section of) the Internet

The high-level vulnerability analysis required yet another layered model that was derived from extending the basic layer model with an infrastructures logical and physical interaction layer (convergence and entanglement), and the physical environment. For these six layer domains the weaknesses, threat probability (high, medium, low) and their possible impact (high, medium, low) were categorised by distinct area of responsibility.

Table 1: Decision table (H = High; M = Medium; L = Low)

Domain	Chance	Impact L	Impact M	Impact H
One single area of management control and responsibility (single actor)	L			
	M			
	H			
Multiple management control and responsibility areas	L			
	M			
	H			
Multiple areas; international scale	L			
	M			
	H			

The responsibility domains are: one single domain of management control and responsibility (e.g. a single Bank or Internet Service Povider), multi-responsibility domains and national level disturbance (e.g. a multi-party single-fibre backbone) and the global domain (e.g. dealing with an I-Love-You virus type outbreak).

Table 2: The most important vulnerabilities of the Netherlands Internet and their priority.

	Geographical Impact Area			
	Citizen	Enterprise	National	International
1. Breaches of integrity of services & privacy				
2. Viruses and Trojan Horses				
3. '(Distributed) denial-of-service' attacks				
4. No base level security (e.g. BS7799/ISO17799)				
5. Vulnerable facility services (e.g. power)				
6. Capacity failures (Single-point-of-failure, inadequate quality-of-service, shortages)				
7. Computer crime				
8. Inadequate knowledge and training				
9. Infrastructure impact of mobile Internet access				
10. Vulnerability of not-well understood interdependencies				

Priority 1
Priority 2
Priority 3

This resulted in a table (Table 2) showing the most important vulnerabilities of the (Netherlands section) of the Internet. In this table, the impact of selected vulnerabilities on citizens, enterprises, the nation and society as well as vulnerabilities with global impact were assessed. Three priority levels were assigned to understand the highest risks per (geographical) impact area. These results were used to devise a number of measures that were consequently proposed to the Dutch government.

For all the six layer domains and three responsibility domains, the vulnerabilities were investigated with respect to the security aspects confidentiality, privacy, integrity, and availability on the one hand, and with respect to natural causes, deliberate attacks by insiders and deliberate attacks by outsiders on the other hand. This resulted in six tables that were aggregated and condensed using a decision table (shown in Table 1) to select the most important vulnerabilities in the Netherlands section of the Internet.

9. International Critical Infrastructure and Internet security activities

To understand which recommendations could possibly be successful and to learn which pitfalls to avoid, critical infrastructure and other information protection activities by various countries and international organisations were studied. To aid the analysis, the matrix approach that has been proposed by King's College (Rathmell, 2000) was extended. Analysis of the various critical information infrastructure protection activities was eased by assigning each (inter)national activity to one or more cells. Table 3 contains this overview of international critical infrastructure protection studies, initiatives and activities, and Internet security activities. The following activities were recognised:

(1) collaboration of competitors, e.g. banks sharing best-practices or pre-competitive R&D;
(2) CIP policy development;
(3) Infrastructure security, split into the general critical (information) infrastructure activities and the Internet as a specific critical information-infrastructure;
(4) threat and information sharing, e.g. incident response centres; and
(5) public advice activities.

When looking at the various countries, Canada took a fast-track approach. Leveraging upon their Y2K-protection experiences, the Critical Infrastructure Protection Task Force (CIPTF) delivered a report in November 2000. Prior to this, the CIPTF urgently recommended a government-wide co-ordination centre. This resulted in the establishment of the Government of Canada Information Protection Co-ordination Centre (GIPCC) in October 2000. Early February 2001, the Canadian government announced the creation of the government Office for Critical Infrastructure Protection and Emergency Preparedness (May 2001) that assumes the day-to-day CIP-responsibilities.

Table 3: Overview of relevant (inter)national ICT-security and CIP-activities.

	Co-operation with competitors	CIP policy development	Infrastructure Security: all infrastructures	Infrastructure Security: Internet	Threat & Information-exchange	Public advise
International		EU cybercrime G8, OECD UN	EC JRC/DEPPY	G8	FIRST "cybercops" Europol EU EWIS	(FIRST) EU EWIS
Multinational		MIC PX				
Government internal (e.g. defense only)		CH INFORMO SWE IO-D	UK DCSA US CIAO CH INFORMO UK GOSCC		US JTF-CND US FEDCIRC CAN IO cell UK GOSCC	
Government at large	US NIAC	SWE IO-D UK NISCC DK ITS CAN OCIPEP GE KRITIS GE RKRTS ISR NSC NL INFODROME Japan	UK NISCC NO NRC/DSB CAN CIPTF GE KRITIS GE RKRTS ISR NSC CH RAC Japan US NIPC	DK ITS NL TF-PKI GE SI	UK GOSCC UK NISCC CAN GIPCC CH RAC US NIPC	GE SII
Public private co-operation	US NIAC US NSTAC UK IAAC	SWE IO-D Japan NL INFODROME UK NISCC US PCCIP UK IAAC NL KWINT	Japan US NIPC GE KRITIS GE RKRTS UK NISCC US PCCIP GE AKSIS	GE SI NL KWINT	US NIPC AUS CIRCA UK NISCC CERT/CC	US NICE Cyber Citizen NL NPC NL SIF UK DTI GE SBI
Cross-sector	ECP.NL UK IAAC ISTF CH Info	US NSTAC UK IAAC Surance	GE AKSIS	CERT/IRTs	CERT/IRTs US ISACs	GE SBI CERT/IRTs UK DTI
Single line of business	ISTF CH Info UK IAAC	Surance UK IAAC	US NSTAC		US ISACs	
Public/ consumers					US IFCC police NL SIF-complaint	CERT/IRTs ISPs

AUS CIRCA	Computer Incident Research Coordination Austria - virus warning system led by the Chancellor Office
CAN CIPTF	Canadian Critical Infrastructure Protection Task Force
CAN GIPCC	Government of Canada Information Protection Co-ordination Centre
CAN IO cell	Canadian Department of Defence Information Operations cell
CAN OCIPEP	Canadian Office for Critical Infrastructure Protection and Emergency Preparedness
CERT/IRT	Computer Emergency Response Team/ Incident Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CH Informo	Swiss INFORMO 2001
CH InfoSurance.	Swiss InfoSurance initiative (www.infosurance.ch)
CH RAC	Swiss Response and Analysis Center (under development)
DK ITS	Danish IT-sikkerhedsrådet
EU	European Union
EU DEPPY	EU Dependability and Vulnerability in Information Infrastructures Initiative (http://deppy.jrc.it)
EC JRC	European Commission – Joint Research Centre (http://ntsta.jrc.it)
EU EWIS	European Warning and Information System (under development; http://ewis.jrc.it)
FIRST	Forum of Incident Response and Security Teams
GE AKSIS	German Arbeitskreis Schutz kritischer Infrastrukturen (1997-2000)
GE KRITIS	German Arbeitsgruppe Kritischer Infrastrukturen
GE RKRTS	German BSI Referat Kritischer Infrastrukturen
GE SBI	German Secure Business on the Internet
GE SI	German Sicheres Internet
GE SiI	German Sicherheit im Internet
ISR NSC	Israeli National Security Council
ISTF	Internet Security Task Force
MICPX	Multi-lateral critical infrastructure protection (CIP) contingency planning exercise (GE, FR, UK, US)
NL ECP.NL	Netherlands E-commerce Platform Nederland
NL INFODROME	Netherlands Infodrome project (www.infodrome.nl)
NL KWINT	Netherlands 'Kwetsbaarheid van het Internet' (KWINT- project)
NL NPC	Netherlands Nationaal Platform Criminaliteitsbeheersing (www.informatieveiliging.nl)
NL SIF	Safe Internet Foundation - Netherlands chapter (www.veiligophetweb.nl)
NL TF-PKI	Netherlands Task Force on the Public Key Infrastructure

NO DSB	Norwegian Direktoratet for sivilt beredskap (www.dsb.no)
NO NRC	Norwegian National Research Council
OECD	Organisation for Economic Co-operation and Development (www.oecd.org)
SWE IO-D	Swedish Information Operations – Defence group
UK DCSA	United Kingdom Defence Communications Services Agency
UK DTI	UK Department of Trade and Industry together with industry developed BS7799/ISO 17799
UK GOSCC	UK Government Security Co-ordination Centre; Unified Incident Reporting & Alert Scheme (UNIRAS)
UK IAAC	UK Information Assurance Advisory Council (www.iaceac.uk)
UK NISCC	UK National Infrastructure Security Co-ordination Centre (www.niscc.gov.uk)
UN	United Nations
US CIAO	United States Critical Information Assurance Office (www.ciao.gov)
US FEDCIRC	US Federal Computer Incident and Response Capability
US IFCC	US Internet Fraud Complaint Center (www.fbi.gov/programs/ifcc)
US ISAC	US Information Sharing and Analysis Center
US JTF-CND	US Joint Task Force – Computer Network Defence
US NIAC	US National Infrastructure Assurance Council
US NICE	US Network for Internet and Computer Ethics (www.nicekids.net)
US NIPC	US National Infrastructure Protection Center
US NSTAC	US National Security Telecommunications Advisory Committee
US PCCIP	US Presidential Commission on Critical Infrastructure Protection (1996-1997)

In the United States, there are many CIP and information security related activities. A number of them were initiated by the Clinton Administration as result of the '*President's Commission on Critical Infrastructure Protection*' study (PCCIP, 1997). The National Infrastructure Protection Center (NIPC) and the Critical Information Assurance Office (CIAO) are but two examples. When looking at Table 3, many of the cells seem to be covered by US initiatives. However, the US government initiatives are hampered by internal competition between the government agencies, neglecting the goal of the intended activity. Public-private partnership are also hampered by anti-trust acts as well as the freedom-of-information act which restricts the willingness of companies to share company sensitive information with government agencies.

Information Sharing and Analysis Centers or ISACs, e.g. the Financial Services ISAC (FS-ISAC), are cross-sector initiatives to share information on threats and vulnerabilities, as well as best practices. The existing National Security Telecommunications Advisory Commission (NSTAC) can be seen as a special form of ISAC. In the course of 2000 and early 2001, more ISACs were established.

The FBI Internet Fraud Complaint Center (IFCC) provides a "one-stop shop" entrance to the public to halt, for example, identity-theft problems on the Internet. Both the Network for Internet and Computer Ethics (NICE) and the Cyber Citizen initiatives relate to the aims of the Department of Justice to raise the awareness of children and citizens that computer crime is a thing 'not done'.

In Europe, the German government started a critical infrastructure analysis study in 1997. The Arbeitsgruppe Kritischer Infrastrukturen (AG KRITIS) completed its final report, however, mid 2000. The Arbeitskreis Schutz Kritischer Infrastrukturen (AKSIS) is an industry initiative for exchanging threat information as well as best practices on crisis management.
Several incidents on the information highway in early 2000, caused the Minister of Interior to act swiftly. A task group "Sicheres Internet" (SI) was established with the goal to increase the level of information security both by the public, the Internet and Application Service Providers, and also by private companies. In parallel the Minister

of Economic Affairs initiated the Secure Business on the Internet (SBI) public-private partnership.

The Scandinavian countries Norway, Denmark and Sweden all have CIP-studies underway. Norway has various governmental commissions on this topic, for instance the Government Commission on the Vulnerable Society (DSB, 2000), as each ministry is responsible for its own infrastructure. The Ministry of Justice has a co-ordinating, but not a leading role. Several research projects took place or are underway, e.g. the electrical power supply study (1999-2001) and a transportation and logistics study starting this year (Nystuen, 2000). Sweden has brought together a large group of representatives from Government agencies, banks, airports, telecommunication providers, power distributors and the like, to study Information Operation threats and vulnerabilities, and to protect the infrastructures against these threats. As various Swedish government agencies claim responsibility for the nation's critical infrastructure, the originally energetic approach has been understandably delayed.
The Danish IT-security council (IT-sikkerhedsrådet) broke off its study of the critical infrastructure as the task turned out to be too complex. A new project to study the dependency of Denmark on Internet has been initiated.

Switzerland has started a public-private-academic co-ordinated effort on information assurance called InfoSurance. To prepare government officials for crisis management in case of disturbance or disruption of Swiss critical information-infrastructures, yearly exercises take place (e.g. Informo 2001).

In the United Kingdom, both Government and public-private co-operation activities were started up over the last two years. The Government Secure Internet is monitored for incidents by the operational Government Security Co-ordination Centre (GOSCC) which is part of the Defence Information Warfare cell (DIW), under the responsibility of the Defence Communication Services Agency (DCSA).
The National Infrastructure Security Co-ordination Centre (NISCC) was established in June 2000 and has been tasked to protect UK's critical government and industry infrastructures. The NISCC is also responsible for the Unified Incident Reporting and Alert Scheme (UNIRAS), which is the UK government computer emergency response team (CERT).
The Information Assurance Advisory Council (IAAC), established by the Department of War Studies of the King's College in London, can be seen as a think-tank for critical infrastructure protection studies. BT, BAE Systems, the Post Office, the Cabinet Office and CESG are amongst the partners.
The UK Department of Trade and Industry promotes the use of the British Standard 7799 (ISO 17799) by companies to raise the level of information protection. Other governments, such as Germany and The Netherlands, issued the same kind of 'best practice guidelines' on information security but with far less promotional efforts and government backing.

Other countries in the world have undertaken CIP-studies (Australia (Cobb, 1999)) or recently started CIP-studies (e.g. Japan, Israel, and Singapore). In Switzerland, the InfoSurance initiative by industry, organisations and universities aims to raise information security awareness, to stimulate protection and the exchange of public-private information.

In addition to these national initiatives, there are some multi-national initiatives as well. As example, France, Germany, the United Kingdom and the United States co-operate in a multi-lateral CIP contingency planning exercise (MICPX). This "The Day after ... in the Caspian"-exercise was developed by the US RAND Corporation. It aims to train their government policy makers and defence staff and raise their awareness and help to put enough controls in place today to be able to effectively address tomorrow's incidents in multi-national critical infrastructures.
Internationally, the European Union puts an enormous effort into harmonising international cyber-crime laws as part of the eEurope 2002 action plan (eEurope, 2000). The DG Joint Research Centre (JRC) of the European Commission looks at the topic of critical infrastructure research to become an action line in the 6th Framework programme. Also, work is in progress to establish a European Warning and Information System (EWIS) for threats to the information-based society.
The G8 established 7*24 high-tech crime contact points in all the G8-countries. Europol established a similar infrastructure in Europe. Last, but by no means least, in the row of activities, the Forum of Incident Response and Security Teams (FIRST) co-ordinates the information exchange between computer (CERT) and incident response (IRT) teams throughout the world.

Using all the above efforts as a potential yardstick for ways ahead in the Netherlands, the matrix with the currently documented Dutch efforts was finalised. It became evident quite quickly that, apart from the KWINT study in question, there were only a limited number of unrelated efforts. Moreover, it also became clear that the Ministries of Interior and Justice, on the one hand, and the Directorate for Telecommunications and Post of the MoT, on the other hand, were sponsoring two different web sites for public advice, totally unaware of each other's existence!

The following conclusions were drawn:
(1) In countries where no single Government Department is held responsible for the strategic approach to the critical infrastructure protection problem, the lack of vision, sense of urgency and internal power struggles cause delays, duplication, ineffectiveness and a grand waste of efforts.
(2) Critical infrastructure protection studies are complex and require full co-ordinated co-operation of all parties involved at the tactical level. Counter-productivity is exacerbated by both internal competition between government agencies and lack of trust between the parties needing to share information. The failure of the US NIPC in responding quickly to the I-Love-You threat is a case in point (GAO, 2000).
(3) With the exception of Germany and some smaller UK and Netherlands initiatives, not many government efforts were identified to raise the security awareness by providing information to small and medium enterprises (SMEs) and to the public. Lower security thresholds increase the vulnerability of a country for large-scale incidents on the Internet (distributed denial-of-service and devastating virus outbreaks are but two examples).
(4) Internet is not considered as a critical infrastructure on its own by most countries. Only the telecommunications layer continuity is considered critical by a number of countries, overlooking the additional critical layers of the Internet infrastructure as depicted by our models (Section 3).
(5) With the exception of Canada, the Y2K-efforts in most countries have not lead to consolidation of the knowledge and effective approaches to the CIP-problem.

(6) Lacking effective government CIP-actions caused industry to start CIP-studies, Germany is a point in case.
(7) The international initiatives mainly concentrate on the international legal and computer crime aspects.

10. Results and Policy Recommendations

Before policy recommendations could be derived from both the prioritised list with vulnerabilities and the results of the international initiatives analysis, some basic principles had to be taken into account: (1) 100% security is an utopia; (2) in a liberated market, interference by government should be minimal; (3) the Internet is a global network that is not controlled by one central body; (4) each market actor is in principle responsible for its own security measures and service performance; (5) measures by government should be supported by market actors and the public; (6) decreasing the vulnerabilities of the Dutch section of the Internet is a joint public-private responsibility and task.

The first principle that it is impossible to achieve a critical infrastructure that is secured for one hundred percent is based on the open functionality of the Internet, the fast emerging new threats, the international and multiple actors situation, and, last but by not least, the prohibitively high costs associated with removing or reducing all vulnerabilities. This is not new. People in the Netherlands who live below sea-level have learned to live with the risk of floods. Large-scale emergencies may happen, but people expect that their national government takes control swiftly and leads society back to a controlled and a restored situation. Measures to reduce the vulnerabilities of Internet as critical infrastructure should be aimed at situational awareness, control, recovery and reconstitution.

The other principles were derived from discussions with the MoT who commissioned the KWINT study, and on final thesis work by a student from the Faculty for Technology, Policy and Management at the Delft University of Technology (de Kamper, 2000).
Many organisations have learned that outsourced tasks may require more management attention than before the outsourcing. Management should set priorities to the outsourced services and should task someone in the own organisation to supervise the price, performance and quality on a daily basis. If necessary, immediate action should be taken in support of the organisations' mission. In the same way, the division of the responsibilities and tasks of government and market actors were drawn. Firstly, the strategic level at the top (Figure 4) where government determines the long-term vision, sets priorities, and states security and performance requirements. Secondly, the operational level at the bottom, where government has only a limited number of tasks (e.g. police investigations, national security tasks). In a liberated market, the market actors have the main business at this layer. Thirdly, the tactical level, between the previously mentioned levels, is the crucial interaction place between both government and market actors. Based on well functioning information flows, immediate action at the tactical level should be taken at this level when the threat, performance or quality situation in the Internet threatens to shift beyond control. This may be the sole responsibility of either the government or the market actor(s). However, this is a predominantly joint collaborative responsibility and task. Especially, Internet vulnerability issues that can be controlled, either alone or by (inter)national co-operation, should be addressed. It is considered a very achievable

goal, provided the appropriate reaction capability and international contacts are in place.

From the foregoing, it will be obvious that the policy recommendation to the government could not state a complete blueprint for the public-private partnership at the tactical level as this requires support, co-operation, and trust, although the KWINT report presents a first move. The KWINT draft policy recommendations state recommendations for a government vision, seven primary measures and a number of supporting measures. The measures address the main vulnerabilities. When the proposed actions are taken, a process starts that brings together government and the various (groups of) market actors, e.g. telecommunication providers, banks, ISPs, at the tactical layer. It is expected that the joint collaboration will carry on into the collaborative combating of the vulnerabilities of the Internet as a Dutch critical information infrastructure.

Considering all previously mentioned analyses, the prioritised vulnerabilities, support by government departments and market actors, the following policy recommendations were made to the MoT. Firstly, the Cabinet should decide for a single policy to identify and classify the (Dutch) Internet as critical information infrastructure. As a consequence, the government should: (1) understand that 100% security is an utopia; (2) stimulate that the 'electronic' safe high water mark is reached by government at large, by all critical cross-sectors and desirably by all SMEs ("a national higher electronic dwelling mound"); (3) create favourable conditions for market dynamics, and (4) master and control large-scale incidents and emergencies.

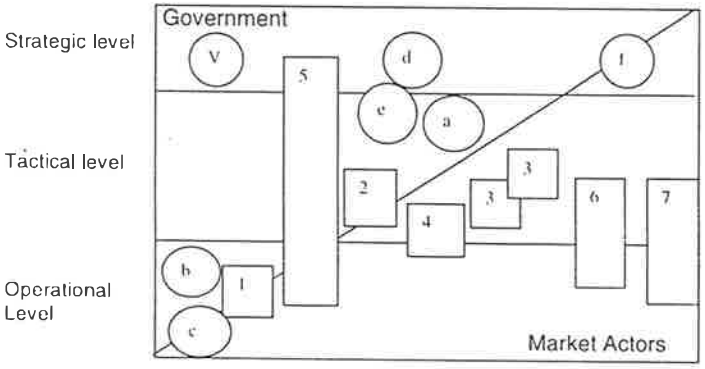

Figure 4: The division of responsibilities and tasks.

Secondly, seven primary measures are recommended to reduce the identified vulnerabilities. Some of these measures bundle already existing, currently isolated Dutch activities into the larger context: (1) Education measures to increase security awareness and public trust and to lower consumer risks. The main target audiences are: children at school ("safe Internet campaign"), consumers and seniors ("do's and dont's") and small and medium enterprises (SME's); (2) Central co-ordination of incidents by means of 7*24 incident response centre that maintains international contacts, classifies threat and intrusion reports, alarms and co-ordinates repression

actions, develops blue-prints and regularly undertakes and co-ordinates training exercises; (3) decentralised co-ordination of incidents by various cross-sector organisations by stimulating the establishment of cross-sector computer emergency / incident response teams or capabilities, e.g. ISP's, universities, telco's, banks, as well as the recently established Dutch government CERT; (4) Security baseline: stimulate the implementation of an information security baseline in all cross-sectors and for SMEs, e.g. BS 7799/ISO 17799; (5) Measure and statistics: develop a set of broadly accepted Internet reliability indicators that are systematically measured and collected (see section 4). This information is required for transparency of service provision and to obtain an objective view on the information assurance of the Dutch Internet; (6) Raise consumer trust: ensure the authenticity, integrity and confidentiality of data to maintain a high end-user confidence level in electronic transactions; (7) Guarantee privacy of end-users according to the new Dutch data privacy act ("Wet Bescherming Persoonsgegevens"), the Netherlands implementation of the European privacy regulations.

Thirdly, the supporting measures support the policy vision and the primary measures: (a) enhance legal security and liability in an e-commerce environment; (b) show as government the sense of urgency and making clear that it takes the problem seriously by setting the example, e.g. by transparently reporting on the number and impact of incidents, quite similar to the actions of the US government (GAO, 2000); (c) stimulate R&D and education at university level in the topic areas information assurance and critical infrastructure protection; (d) up-to-date cyber crime legislation; (e) one single Internet vision and policy plan which is widely published instead of several uncoordinated policy directions by various departments. Both within and outside of the Netherlands various cases of duplication of effort (and waste of time) were identified as well as conflicting policies causing a lack of willingness by market parties to co-operate; (f) stimulate innovation in information assurance.

Figure 4 depicts the relative centres of gravity of the vision (V) and the primary (1-7) and supporting (a-f) measures in the strategic, tactical, operational domain model. Interestingly, the recommendations cover nearly all areas evenly, clearly illustrating that the vulnerabilities of the Internet can only be addressed by a broad joint public-private effort, at all levels of management.

The KWINT recommendations mentioned above have been described in much more detail in the full report in Dutch by (Stratix/TNO, 2000). The Dutch Cabinet discussed and endorsed the KWINT memorandum and the action lines on July 6, 2001.

> Hardly any discussion was required as the KWINT study identified two vulnerabilities that became reality on July 5th, the day before the Cabinet meeting: (1) power distribution problems for data hotels around Amsterdam and (2) the criticality of the Amsterdam Internet Exchange (AMS-IX) in the Dutch Internet. Due to high temperatures and high additional demand by air-conditioning systems, power cables tended to overheat. They were shut down to avoid molten cables. The AMS-IX backbone itself was not affected by the power outage, but most routers of ISPs at the AMS-IX were not connected to back-up power circuits causing the Dutch Internet access by various providers either to be disruspted or to run very slow.

In July 2001, a so-called 24-hour Cabinet meeting organised by Infodrome took place. Security and other experts from various large organisations and sectors (e.g. banks, telecommunication) discussed for 24 hours the critical infrastructure vulnerability issues mentioned in the Bitbreuk study. They stated in a manifest 'The KWICT-institute' (Infodrome, 2001) that the vulnerability of Dutch information-infrastructures at large requires urgent attention by government, politicians and

society. A number of urgent action lines were devised addressing the vulnerabilities of the Dutch critical information-infrastructures ("Het KWICT-Instituut").
These recommendations overlapped those of the KWINT-study. They stress the strategic role of the government. The manifest states the need for a single ministerial responsibility and control over the total set of issues as the security of the State (Ministry of Interior), cyber crime (Ministry of Justice), economical impact (Economical Affairs), international co-ordination (Foreign Affairs), and so forth, with respect of critical infrastructure protection. Also, a public-private collaboration should be started as soon as possible to address the issues. An independent institution was thought of, the KWICT Institute.

On October 2, a meeting took place at the ministerial level to address vulnerability issues. For the moment, one looks at the progress of the KWINT-action lines and the alignment of various departments within government.

11. Conclusions

Our new information-based society is vulnerable. First of all, by the low levels of protection caused by an underestimated attention for security and system management in this area. The attackers increasingly have more powerful tools available to cause harm.
Secondly, as our perception - see the discussion about the vulnerability paradoxes - is often at the optimistic side, we intend to forget all the warnings that we read about on a daily basis.

Increasingly, we make use of fast renewed, inter-networked, interdependent, entangled and converged information and communication technology. Introduction of a new technology cycles causes us to throwaway immediately the alternative infrastructures and to forget "old procedures". In case of a severe disruption, we are surprised and ask ourselves how it happened that we do not have an alternative left.

Our KWINT study assessed the vulnerabilities (of the Dutch section) of the Internet, which is considered to be, or to become soon, a critical information infrastructure for the Netherlands. The study concluded that the Dutch controlled part of the Internet is too sensitive for a manifold of vulnerabilities. As the Dutch Internet has a European hub function, not only the Netherlands is impacted in case of a large-scale incident, but many organisations in a number of countries. The Internet infrastructure as compared to other infrastructures, is much more complex than other infrastructures because many different type of actors are involved on various layers and on a geographical scale that ranges from local to global.
Several models were developed to assess the complex market and government responsibilities, geographical and market areas of interest, tasks, vulnerabilities and threats. These models efficiently helped to pinpoint the vulnerabilities that reside in a large number of locations and responsibility areas in the Internet. The study observed a lack of a transparent set of reliability indicators and a lack of uniformly collected statistics. This made the risk assessment study not an easy task. Moreover, many hundreds of vulnerabilities had to be condensed using a set of principles that reflect market and government responsibilities as basis for the selection and prioritising processes.

Analysis of international activities helped to avoid pitfalls in stating recommendations. Workshops with representatives from market actors, consumer organisations and

government departments helped to determine the level of urgency for taking measures. The workshops increased the support for the draft policy recommendations and the set of primary and supporting measures. The various models helped to convince all parties to understand that no one on his own is able to increase the reliability of the Internet as ones' infrastructure depends upon on services delivered by a number of other actors in the Internet, transmission and power distribution providers, and the intentions and whereabouts of people.

12. Acknowledgements
The author would like to thank J. van Till, R. de Boer, C.H.C. van de Sandt, P. Maclaine Pont (Stratix Consulting Group BV), and M. Klaver and J. Huizenga (TNO) who took part in the KWINT project, as well as Ronald van der Luit and Tim de Kamper (Ministry for Transport, Public Works and Water Management, Directorate of Telecommunications and Post) for the in-depth discussions on the possible role and responsibilities for the government and the available governmental management and control mechanisms.

References

CAIDA (2000). *Various Internet performance measurement tools*. Cooperative Association for Internet Data Analysis [On-line]. Available: http://www.caida.org

Cobb, A. (1999). Critical Infrastructure Attack: An investigation of the Vulnerability of an OECD Country, pages 201-221 in J.M.J. Bosch, H.A.M. Luiijf, A.R. Mollema (eds.), *Netherlands Annual Review of Military Studies 1999 on Information Operations*, Tilburg: Tilburg University Press

Direktoratet for sivilt beredskap (2000). *Government Commission on the Vulnerable Society*. Oslo, Norway: Directorate for Civil Defence and Emergency Planning [On-line]. Available: http://www.dsb.no/nivaa_tre_english/saarbarhetsutvalget.htm

eEurope (2000) *eEurope2002, An Information Society for All: Action Plan*. Brussels: European Union [On-line]. Available: http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm

GAO (2000). *Critical Infrastructure Protection. "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Co-ordination Capabilities, GAO/T-AIMD=00-181*. Washington D.C.: U.S. General Accounting Office [On-line]. Available: http://www.gao.gov

IPPM (2000). IP Performance Metrics (IPPM) Working Group: IETF

De Kamper, T.G. (2000). *De kwetsbaarheid van het Internet, de risico's voor gebruikers en de sturingsmogelijkheden van de overheid*. Delft, The Netherlands: Delft University of Technology, for Technology, Policy and Management (TBM)

Infodrome (2001) *Het KWICT-instituut: Regulerend én stimulerend naar een betrouwbare ICT-infrastructuur*. Amsterdam: Infodrome. [On-line]. Available: http://www.infodrome.nl/download/pdf/deb_kwets.pdf (in Dutch).

InfoOps (1999) *Prerequisites and Implications of Information Operations (Info Ops) within Multinational Operations of Armed Forces*. Den Haag/Bonn: Ministerie van Defensie/Bundesministerium der Verteidigung.

Kyriakopoulos, N., Wilikens, M. (2001). *Dependability and Complexity: Exploring Ideas for Studying Open Systems, report EUR 19797 EN*. Brussels, Belgium: European Commission Joint Research Centre [On-line]. Available: http://deppy.jrc.it

Luiijf, H.A.M. (1999). Information Assurance. In J.M.J. Bosch, H.A.M. Luiijf, A.R. Mollema (eds.), *Netherlands Annual Review of Military Studies 1999 on Information Operations*. (pp. 137-154) Tilburg: Tilburg University Press

Luiijf, H.A.M., Klaver, M.H.A. (2000). *Bitbreuk: de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de Informatiemaatschappij*. Amsterdam, The Netherlands: Infodrome [On-line]. Available: http://www.infodrome.nl both in Dutch and English ("In Bits and Pieces") and on http://www.tno.nl/instit/fel/infoops

May, K. (02/07/2001). *'Cyber Security Agency Unveiled*. Ottawa, Canada: Cybercitizen [On-line]. Available: http://www.infowar.com

MinEZ (2000). *Digitale Delta, e-Europa voorbij*. The Hague, The Netherlands: Netherlands Ministry of Economic Affairs [On-line]. Available: http://www.minez.nl/publicaties/pdfs/05R114.pdf

NEN (2000). *Code voor Informatiebeveiliging:2000*. Delft, The Netherlands: Nederlands Normalisatie Instituut

NLIP (2000). *Het NLIP-keurmerk 2.0*. ["Quality label"]. http://www.nlip.nl

Nystuen, K.O. (2000). Information and Infrastructure Protection - A Norwegian View. In *Proceedings Tulsa Security Workshop*. Tulsa, Oklahoma, USA: NTIA [On-line]. Available: http://www.ntia.doc.gov/osmhome/cip/workshop

OESO (1998). *Internet Infrastructure Indicators, report DIST/ICCP/TISP(98)/Final*. OESO: Working Party on Telecommunications and Information Services Policies

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

Rathmell, A. (2000). International Perspectives on Infrastructure *Protection*. In *Proceedings of the InfowarCon 2000 conference*. Washington DC, USA: MISTI

Stratix/TNO (2001). Luiijf, Klaver, Huizenga, van Till, de Boer, van de Sandt, Maclaine Pont. *Samen werken voor veilig Internet verkeer: Een e-Deltaplan*. The Hague, The Netherlands: Ministerie van Verkeer en Waterstaat/DGTP [On-line]. Available: http://www.minvenw.nl/dgtp/home/data/scriptgifs/985003518-1.pdf

Van Till (1993). Visions of the combination of SDH, ATM and LANs as seen from the cutomer side. In Villy B. Iversen (ed.), *IFIC TC6 / ICCC International Conference on Integrated Broadband Communication Networks and Services, April 2-23 1993, Copenhagen, Denmark* (pp. 35-43).Amsterdam: North-Holland, ISBN: 0444815848 (1994)

VIR (1994). *Voorschrift Informatiebeveiliging Rijksdienst* [Information Security Regulation for the Government]. The Hague, The Netherlands: Ministerie van Binnenlandse Zaken

4. odborná konference s mezinárodní účastí

Současnost a budoucnost krizového managementu

Praha

28. – 29. listopadu 2001

Hotel Olšanka

Táboritská 23, Praha 3