

ISSUE PAPER

**IN BITS AND PIECES**

**Vulnerability of the Netherlands ICT-infrastructure  
and consequences for the information society**

*Translation in English of the Dutch Infodrome essay  
“BITBREUK, de kwetsbaarheid van de ICT-  
infrastructuur en de gevolgen voor de  
informatiemaatschappij”.*

*This essay was written in March 2000 by order of  
Infodrome as a basis for discussion in the Infodrome  
workshop “Vulnerabilities of ICT-networks”. The  
workshop was held in Amsterdam.*

**INFODROME**

**(<http://www.infodrome.nl>)**

**Ir. H.A.M. Luijff**

**Dr. M.H.A. Klaver (Mrs)**

## **ABOUT INFODROME**

Infodrome's aim is to chart the consequences for society of developments in the field of information and communications technology (ICT). In the context of the Infodrome domain study on "Citizenship and Security", various members of the Infodrome steering committee indicated during the tour de table that the topic "Vulnerability of the ICT-infrastructure" needed to be examined in greater depth. At the end of the day, the information society owes its continued existence to a highly complex entity of networks and network-based services. What is the position regarding the availability of that infrastructure and the degree of confidence in the basic information services provided? Is there a possibility that serious disturbances may occur, or is the situation permanently under control? Reason enough for Infodrome to place these problems on the agenda. The Infodrome essay IN BITS AND PIECES offers an initial vulnerability analysis, while at the same time sparking off discussion on whether the public authorities have a role to play in this area (and, if so, what kind of role).

Dr. K.F. van Beek  
Director of Infodrome  
<http://www.infodrome.nl>

**CONTENTS**

ABOUT INFODROME ..... 2

CONTENTS ..... 3

SUMMARY ..... 4

1 INTRODUCTION ..... 5

    1.1 Little attention paid to the vulnerabilities of the fast-moving world of ICT ..... 5

    1.2 Fundamental questions ..... 5

    1.3 The purpose of this issue paper ..... 6

2 VULNERABILITY: DEFINITIONS AND DOUBLE PARADOX ..... 6

    2.1 Definitions ..... 6

    2.2 The double vulnerability paradox ..... 7

3 ICT-INFRASTRUCTURES ..... 8

    3.1 The information chain society ..... 8

    3.2 Network infrastructure layer for information transmission ..... 9

    3.3 Transmission service infrastructures ..... 10

    3.4 Information infrastructure middle-layer ..... 10

    3.5 Added-value services infrastructure ..... 10

4 THE VULNERABILITY OF ICT-INFRASTRUCTURES (CHAIN VULNERABILITIES AND DEPENDENCE) ..... 10

    4.1 Vulnerability of the underlying electrical power infrastructure ..... 10

    4.2 Vulnerability of the network infrastructure layer (information transmission) ..... 12

    4.3 Vulnerability of the transmission service infrastructures ..... 13

    4.4 Vulnerability of the ICT-infrastructure middle-layer ..... 14

    4.5 Vulnerability of the value-added services ..... 15

    4.6 Vulnerability resulting from convergence and intertwining ..... 15

    4.7 International vulnerability studies ..... 16

    4.8 Vulnerability, threats and incidents ..... 17

5 TRENDS AND FACTORS ..... 18

    5.1 E-commerce ..... 18

    5.2 Explosive growth ..... 19

    5.3 Responsibility ..... 19

    5.4 Complexity of services ..... 19

    5.5 Internationalisation and deterritorialisation ..... 19

    5.6 Cyber-criminality ..... 19

6 HYPOTHESES ..... 20

7 CONCLUSION ..... 22

8 BIBLIOGRAPHY ..... 22

9 OTHER SOURCES ..... 24

ABBREVIATIONS ..... 24

THE AUTHORS ..... 24

## SUMMARY

Society is changing rapidly as a result of the frenzied pace of successive developments in the field of information and communications technology (ICT). As well as presenting positive developments, the creation of new technology also poses risks. As far as society is concerned, this frequently seems to manifest itself in a stop-and-start fashion. The learning effects of a cluster of incidents help to tone down the consequences of incidents, but only until a new problem raises its head. ICT is no exception. What is new is the relatively rapid development of new ICT, the convergence and interdependency of infrastructures and the high levels of complexity - all against the background of a dynamic international market.

Foreign studies have identified society's vulnerability in the event of disruption to (critical) infrastructures, thereby giving grounds for grave concern and highlighting the need for new policies. It is also gradually dawning on people in the Netherlands that ICT-infrastructures are vulnerable (Kok Cabinet II, 1999:12 and 27; Ministry of Defence, 1999: 27 and 59). The already far-reaching dependence on ICT in the Netherlands, combined with the fact that this dependence is growing at an ever-increasing rate, means that Dutch society is also becoming vulnerable. After all, the information society owes its continued existence to a highly complex entity of networks and network-based services.

The scale of the threat ranges from prolonged electrical power cuts to deliberate or inadvertent disruption of ICT-infrastructures and/or services affecting business and industry, as well as the government and public services. It is a well-known paradox that greater availability, integrity and confidentiality of public utilities result in a lower level of tolerance on the part of society to disruptions to those public utilities. Consequently, the disruption of (parts of) the critical ICT-infrastructure, whether deliberately or inadvertently, could have potentially drastic repercussions on society and the economy. The question is whether the Netherlands is adequately prepared to cope with such a situation with any degree of control. Can the Dutch authorities or, in the first place, Dutch business and industry after all cope with large-scale disruptions in cyberspace without (inter-)national co-operation?

These questions, in themselves, provide sufficient grounds for Infodrome to examine the vulnerability of the Dutch ICT-infrastructure in the context of the domain study on "Citizenship and Security". This issue paper IN BITS AND PIECES (Dutch original "BITBREUK") provides an initial analysis and postulates a number of relevant hypotheses for further discussion and examination by the authorities in co-operation with appropriate national public and commercial organisations.

## 1 INTRODUCTION

### 1.1 Little attention paid to the vulnerabilities of the fast-moving world of ICT

Society is changing rapidly as a result of the frenzied pace of successive developments in the field of information and communications technology (ICT). New technological breakthroughs, which are the order of the day, are swiftly coming to fruition through the efforts of the commercial sector and are achieving widespread public acceptance. The lessons of history clearly show that, in addition to the many positive benefits it brings to mankind and society, technological change also has its negative side. New threats unfold and aim at the vulnerable aspects of the new technology and the way in which it is implemented.

One of the vulnerabilities highlighted in international studies is the vulnerability of (critical) infrastructures, including the ICT-based infrastructures. 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 Dutch 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.

In its memorandum entitled “The Digital Delta” (1999), the Dutch Cabinet also points out that the high level of integration of ICT in society makes the functioning of that society increasingly dependent on the technical reliability of the (tele-)communications systems. The memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructures and of mastering the growing complexities of IT-applications that are already advanced in nature.

Similarly, the Dutch Defence White Paper 2000 contains the following warning: “However, given the Armed Forces’ high level of dependence on information and communication technology, it cannot be ruled out that in the future attempts will be made to target the Armed Forces in precisely this area. Other countries are also aware of this fact.” (MinDef, 1999:59).

### 1.2 Fundamental questions

Do such vulnerabilities exist? When can they be expected to manifest themselves? Is each chain only as strong as its weakest link? Or do networks, by the nature of their design, have a built-in ability to recuperate and dispense with redundant features? Is The Netherlands adequately prepared to cope with an infrastructure crisis with any degree of control? Can Dutch society as such cope with large-scale disruptions in cyberspace<sup>1</sup> as they occur? Must government take on this extra task? Can it do it on its own, or will co-operation between the public and private sectors be necessary?

These are legitimate questions requiring urgent answers, if The Netherlands is to develop into an information society with confidence, and reliably “play its part in the vanguard” (Jorritsma, 1999) of electronic world trade in line with the ambitions of the Dutch Cabinet (Kok Cabinet II, 1999:10). Given the nature of our complex, converging, interdependent and interlinked ICT-infrastructure, the kind of warnings that society receives these days and that are often brushed aside as mere incidents may have turned into a very real crisis before the day is out.

For this reason, Infodrome asked the authors to produce an issue paper which would serve as a starting-point for discussions on the current situation, and future trends and prospects in this area as well as what role the government should, or should not, play in all this. By identifying vulnerabilities, the intention is to provide a structured view of what risks need to be overcome if the Netherlands is to

<sup>1</sup> Cyberspace is the virtual world of the “communicating citizen of the world” where physical distances, the scene of the action and the time dimension have become (practically) irrelevant (WRR 1998).

aspire to be a reliable information society, and what role the government should play. This issue paper also examines relationships between national and international authorities, business and industry, and society as a whole. After all, cyberspace does not respect boundaries between established national and international social structures and, as a result, it brings its own complexities into the equation.

“A world without frontiers creates both opportunities and risks. Dutch business and industry is well versed at grasping the opportunities. But these developments also engender vulnerability, certainly in the case of an open country such as the Netherlands which, in this respect, is susceptible to external influences.”  
(Ministry of Defence, 1999: 27)

This issue paper was given the title IN BITS AND PIECES (“BITBREUK”). This title reflects such aspects as disrupted communication links, failure of electronic services and possible loss of confidence in the information society on the part of society itself.

### **1.3 The purpose of this issue paper**

Section 2 of this issue paper begins with a brief discussion of such concepts as dependence and vulnerability. Section 3 follows on with an inventory of ICT-infrastructures. The next section examines chain vulnerability and dependence. Section 5 looks at trends and factors affecting the vulnerability of ICT-infrastructures. Section 6 sets out a number of hypotheses designed to trigger further broad discussion and encourage the formulation of in-depth research topics. The conclusions and recommendations are followed by a bibliography and a list of important reference works for further study.

## **2 VULNERABILITY: DEFINITIONS AND DOUBLE PARADOX**

### **2.1 Definitions**

The Dutch Government Information Security Regulation (Voorschrift Informatiebeveiliging Rijksdienst – VIR) defines the concept of information system *vulnerability* as: “the effects of the manifestation of threats on the functioning of an information system or an area of responsibility” (VIR, 1994). In accordance with the regulation, vulnerability analysis is based on a balanced appraisal of the following classic security aspects: availability, integrity and confidentiality.

*Availability*, according to the VIR, is: “the extent to which an information system is functioning at the moment the organisation needs it”. *Integrity* is: “the extent to which an information system is error-free”. *Confidentiality* is defined as: “the extent to which access to, and consultation of, an information system and the information contained therein is restricted to a specified group of authorised persons or processes running on their behalf”.

In the case of the security aspects referred to above, the Code of Practice for Information Security Management (Code of Practice, 1994) - much used by business and industry - contains definitions that differ slightly from those employed by the VIR. In the context of the following sections, these differences are unimportant.

In principle, the definition of availability covers all conceivable circumstances. Nevertheless, in the case of vulnerable critical systems and infrastructures, the *survivability* aspect is also examined. Survivability is a measure of the extent to which availability can be re-established in extreme circumstances (serious disruptions).

In the Dutch report “Stroomloos” (in English: “Disrupted Electrical Power”), the term ‘vulnerability of society’ is taken to mean “the susceptibility of social functioning to the failure of specific functions” (Steetskamp and van Wijk, 1994: 10). Social resilience is related to this: “reduction in the pattern of demand in emergency situations and ability to restore normality” (Steetskamp and van Wijk, 1994: 18).

The subsequent sections of this issue paper use these definitions as their starting-point.

## 2.2 The double vulnerability paradox

According to the “Stroomloos”-report, 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”.<sup>2</sup> 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 (Millennium Co-ordination Commission OOV, 1999).

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 electricity consumption in society, even goes so far as to create a *double* vulnerability paradox.

Recent incidents involving electricity supply and communication infrastructures point to the probability that this double availability paradox also applies specifically to ICT-infrastructures in the Netherlands. If, on top of this, we include the vulnerability of integrity and confidentiality (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 the Achilles heel of Dutch 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, especially if 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, increasingly, lead to a similar situation after a number of hours, given that our society is becoming increasingly dependent on chain processes such as electronic payment, logistical just-in-time systems, etc.

There is yet another dualism associated with the reliability of the ICT-based infrastructures. If the ICT-infrastructures are unreliable, then electronic services will be developed either at a slower pace or not at all. If, on the other hand, confidence is high, there is the possibility that a serious incident will lead to the withholding of trust on the part of consumers, business circles and government. This may create a rift in the development and use of ICT: a part of society will move ahead while another part of society will reject the new technology.

Moreover, when it comes to building up confidence on the part of business and the general public, interactive electronic transactions are at a disadvantage compared to more traditional infrastructures. For example, in the event of disruption to the power supply, consumer confidence is quickly restored following the incident in question. After an incident involving ICT services, however, doubts about the extent to which data confidentiality has been compromised haunt the consumer for a long time to come<sup>3</sup>.

<sup>2</sup> The “Stroomloos” report was written before the introduction of GSM, the rapid growth in interconnected information networks among companies and organisations and the Internet dependence explosion. Consequently, the vulnerability of telecommunications is touched on only summarily.

<sup>3</sup> A third of e-consumers say that, following the recent incidents involving credit card data, they will no longer be so quick to make electronic payments (source: Washington Post 2/3/2000)

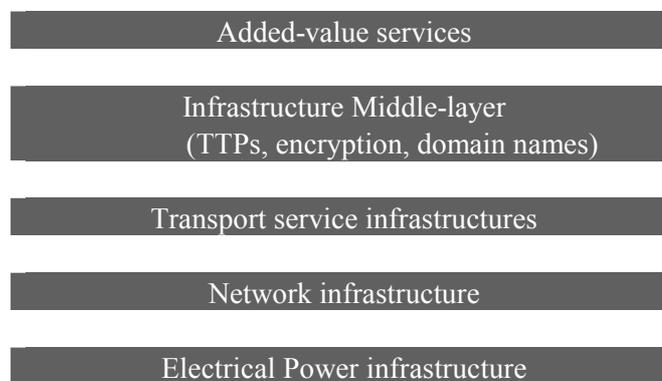
### 3 ICT-INFRASTRUCTURES

#### 3.1 The information chain society

The high degree of ICT integration in society makes the latter increasingly dependent on the underlying infrastructures. Recent problems with the millennium transition have demonstrated modern society's acute dependence on ICT for its very functioning as well as its very limited insight into the underlying infrastructure chains<sup>4</sup>. In the meantime, the ICT-infrastructure has grown into a complex intertwined and interlinked mass of networks and services involving several distinct layers (see Figure 3.1).

Electrical power supply should be seen as the single factor underlying all ICT. Above this is the ICT network-infrastructure consisting of information-transmission facilities such as telecommunications equipment, glass fibres and cables, radio and TV transmitters, satellites, the local loop. In addition, these facilities themselves also make use of ICT hardware and software components for monitoring and control.

Figure 3.1 Model of vertically stacked infrastructures



On top of this network infrastructure, transmission services may also be offered, such as telephony, fax, Internet transmission and routing, and television and radio signal distribution. These transmission services are offered by a wide variety of providers, who may, or may not, make use of the same underlying network infrastructure.

In addition, an infrastructure middle layer involving services can be discerned. This middle layer makes it possible to provide the added-value services, e.g. Trusted Third Party, domain name service, message services (e.g. voice mail, SMS), Internet servers and links between various underlying (national and international) infrastructures.

The middle layer provides the basis for the provision of more advanced chains of services (information services) by the government and by public and commercial organisations, cf., in this connection, location-dependent Internet information services for the motorist or stock market overviews using WAP.

All these added-value services are dependent on the availability and integrity of the underlying infrastructure layers. This points to a vertical dependence but also involves horizontal information flows and information service chains between companies, government, organisations, society as a whole, and individual citizens. ICT makes possible the streamlining of trading chains. Many of today's distribution chains are based - according to planning or assessment - on the development and

<sup>4</sup> The general public thinks that the millennium problem was a storm in a teacup. In a press-report (29/2/2000) the Statistics Netherlands organisation (CBS) stated that, despite the thorough preparations, significant problems were encountered in a number of sectors.

production of goods and services which are subsequently brought to the customer using many links (wholesale trade, retail trade, administrative body). Within the information society, new chains are created which start not with the provider but with the customer.

Leaving aside these positive ICT developments, a number of vital services in today's society have, slowly but surely, becoming heavily dependent on ICT. Examples are telecommunications services, energy distribution (monitor and control), the electronic payment infrastructure, drinking-water supply, emergency services, communication media, the transport sector (e.g. logistics and distribution, rail infrastructure), food supply, and water management. In many cases, these vital infrastructures, in turn, are (or have become) dependent on other horizontal (same layer) and/or vertical infrastructures, thereby forming vital infrastructure chains. The millennium experience has shown that this underlying complex chain-dependence is poorly understood, even by those who are responsible for the continuity of a service. Hence, the confidence that problems would not arise did not always exist<sup>5</sup>. According to Jan Timmer<sup>6</sup> on 1<sup>st</sup> January 2000: "Our awareness of the extent to which we are dependent on information technology has been growing all the time. Indeed, it is essential that it should do so, since this dependence on ICT can only increase in the years to come" (Timmer, 2000).

Chain dependencies may produce unforeseen domino effects, whereby disruption of one infrastructure may spill over to other infrastructures. Coping with such domino effects will only be possible if the extent of the interdependence is clearly understood and if effective, well thought-through emergency preparedness measures have been taken. The fact that, in some cases, this interdependence transcends national boundaries constitutes an additional complicating factor.

### **3.2 Network infrastructure layer for information transmission**

In order to get to grips with these problems, we shall use the model set out in Figure 3.1. The ICT network infrastructure layer consists of information transmission facilities associated with licensed telecommunications operators, radio and TV transmitters, satellites and corporate networks (Ethernet, microwave, glass fibre). This layer handles the "bit transport" for the transmission services operating over these infrastructures. The following are examples of these infrastructures:

- a) The "local loop": the transmission infrastructure between the end-users and the operator's initial point of concentration (e.g. the telephone exchange). This infrastructure frequently includes buried copper cables, CATV cables, glass fibre and, on occasion, a microwave link. In the near future, the Wireless Local Loop (WLL) is to be added to this list as a transmission facility.
- b) Glass fibre bundles and, where appropriate, switching equipment belonging to licence-holders with right of way (examples: Netherlands Rail (NS); Ministry of Defence).
- c) National transport networks and the switching/routing layer of the telecommunications operators (e.g. the KPN Universal Transport Network (UTN)). These broadband infrastructures consist of glass fibres, microwave links and transmission equipment.
- d) Infrastructure associated with base stations for mobile communications.
- e) Broadband international and transcontinental terrestrial transmission infrastructures (e.g. PTAT).
- f) Radio and TV transmitters.
- g) Satellite communications, the anchor station or the up-link and the reception facilities within a specified area ("spot"). Examples: Eutelsat, Inmarsat, low-orbit (LEO) satellites.
- h) Satellite navigation infrastructure.

All these infrastructures have differing characteristics in terms of their vulnerability and impact on the ICT-infrastructure services using this layer.

<sup>5</sup> As a precaution, one electrical power generation and distribution company had obtained a large number of decades-old crank handle telephones from the Museum of the Royal Netherlands Army Signalling Corps.

<sup>6</sup> Translation note: Jan Timmer was the Chairman of the Dutch Millennium Platform.

### 3.3 Transmission service infrastructures

Above the network infrastructure layer, various transmission services (see Figure 3.1) are offered:

- a) Data services such as fax, Internet and other data traffic can be accessed by end-users via modems: over the analogue telephone network (POTS); over ISDN or ADSL (“KPN Snelnet/Mxstream”); X.25 via ISDN; over leased lines (2 Mbps to 622 Mbps); over CATV modems; and over “black fibre” (leased glass fibres).
- b) Data links (9600 bps) and Short Message Service (SMS) are offered as a service by the mobile telephone operators. With the introduction of GPRS (late 2000), followed by UMTS (in 2002), the mobile bit bandwidth is poised to increase dramatically in the near future. The expectations are that mobile use of the Internet via GPRS in 2004 will require as much capacity as use of the Internet via the fixed communications infrastructure requires at the moment.
- c) Radio and TV transmitter frequencies which are also used by information services (e.g. teletext applications such as stock market prices, Wegener services, etc.).
- d) Tetra/C2000 and radio-paging which use a separate transmitter infrastructure.
- e) Internet backbone interconnectivity of ISPs using the network infrastructures §3.2.a), b), c) en e).

### 3.4 Information infrastructure middle-layer

The information infrastructure middle-layer (see Figure 3.1) makes use of the transmission services. This middle layer facilitates the provision of added-value services. Below is a, non- exhaustive, list of potentially important services to government, organisations, businesses and industry:

- a) Domain name services, e.g. the *.nl* domain.
- b) Trusted Third Party (TTP) services for organisations wishing to engage in e-commerce.
- c) Trusted Third Party (TTP) service for government (Ministry of Foreign Affairs 1999) for secure e-mail between government departments.
- d) Transparent gateway services between various national and international infrastructures.
- e) Message store-and-forwarding servers (e.g. e-mail boxes, voice-mail boxes, SMS, EDI).
- f) Secure data communication in terms of confidentiality and integrity, so as to permit secure financial transactions (e.g. SET-protocols).
- g) Virtual networks (VPN) belonging to organisations.
- h) The infrastructure for electronic money transfers using e.g. bank card readers and ATMs.
- i) The infrastructure for alerting services (e.g. burglar or fire alarm).
- j) The Global Positioning System (GPS) offers accurate position determination and an accurate time signal. These functions are used in in-car navigation systems and position-dependent mobile information services.

### 3.5 Added-value services infrastructure

The availability of the information infrastructure middle-layer offers the government and public and commercial organisations opportunities to provide added-value services (Figure 3.1), examples being, trading over the Internet (e-commerce), automated tax collection, processing of transport licences, provision of position-dependent Internet information services (GPS and mobile telephony-dependent) for the motorist; 24-hour government information points.

These added-value services are heavily dependent on the availability, integrity and confidentiality of the underlying infrastructures. Accordingly, due to the stacking of underlying infrastructures and services, vertical (frequently unclear) degrees of dependence and vulnerability can be identified.

## 4 THE VULNERABILITY OF ICT-INFRASTRUCTURES (CHAIN VULNERABILITIES AND DEPENDENCE)

### 4.1 Vulnerability of the underlying electrical power infrastructure

The underlying element as far as the ICT-based infrastructures are concerned is electrical power supply. The availability and vulnerability of electrical power generation and distribution in the

Netherlands is discussed in the “Stroomloos”-report (Steetskamp and van Wijk 1994). The report by the Millennium Co-ordination Commission OOV (1999) also examines the possible consequences of electrical power cuts for all sectors, including the consequences for (tele)communications.

Within the electrical power generation and distribution sector the infrastructure is divided into two parts: the medium-voltage and low-voltage network (village communities, districts), on the one hand, and the production systems, switching systems and high-voltage network, on the other. The relative occurrence of interruptions in the medium- and low-voltage network is much more frequent because of damage to cables during digging and as a result of technical malfunctions. In general, this affects one or more districts/villages for between several hours and several days (e.g. Bleiswijk 1995). Failure of the high-voltage infrastructure is caused by severed cables, technical disturbances, overloading and operational errors. The blackout in the province of Utrecht and surrounding areas (23/6/1997) as a result of a combination of operational errors and technical malfunctions produced a ripple-effect with far-reaching consequences.

Such a blackout over a larger area would mean that ICT-infrastructures either cease to function or are exposed to serious congestion. The latter is caused by the concentration of bit-streams on the few operative links that are equipped with emergency power facilities.

As far as we are concerned, the position regarding the safeguarding of electronic monitoring and control systems in the switching systems for electrical power in the Netherlands is unclear. The ever-growing trend in the United States is towards the use of “commercial off-the-shelf” equipment and the carrying-out of remote maintenance via links with and over public communications networks. This interlinking and the existence of a “backdoor”, often poorly secured and penetrable from the outside, creates new vulnerabilities.

<p>In June 1997 the Pentagon conducted the “Cyber-wargame Eligible Receiver”. Part of the exercise involved simulated assaults on the civil infrastructure. Closer analysis revealed that monitoring and control systems for the distribution of electrical power in the US were accessible from the Internet. The conclusions drawn from the exercise indicated that there was a high risk that the simulated assaults would cause serious disruption, at least temporarily, to the civil infrastructures. (Mr Hamre, US Under Secretary for Defense, 1998)</p>
--

In the Netherlands, with the exception of the National Emergency Network and the bulk of the fixed telephony infrastructure, the public ICT-infrastructures are not, as a rule, equipped with emergency power supply facilities. Consequently, almost all mobile telephony base stations would immediately be put out of action in the event of a failure in the public electricity power supply, with radio-paging going down after 90 minutes (Millennium Co-ordination Commission OOV, 1999; Tweede Kamer, 1999).

The rapidly increasing concentration of telecommunications companies around Amsterdam has resulted in an electrical power supply shortage. Expansion of the electricity distribution capacity cannot cope with this growth fast enough. Delays of between one and two years are common in the installation of new connections and extensions. The consumption requirements of the telecom giants are of the order of 20-30 000 kilowatts. In order to meet this demand, the electricity production network will need to supply additional capacity equivalent to the existing energy consumption of the City of Amsterdam (Beuningen, 2000).

The local Nuon/ENW power distribution company states that, in the meantime, the electricity infrastructure around Amsterdam has become critical. Market trends have led to runaway shortages in the main electrical power distribution network that have taken both the government and the energy distributors by surprise. Finding solutions to these problems necessitates recourse to a number of long drawn out licensing procedures as well as changes to operational plans.

As a consequence of the high level of use of circuits following on from the capacity shortfall, the failure of critical circuits could trigger a cascading of overload situations. For this reason, it is not inconceivable that one or more telecom operators may experience prolonged outage of their services.

#### **4.2 Vulnerability of the network infrastructure layer (information transmission)**

The network infrastructure layer handles the “bit transport” for the transmission services. In this instance, vulnerability is linked specifically to availability. Physical disturbances attributable to the intentional or unintentional disabling of cables are the most acute manifestations of this vulnerability.<sup>7</sup>

19/1/2000: In a press report the Cable and Conduit Information Centre (Klic) states that each year damage to cables and conduits amounting to 100 million guilders occurs as a result of digging. According to KPN Telecom, something goes wrong somewhere in the Netherlands every minute of the day.

While the risk of deliberate manipulation or sabotage of network switching equipment can be assessed only by the Dutch intelligence and secret services, this risk can be significantly reduced through the implementation of preventive (often physical) safety measures.

Since a single physical infrastructure can carry multiple types of communication services (radio and TV signals, telephony, mobile telephony, fax and data traffic), such disturbances will clearly lead to major disruptions in our social and economic life.

On 15/6/1999 a sheetpile severed simultaneously 4 glass fibres belonging to KPN Telecom at the harbour of Groningen. The result was that, between 8 a.m. and 5 p.m., the province of Groningen and large parts of the provinces Friesland and Drenthe were without any mobile and fixed telephony, 1-1-2, alerting services, fax and data traffic, electronic money services and the Internet. The mobile telephones of KPN's competitors also failed because they made use of part of the same physical glass fibre infrastructure. Information services to other parts of the Netherlands likewise failed, an example being the RDW (government Vehicle Licence Plate-database) services used by the police, post offices and motor vehicle, scrap and insurance sectors. What is striking in this connection is the fact that the emergency microwave transmitter links between the RDW and the KPN Telecom data services network via Stadskanaal and via Arnhem were not activated. There were no complaints by telephone from their 'customers'....

The jamming of GPS-signals (up to a distance of 200 km; source: EC Monitor, 8/1999); interfering with GSM-communications (locally and within a radius of about 10 km) using a jamming transmitter and the overloading of satellite circuits illustrate some of the options open to activists but are less likely to occur and are relatively easy to pinpoint.

Both in 1999 and on 10/1/2000, defective glass fibres in the vicinity of Bergen op Zoom cut off communications between parts of the province Zeeland and the rest of the Netherlands for a number of hours.

CATV does not provide an alternative to the electronic highway as long as the CATV-operators are continuously obliged to close down their facilities for hours on end for “maintenance” or moving of cables. Apparently, no alternative routing is available.

On 29/9/1999 in Ohio four glass fibres of 10 Gigabits per second were all damaged. Internet traffic between the east and west coasts of America was routed via Copenhagen and London. This resulted in long delays.

Conclusion: it is simple to close down a significant section of the economic and social traffic in a large region of the Netherlands; in parts of the Netherlands no alternative routings exist.

The software in the switching and routing layer may in unforeseen circumstances, provoke unexpected disturbances in the backbones/broadband networks of the operators. Given the time-to-market pressures, there is always the risk that the most modern equipment and software may be brought into production before the stability of the equipment has been adequately tried and tested.

<sup>7</sup> The KPN Telecom transmission network, Lambda, officially commissioned in January 2000, is “double implemented throughout (...) a breach or disturbance in the network at any specific point” is completely transparent. This network links the 18 biggest towns and cities in the Netherlands (source: KPN press report 18/1/2000).

In the report that appeared in March 2000 entitled “Frame Relay and ATM: Are they really secure?”, the Yankee Group states that the wide-area connections are poorly safeguarded both physically and in software terms. Given the lack of adequate protection, tapping into the connections and manipulation of the network is easy.

In 1995 the hackers’ group, the “Phonemasters”, controlled the telephone networks of AT&T, Sprint and MCI; they diverted an FBI field office phone line to a sex line, manipulated radio-paging calls and were privy to the list of telephone numbers being tapped by the FBI, including their own telephone number. (CNN, 14/12/1999)

In 1998 many switching nodes in the AT&T frame relay infrastructure failed because of an error in the software which was supposed to be dealing with unstable situations. In 1999 MCI/Worldcom was beset with major problems in its frame relay network because of shortcomings in the configuration and testing of software in the switching nodes. BT’s intelligent network was early 2000 out of action for a day, with the result that BT services for ISPs and call centres were not available.

Rotterdam’s telephone traffic was silenced in 1999 because of a fault in an ISDN-exchange (including 90% of the “computer traffic” for more than 7 hours) (source: Newsletter No 10 Information Protection Platform)

Moreover, the Netherlands is a major termination and switching node in Europe for submarine transmission fibres and cables. One consortium after another is bringing ashore glass fibres with capacities ranging from many gigabytes to many terabytes per second. The failure of a glass fibre of this kind may necessitate the rerouting of the information streams. In view of the high trans-Atlantic bandwidth requirements, the question arises whether the failure of one or more of these infrastructures can be adequately absorbed without resulting in unexpected congestion, or even instability, in other networks (triggering a ripple-effect).

Radio and TV signals are distributed from points of reception (on the Dutch border) to central antenna distributors in the Netherlands. In addition, traffic between studios and transmitter installations is being routed increasingly via glass fibre links. The Burum satellite ground station is linked through the KPN Universal Transport Network to the rest of the telecommunication transmission infrastructure and transmission capacity is also leased to several major customers.

Mobile (GSM) communications are vulnerable to loss of integrity, and confidentiality cannot be guaranteed. Once GPRS is brought into use on a larger scale, it is possible that the interception of information and the use of data intercepted in this way may become a lucrative pursuit. Confidence in GPRS (later UMTS) as a carrier for mobile e-commerce may suffer as a result (BSI, 1999).

The switching layer is monitored and controlled from a central network management centre using the same technology. It is unclear how secure this network management infrastructure is. Modems are frequently used for remote maintenance access. Who actually uses them, and whether that individual is officially authorised to do so, is often unclear.

### **4.3 Vulnerability of the transmission service infrastructures**

There are many reasons why the transmission service infrastructure is vulnerable. We do not propose at this juncture to examine the vulnerabilities of the actual systems that are required to deliver these services, although this aspect is indeed a source of worry (GAO, 1999b; ANAO, 1999). The most acute area of vulnerability involves wilful acts that render these services inoperative. Examples of this are physical or electromagnetic attacks (HPM); spoofing and denial-of-use (denial-of-service attack) from outside. In recent times, this latter-mentioned type of attacks attracted a lot of media attention.<sup>8</sup> In addition, there is the risk that, as a result of the fast-moving growth of the infrastructure, inadequately staffed and trained network operators and technical failures. In this process, redundancy

<sup>8</sup> In February 2000, web sites belonging to prominent Internet companies, such as Yahoo, eBay, Amazon.com and CNN.com, went down for several hours as a result of so-called DDoS (distributed denial of service) assaults. (source: NRC February 2000)

will be overlooked and single-point-of-failures will be built in. Only through careful analysis can this be brought to light at an early stage.

#### 4.4 Vulnerability of the ICT-infrastructure middle-layer

The ICT-infrastructure middle-layer handles such basic services as e-commerce (financial transaction infrastructure), electronic notarisation (e.g. TTP), reliable messaging (e.g. digital signature), naming and addressing (e.g. domain names in the .nl domain). The trustworthiness of these services is crucially important in ensuring the use of added-value services and in inspiring confidence among the public and the government in the far-reaching integration of ICT in our society. When we speak of the vulnerability of these ICT-services we mean the vulnerability of the system offering the service and the vulnerability of the infrastructure through which the service is provided.

Safeguarding the integrity and confidentiality of the servers on which these services are offered is primarily the responsibility of the service providers themselves. The recent disclosure of all the data relating to 300 000 credit cards following an intrusion by hackers<sup>9</sup> and the need to issue new access codes for 170 000 Internet users<sup>10</sup> are examples of such vulnerabilities. These problems are comparable to the problems encountered when a bank vault is broken into and can be largely prevented if adequate data security measures are taken. Such incidents may deter the consumer from using e-commerce. Availability can be guaranteed by means of redundancy.

The estimated cost of replacing a compromised credit card and of making good the losses incurred through fraudulent deductions is \$125 per card (ISR May/June 1999: 24).

However, the reliability of the addressing structure constitutes vulnerability of a different kind. If, within an "Internet community" all the street names and house numbers are removed or if the direction-indicators point in the wrong direction, then the government and companies and the services they provide cannot be reached. In the light of actual incidents, the vulnerability of the domain name structure on the Internet, which provides such a pathfinder service, appears to be greater than had previously been thought. In addition, the availability of the critical domain name service is not always guaranteed. Technically, single-point-of-failures seem to exist, and there is a lack of redundancy; domain name servers may become overloaded, and there is a risk of administrative errors. The creation of a "false facade", whereby services are redirected to another party, and the pilfering of addresses and failure of parts of the naming structure are frequent occurrences. The important domain name services for the Netherlands, and their back-up servers, can be made inaccessible by means of a carefully targeted attack, resulting in overloading and blocking for a period of time (of the order of hours). All these vulnerabilities result in the failure, either total or partial, of all the added-value services referred to above.

On 25/12/1998, the Netherlands was largely inaccessible on the Internet all day because of a defective transformer in the low-voltage network.<sup>11</sup>

As a result of the incorrect installation of a domain name server database, about a million sites were inaccessible in July 1997. (Source: Wayner 1997)

From 18 to 22/1/1999 a fault in the .nl domain name registry database caused routing errors, thereby rendering inaccessible certain systems in the .nl domain.

Conclusion: minor disturbances may have the effect of seriously compromising the ambitions of the Netherlands as far as the electronic highway is concerned.

Basic services for the national or government infrastructure can be effectively blocked over a period of time as a result of externally generated overloading. Known dangers include e-mail bombs and distributed denial-of-service assaults (examples: Yahoo, FBI, Microsoft Benelux). A striking feature of the report on Trusted Third Party (TTP) services for the Government (Dutch Ministry of Foreign

<sup>9</sup> CD Universe in the United States, 25/12/1999

<sup>10</sup> Virgin Net in the United Kingdom, end of January 2000

<sup>11</sup> The original BITBREUK essay incorrectly stated here that the nl-domain name services went down. However, the outage was caused by a number of crucial routers at the Amsterdam Internet Exchange (AMS-IX) that were not connected to back-up power resources.

Affairs, 1999) is the fact that the section on availability concentrates solely on technical failure of the server and the risk that some third party may go bankrupt in its capacity as the administration organisation, or, alternatively, may come under foreign control. The vulnerability of the electronic availability of TTP-services, both within the Department itself as well as across other departments, is not (yet) on the agenda.

Also vulnerable are basic services supplied by Internet service providers (ISPs). Where only one service provider is affected, this can be regarded as a business risk. If, however, services of this kind supplied by ISPs across the board are rendered inaccessible for prolonged periods, confidence in the management of the information and communication technology may be shaken as a result.

On 1/3/2000, 1700 Dutch post offices opened late because, owing to a fault, it had not been possible to download essential databases in time which were needed to enable counter transactions to be conducted (authors' note: in this instance the fault in question was a computer failure, but the incident demonstrates the potential vulnerability. A simple disturbance to the communications infrastructure at the right place can keep post offices closed.)

Powerful e-mail bomb knocks out e-mail service for 40 000 Dutch Wanadoo users for over 5 days (webwereld.nl news report 25/1/2000).

For the sake of completeness, attention needs to be drawn to the risk that the announcement of any extended disruption to the security of electronic transactions may have major repercussions for the confidence in the e-commerce financial infrastructure.

#### **4.5 Vulnerability of the value-added services**

These services require reliable, customised, underlying basic services and infrastructures. The problem here lies in the fact that the underlying chains of ICT-services are difficult to fathom. For this reason, it is difficult during design of a new ICT-based service to properly assess and reduce the dependence and vulnerabilities of the service. The failure of a minor link will cause the failure of those services as well, even though, in principle, sufficient alternatives should be available to ensure continuation of service provision (possible with a slightly lower level of performance). The vulnerability of these services is largely determined by the reliability of the underlying layers and the level of expertise and control in rectifying incidents. An emergency that runs out of control may cause severe disruption to the round-the-clock service that is now a rapidly expanding phenomenon, as well as causing loss of confidence on the part of the consumer and the business community in the information society.

As a result of human error, the primary server and two back-up servers of CyberSource Corp. were out of action for 7 hours. CyberCorp verifies and validates credit card transactions for many e-commerce companies, such as Amazon.com and More.com. Four million transactions are checked each month. These transactions are up 376% in a single year.

A number of e-commerce companies were unable to continue trading. Amazon.com conditionally accepted orders involving known customer credit card combinations. Source: PC Week: 23/11/1999

#### **4.6 Vulnerability resulting from convergence and intertwining**

Transmission services are offered to the government, and the market in general, by a wide variety of providers. The latter often use the same underlying infrastructures, without this being clear to the customer. Examples: mobile telephony providers use the fixed telecommunications links belonging to competing companies; 'Voice-Over-IP' is telephony over Internet links for onward transmission via a CATV cable or fixed telephone connections. For the transmitter-receiver link, the Tetra network uses the same glass fibre backbone as all the other communications services, early warning signals, control and test signals for remote control operations, etc. This convergence and the effects of and intertwining are not transparent to the user (government, organisation) at the time of entering into a contract for a service or operator. However, even if the contrary were true and transparency was assured today, the contracted operator could decide, for market considerations, to change the underlying infrastructure arrangements tomorrow - by selling the low-use glass fibres and leasing

capacity elsewhere. On the other hand, a decision may be taken, in the case of capacity shortage, to lease additional capacity from a competitor. As a result, the customer may suddenly find himself in an unwanted, unplanned, dependent and vulnerable position where primary connection provided by one operator and back-up operation provided by another are invariably routed over one and the same bundle of glass-fibre cables. In keeping with Murphy's law, such a situation will only become glaringly apparent at the most inopportune moment possible. OPTA (the Dutch Independent Posts and Telecommunications Authority) is also aware of this unforeseen dependence and vulnerability (OPTA, 1999).

Emergency services, for which accessibility is crucially important, are being strongly advised not to use the mobile KPN Telecom network. Other services are available for that purpose.  
(De Telegraaf, 2/1/1999)

On 27<sup>th</sup> January 2000 the east coast of America was swathed in a thick blanket of snow. Internet users in Washington DC and a number of other counties were urged over the radio to cease all teleworking activities. As a result of the overloading of telephone exchanges, 9-1-1 emergency calls and communications between emergency services were blocked.  
(emergency net, 01/27/2000)

Another vulnerability results from the increasing use of commercial-off-the-shelf (COTS) equipment, software and services. In the past, equipment and software were specifically developed for applications such as network monitoring and control, the emergency services and defence applications. The inherent security element was attributable in part to the small-scale nature of the operation and in part to the fact that third parties were unfamiliar with the control system and applications software being used.<sup>12</sup>

In 1999 the Melissa worm spread with lightning speed via e-mail. A US Air Force base responsible for supporting the Kosovo-operations, was also affected by this worm, which was brought in by a supplier. The result was the effective shutdown of the entire base for a whole day (GAO, 1999a).

## 4.7 International vulnerability studies

### 4.7.1 The United States

In 1996 President Clinton, alarmed at the effects of a number of large-scale blackouts, set up a committee of inquiry. This President's Commission on Critical Infrastructure Protection (PCCIP), made up of members of the government and representatives from five critical sectors (information and telecommunications sector, energy sector, financial institutions, transport, essential (emergency) services), produced a final report in 1997 (PCCIP, 1997). The commission concluded that the complex subsystems in the infrastructures are highly vulnerable to a variety of problems ranging from natural causes (e.g. storms, black ice, and floods), malfunctions and technical disturbances to human causes (from unintentional operating errors to actual attacks). There appeared to be little awareness of the existence of these threats, either on the part of government or on the part of the business community and key industries.

Prof. Desmedt is critical of this study: the investigation was confined to vulnerabilities that have a direct visible impact (breakdown of functions). He identifies a number of vulnerable sectors with a long lead-time constant (weeks, months) whereby minor unobtrusive changes ultimately have a major impact on the availability and integrity of goods and services in other sectors: the mechanical engineering sector (minor measurement differences during production may ultimately lead to accelerated wear and tear and a shortage of spare parts), food production (e.g. automated overfertilising), production of medicines, manufacturing of chips and automated storage systems (Desmedt, 1999). At the same time, Desmedt warns of serious economic damage and the shaking of consumer confidence.

<sup>12</sup> This is known as 'Security by Obscurity'.

In May 1998, the Clinton Administration translated the recommendations of the PCCIP into a number of lines of action laid down in Presidential Decision Directive 63 (PDD63, 1998). Several new ‘offices’ were set up, including: the Critical Infrastructure Assurance Office (CIAO; [www.ciao.gov](http://www.ciao.gov)); the National Infrastructure Protection Center (NIPC; [www.nipc.gov](http://www.nipc.gov)) - a subdivision of the FBI; the National Information Assurance Partnership (NIAP), and the Computer Network-Defense functionality within the US Defense Space Command (and Computer Network (counter) Attack as per 1/10/2000). An overview of these developments was set out in *Technieus* Edition 38/1, published by the Ministry of Economic Affairs (Koppeschaar, 2000).

On 7<sup>th</sup> January 2000, President Clinton launched a 2 billion dollar Delta Plan for the protection of systems and infrastructures. The aim of this national action plan (Clinton, 2000) is to ensure that, by the end of 2003, American society is impervious to serious disturbances in the information society. There are ten programmes covering a range of areas such as critical infrastructure protection, attack identification, streamlining of legislation, early warning systems, training and promotion of R&D.

#### 4.7.2 Germany

In 1997 the Working Party on Critical Infrastructures (AG KRITIS) was set up in Germany. For some time the Federal Department for the Security of Information Technology (BSI) has been drawing up an inventory to determine what critical infrastructures exist in Germany. An interim report should have been ready by the end of 1998. Owing to a lack of co-operation between the various government departments and the business community, little has yet been achieved by way of results. After the hacking campaigns at the beginning of February 2000, which made systems inaccessible in the United States (Yahoo, CNN, FBI), the Netherlands and also in Germany, the German Minister for Foreign Affairs, Otto Schily, set up a task force (BSI, Federal Crime Office and Federal Ministry of the Interior) in order to tackle the problems more assiduously (BMI, 2000). This task force also covers the business community (banks, service providers), e.g. a workshop should be organised by Easter 2000.

#### 4.7.3 Other countries

Other countries whose governments are working to protect critical infrastructures include Canada (co-operation involving the Privy Office, Ministry of Defence, Royal Canadian Mounted Police, intelligence services, etc.), Australia (Cobb, 1999), Singapore, the United Kingdom (through CESG/DERA; little public information available), Switzerland, Sweden, Norway and Finland.

### 4.8 Vulnerability, threats and incidents

The foregoing analysis demonstrates the *vulnerability* of ICT-infrastructures *to the manifestation of threats*. Despite the many examples cited, few serious disturbances/failures appear to occur on a practical day-to-day basis. This would appear to contradict the findings of the analysis. What we have to examine here, however, is just what the chances are that the threat will indeed manifest itself and give rise to an external ‘perceptible’ incident. The chances of this happening will depend on the type of threat, on various environmental factors and on the organisational, procedural and technical security measures already implemented.

If we look at the causes of disturbances/failures, we can divide them into three groups. The first group covers natural causes, technical disturbances and unintentional human errors. These risks, and the measures to counter them, should be fairly assessed in respect of each infrastructure layer *per se*. For this purpose, the Dutch government uses the dependence and vulnerability analyses in accordance with the VIR regulation (VIR, 1994). Comparable methods are also used by market participants. These methods are based on assumptions of what is provided by other parties in terms of services (e.g. as part of a service level agreement). The risks associated with these causes fall within the normal business risk category, and “good husbandry” should ensure that they are adequately contained and counteracted.

The second group involves chain dependence and vulnerability factors. However, as a result of convergence and intertwining, the reliability of chains of services has, if anything, become more nebulous. Dependence and vulnerability analyses require deep insight into the infrastructure chains as well as co-operation on the part of all (market) participants. Such analyses reflect the findings of the complex analyses that have been carried out in this area in the context of the millennium problems. The validity of an analysis may quickly become outdated as a result of rapid, dynamic developments in the market and a sudden influx of new market participants and technologies. Currently, these problems are being managed poorly and are beyond the capabilities of each individual party involved.

The third group involves *deliberate* human disruption by insiders or by external “hacktivists” and terrorists. According to various investigations (NCC in the UK; KPMG; CSI in the US), there often appears to be little perception of the *insider* risk. Insiders<sup>13</sup> are thought to be responsible for between 40 and 80 percent of all security incidents. Responsibility for assessing the *external threat* (serious disruption, attacks and sabotage) rests mainly with the national intelligence and secret services. It should be noted, however, that new and unforeseen threats can quickly unfold, as demonstrated by the fast-moving events prior to the Kosovo-crisis. What is important is the timely anticipation of global threat patterns and the timely implementation of the correct preventive, investigative, limiting and reactive measures.

The external threats (Denning 2000; Luijff 2000; Stol et al. 1999) emanate from a wide variety of sources and have many underlying causes: recreational hackers acting out of curiosity or in a bid to notch up ‘hack-miles’, activists (electronic sit-ins), criminal activities, or hacktivists attempting to propagate their views. The most dangerous category of players is the category consisting of Cyber-terrorists and hostile states. The avowed aim of this group is to deprive the Netherlands of its freedom to act and take decisions and to undermine the population’s confidence in their own government.

## 5 TRENDS AND FACTORS

### 5.1 E-commerce

E-commerce is making headway in Dutch society<sup>14</sup>: “In the field of e-commerce, the Netherlands is lagging far behind other European countries. For its part, Europe scores low compared with the United States but is working hard to catch up.” (eEurope takes off, 1999). “Last year, according to the research, the world-wide e-commerce market doubled in value to 111 billion dollars (about 230 billion guilders). For the most part, this involves so-called business-to-business companies which do not target private consumers but other businesses.”

Because of the dynamic and explosive changes in ICT use and bandwidth, it is not yet possible to measure the economic costs of disturbances to the ICT-infrastructure, for instance in terms of the number of Euro’s per bandwidth-unit per hour of disruption. In order to be able to do this, more in-depth research will need to be conducted on the effects of the disturbances that have occurred, so that an extrapolation can be made into the future. To this end, the approach outlined in the “Stroomloos”-report (Steetskamp and van Wijk, 1994) can serve as a starting-point.

The memorandum entitled “The Digital Delta” states: “Before e-commerce can be fully developed, it is essential to increase confidence in electronic transactions.” (Kok Cabinet II, 1999:53). “One obstacle (but this applies not only in the Netherlands) is the fact that users still lack confidence in identification, fraud prevention, etc., so that they are still rather hesitant about using electronic

<sup>13</sup> The results of the 1999 CSI-FBI Survey show that 38% of the organisations have reported insider incidents; 78 organisations (15%) have reported sabotage involving data or networks (source: www.gocsi.com).

<sup>14</sup> In 1997, Wehkamp’s turnover via the Internet was 1 million per year. In 1999 the same turnover via the Internet (1 million) was being achieved each week.

transactions, and uncertainty still persists regarding the fiscal regimes in force.” (Kok Cabinet II, 1999:V). A key element in creating an atmosphere of confidence and trust is to ensure that electronic payments can be made securely and reliably.

## **5.2 Explosive growth**

Society is moving undeniably towards a 24-hour economy and 24-hour accessibility. The limits to growth in mobile communications and Internet use (in January 2000: 1 million users per day; 56 minutes per person) are not yet in sight. E-commerce over these mobile and fast media will provide a new impetus.

## **5.3 Responsibility**

Until a few years ago, the government had exclusive responsibility for the installation, maintenance, renewal and operation of the ICT-infrastructures in the Netherlands, both in normal circumstances and in exceptional circumstances<sup>15</sup>. Following the liberalisation of the telecommunications market, the government infrastructures have been handed over to market participants, and competition has been stimulated. As a result, infrastructure development, development of capacity and investment are now all market-driven. Consequently, the requisite redundancy in connections and the reserve capacity needed to avoid congestion in the event of an emergency may also enter into the equation. In certain cases, the requisite daily capacity cannot be supplied without the risk of congestion occurring (OPTA, 1999).

## **5.4 Complexity of services**

With the rapid development of many new applications, the provision of electronic services is becoming more complex from one day to the next. These applications are often ‘real-time’ or ‘near real-time’, which means that reliable functioning of the vertical and horizontal infrastructures is essential. If a market participant is perceived by the e-consumer to be too slow or is deemed to be unreliable, buying behaviour will quickly shift to a competitor. Whether this competitor is based in the Netherlands or elsewhere will hardly matter any more.

## **5.5 Internationalisation and deterritorialisation**

As has also been pointed out in the Dutch report entitled “State without a Country”, the provision of e-services is taking on world-wide dimensions. As in the past, the ‘jurisdictions of governments and the powers they wield’ are based on a form of territorial delimitation that is becoming less and less important as a result of information and communications technology. The revolution involving the Internet and other international computer networks came about because, among other reasons, the ICT services totally disregard national territories and because ‘actor, action and consequences of the action’ are no longer tied to a single location. In other words: “deterritorialisation” (WRR, 1999).

## **5.6 Cyber-criminality**

The negative aspects of technological developments, such as “Cyber-graffiti”, “Cyber-vandalism”, ‘common’ criminal activities featuring the use of ICT as a tool, “Cyber-hackivism” and “Cyber-terrorism” are becoming increasingly significant (Clinton, 2000; Luijff, 1999c and 2000). These trends cast a long shadow and must be weighed in the balance in the Infodrome discussions about the vulnerabilities of Dutch ICT-infrastructures during the planning period envisaged by Infodrome.

<sup>15</sup> In terms of a critical information infrastructure in the event of an emergency, the only infrastructure that the government can call its own involves the limited capacity of the National Emergency Network and the Defence Network (NAFIN). Any additional capacity would require the enactment of emergency decrees.

## 6 HYPOTHESES

**Hypothesis 1.** Market pressures and the widespread use of ICT make the risk of large-scale (multi-modal) disruptions, involving several infrastructures simultaneously, increasingly likely in the future. In terms of the availability and reliability of ICT-infrastructures, none of the parties concerned (government, infrastructure operators, the business community or society) is prepared for large-scale disturbances and disruption. Vital interests are being threatened, and the position regarding the tasks and responsibilities of government and the business community is unclear.

Examples: If KPN Telecom's Universal Transport Network suffers long-term disruption resulting in large-scale failure of ICT-services by many providers, will KPN Telecom be left to face the situation on its own or does the government also have a role to play in crisis response? Then again, situations may arise where confidence in the reliability of a whole range of e-service providers is placed at risk.

**Hypothesis 2.** The market mechanism is only partially effective in protecting ICT-infrastructures. Directly visible availability and provision of services to the consumer and the business community represent one aspect where the perceived market image of providers may vary significantly. Emergency preparation for disasters and the occurrence of serious external disturbances are aspects for which providers are not directly covered by a market mechanism. Similarly, integrity and confidentiality are aspects that are not sufficiently transparent to rank as a differentiating market mechanism. There is also still talk of market participants with a 'substantial interest', meaning that market mechanisms – given that they exist at all - are not yet operative. Lastly, the market participants are chain-dependent and do not have complete control over, or the final say on, matters relating to infrastructures they rely upon (see, for instance, § 4.8).

**Hypothesis 3.** In most Western countries, responsibility for the reliability of crucial utilities such as energy and water distribution rests with the government. In view of the ambitious targets set out in the memorandum entitled "The Digital Delta" (Kok Cabinet II, 1999), it would also appear that the government has a role to play as far as ICT-infrastructures are concerned. However, the Dutch Government is no longer in a position to protect Dutch society from serious disruption to, or attacks on, the critical ICT-infrastructure. In order to ensure adequate protection of national interests, a co-ordinated government approach is needed. At this moment, there is a lack of overall vision, and responsibilities are spread too diffusely over different departments.

**Hypothesis 4.** At present, disruptions to ICT-infrastructures are still only attributable in small measure to deliberate attacks from outside. However, as electronic traffic grows in economic importance, we will have to be prepared for a corresponding increase in (inter)national Cyber-crime. Likewise, Cyber-activism will send out a signal proclaiming the combined benefits for the would-be perpetrator of enjoying a high profile while at the same time running little risk of being caught.

The Netherlands, the EU and the OECD-countries are currently at pains to achieve harmonised legal agreements on 'computer crime' and 'Cyber-terrorism'. Cyber-attackers still have a wide territory over which to conduct their operations. Getting off scot-free is also attributable, in part, to the time factor (split-second) as opposed to the slow (steam-age) detection methods associated with conventional law-enforcement. The task for the government is twofold: (i) to oversee the international streamlining of legislation so as to keep one step ahead of tomorrow's developments, and (ii) to develop a battle-ready technical and legal armoury to enable law enforcement services to go into immediate action.

**Hypothesis 5.** The adoption of a purely national approach to the problems outlined above is doomed to failure from the start. For these reasons, and for reasons of cost-effectiveness and speed, the

sensible thing to do is to make use of the ‘lessons learned’ in countries that have already been through the experience.

**Hypothesis 6.** The systematic gathering and analysis by the authorities of information on disturbances to the ICT-infrastructure and other potential threats is a prerequisite for obtaining insight (‘knowledge is power’).

Facilities should exist for the confidential and rapid distribution, through government channels, of accumulated information on threats and information on countermeasures (e.g. CERT information) to departments, government bodies and special-interest organisations (e.g. NLIP or the Banking Association)<sup>16</sup>.

Deliberate attempts to cause disruption, at whatever level of the infrastructures, are always preceded by a reconnaissance phase. The interval between identification of a threat (or receipt of other warnings or preventive information) and the actual materialisation of the threat should be used to optimum advantage with a view to taking the best possible preventive, fact-finding and damage-limitation measures.

At present, there is still no government body that is fully conversant with: (a) the nature and number of security incidents within the government or involving crucial organisations, (b) the consequences of virus and worm attacks, and (c) the extent of infrastructure availability (Luijff, 1999c). An early warning system is lacking. Example: the information distributed on the potentially dangerous Melissa worm in the Netherlands drew mainly on the independent news-gathering activities of the Associated Netherlands Press (ANP).

**Hypothesis 7.** Foreign studies show that, organisationally and technically, the attention paid to the safeguarding of information within government organisations falls short of what is desirable (ANAO, 1999; GAO, 1999b). It is legitimate to ask whether the Netherlands is an exception in this respect. The authors claim that this is not the case (Luijff, 1999b). Experience shows that the security situation in other sectors is no worse, but neither is it much better (NU.nl, 2000). If we are to realise the ambitions set out in the memorandum entitled “The Digital Delta”, serious efforts must be made to achieve a higher level of security in all sectors than is currently the case. In keeping with initiatives undertaken in the US (Clinton, 2000), the UK and Germany (BMI, 2000) designed to provide more adequate levels of security for government services and critical functions, the Dutch Government, in co-operation with private industry, should take steps to develop a comparable “digital delta plan”.

**Hypothesis 8.** The National Emergency (Telephone) Network is experiencing capacity problems<sup>17</sup> and is not designed for the transmission of data other than fax. Government bodies and emergency services, however, are becoming increasingly dependent on ICT applications as part of the decision-making process and when dealing with accidents. The policy-makers at the provincial level, at the national level, and in regional assistance centres, as well as the general public, are increasingly coming to expect the provision of fast and comprehensive information. In emergency situations, this has the effect of creating so-called “hot-spots” in the public communications infrastructure<sup>18</sup>: ICT and telephone network switches where congestion occurs.

With the help of ICT, the relevant information for the authorities, supporting emergency services, and the general public can be brought outside the crisis area, thereby significantly reducing the risk of congestion of public ICT-infrastructures. To this end, the government will need to exercise ICT-vision, based on the realisation that accidents must be dealt with more effectively and reliably. In

<sup>16</sup> The distributed denial-of-service (DDoS) activities which affected sites such as Yahoo and CNN in February 2000 had been predicted by the American banks. Because of a failure to inform the FBI, no “trap” could be set. Consequently, the chances of apprehending the perpetrator(s) would appear to be fairly remote.

<sup>17</sup> See also ANP press report on the millennium test carried out on 9/9/1999.

<sup>18</sup> The telephone exchange in Nijmegen only just managed to cope with the extra traffic when inhabitants were being evacuated from parts of Limburg during the floods of February 1995.

addition, consideration must be given to the setting-up of a national emergency intranet to safeguard the flow of critical (digital) information between government departments and critical undertakings.

## 7 CONCLUSION

This issue paper concludes that, if the Netherlands wants to take its place in the vanguard of the information societies, in accordance with the ambitions set out in the memorandum entitled “The Digital Delta”, then it is absolutely essential to ensure optimum levels of availability and reliability of the ICT-infrastructures. Solving serious failures and malfunctions involving Dutch ICT-infrastructures should be a fully understood, controlled and managed process. In the authors’ view, the current situation of the vulnerability of the Dutch ICT-infrastructures is a compelling cause for concern. Accordingly, the analysis set out in this issue paper and the hypotheses relating to the vulnerability of the ICT-infrastructures should help to trigger discussions within Infodrome.

## 8 BIBLIOGRAPHY

- ANAO (1999) *Operation of the Classification System for Protecting Sensitive Information*, Canberra: Australian National Audit Office. On-line: <http://www.anao.gov.au>
- BMI (2000) *Pressemitteilung 18-02-2000: Task-force “Sicheres Internet” zusammengetreten*, Berlijn: Bundesministerium des Innern.
- BSI (1999) *Mobiletelephone: Gefährdungen und Sicherheitsmaßnahmen*. Bonn: Bundesamt für Sicherheit in der Informationstechnik.
- Church, W. (1998) ‘1997-1998 Infrastructure Vulnerability Report’ *CIWARS Vol 2#23*, San Francisco: CIWARS.
- Clinton (2000) National Plan For Information Systems Protection, Executive Summary, Washington D.C.: White House. On-line: <http://cryptome.org/cybersec-plan.htm>.
- Cobb, A. (1999) ‘Critical Infrastructure Attack: An investigation of the Vulnerability of an OECD Country’, blz. 201-221 in J.M.J. Bosch, H.A.M. Luijff, A.R. Mollema (eds.) *Netherlands Annual Review of Military Studies 1999 on Information Operations*, Tilburg: Tilburg University Press.
- Code voor Informatiebeveiliging (1994) *Code voor Informatiebeveiliging, een leidraad voor Beleid en Implementatie*, Den Haag: Nederlands Normalisatie-instituut.  
(updated since the time of writing of the original Dutch essay): ISO 17799 (2000) *Code of Practice for Information Security Management*. Switzerland.
- Coördinatiecommissie Millennium OOV (1999) *Referentiekader OOV, verstoring in vitale sectoren en openbare orde en veiligheid*, Utrecht: Millennium Platform.
- Denning, D.E. (1999) *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, Washington D.C.: Georgetown University.
- Desmedt, Y. (1999) ‘A Too Limited List of Infrastructures Identified as Critical’ (unpublished) in *NATO IST panel conference on Information Assurance*, Paris: NATO.
- eEurope takes off (1999) *eEurope takes off*, Kopenhagen: Andersen Consulting
- GAO (1999a) *The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data*, Washington D.C.: U.S. General Accounting Office. On-line: <http://www.gao.gov>.
- Beuningen, M. van (2000) Stroomtekort vertraagt start telecomgiganten, *Financiële Telegraaf*, 9 maart 2000.

- GAO (1999b) *Critical Infrastructure Protection Fundamental Improvements Needed to Assure Security of Federal Operations*, Washington D.C.:U.S. General Accounting Office. On-line: <http://www.gao.gov>
- Jorritsma-Lebbink, A. (1999) *Perspresentatie van de ICT-nota De Digitale Delta*, Den Haag: Min. Economische Zaken. On-line: <http://www.minez.nl/speeches99/210699.htm>
- Kok Cabinet II (1999) *De Digitale Delta: Nederland oNLine*, Den Haag: Ministerie van Economische Zaken; Tweede Kamer 26643 nr. 1.
- Koppeschaar, K. (2000) 'Kritieke Infrastructuur, kwetsbare infrastructuur: De betrouwbaarheid van de kritieke infrastructuur in de Verenigde Staten', *Technieuws* 38/1:18:31, Den Haag: Ministerie van Economische Zaken.
- Luijff, H.A.M. (1999a) *Information Assurance and the Information Society*, in: U.E. Gattiker, P. Pedersen and K. Petersen (eds.) Conference Proceedings EICAR '99, Aalborg: TIM-World ApS. On-line: <http://www.tno.nl/instit/fel/refs/pub99/eicar99.pdf>.
- Luijff, H.A.M. (1999b) 'Information Assurance: a long way to go' blz. 137-153 in J.M.J. Bosch, H.A.M. Luijff, A.R. Mollema (eds.) *Netherlands Annual Review of Military Studies 1999 on Information Operations*, Tilburg: Tilburg University Press.
- Luijff, H.A.M. (1999c) Falende informatiebeveiliging bij overheden onvoldoende aan het licht', *Beveiliging* 12(12):60-63, Amsterdam: Keesing BV.
- Luijff, H.A.M. (2000) 'Information Assurance under Fire' in *Conference proceedings Informaton Assurance and Data Security*, London: SMi.
- MinBZK (1999) *Trusted Third Party diensten voor de Rijksoverheid: vertrouwen in communiceren*, Den Haag: Ministerie van Binnenlandse Zaken.
- Ministerie van Defensie (1999) *Defensienota 2000*, Den Haag: Ministerie van Defensie.
- NU.nl (2000) Internet pagina's verzekeraars zo lek als een mandje', *NU.nl*:27-2-2000
- OPTA (1999) *Bundeling van openbare versies met betrekking tot rapportage door Stratix over schaarste in het telecommunicatienetwerk van KPN Telecom en over het onderzoek naar interconnectieschaarste bij KPN Telecom*, Den Haag; OPTA.
- PDD 63 (1998) *The Clinton Administration's Policy on Critical Infratructure Protection: Presidential Decision Directive 63*, Washington D.C.: White House.
- President's Commission on Critical Infrastructure Protection (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.
- Raad voor Verkeer en Waterstaat (1999) *Nederland let op uw Saeck*, Den Haag: Raad voor Verkeer en Waterstaat. On-line: <http://www.raadvenw.nl/tel-advies.htm>
- Steetskamp, I., Wijk, A. van (1994) *Stroomloos, kwetsbaarheid van de samenleving:gevolgen van verstoringen van de elektriciteitsvoorziening*, Den Haag: Rathenau Instituut
- Stol, W.Ph., Treeck, R.J. van, Ven, A.E.B.M. van der (1999) *Criminaliteit in Cyberspace*, Houten: Elsevier bedrijfsinformatie bv.
- Timmer (2000) 'En nu van m'n pensioen genieten', *Haagsche Courant* 03/01/2000:7, Den Haag: Sijthof Pers.
- Tweede Kamer (1999) *Kamervragen met antwoord, vraagnummer 298991650 Nr. 1460:1999*, Den Haag: Ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Verkeer en Waterstaat.
- VIR (1994) *Voorschrift Informatiebeveiliging Rijksdienst*, Den Haag, Ministerie van Binnenlandse Zaken.
- WRR (1998) *Staat zonder land*, Den Haag: Sdu Uitgevers.

## 9 OTHER SOURCES

Anderson, R., Feldman, Ph.M., Gerwehr, S., et al. (1999) *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*, Santa Monica CA USA: RAND.

On-line: <http://www.rand.org/publications/MR/MR993>.

Luijff, H.A.M. (red.) (2000) *TNO-FEL's URLography Information Assurance*, Den Haag: TNO.

On-line: <http://www.tno.nl/instit/fel/infoops>

Schneider, F.B., *Trust in Cyberspace*, Washington D.C.: National Academy Press.

Ware, W.H. (1998) *The Cyber-Posture of the National Information Infrastructure*, Santa Monica CA USA: RAND. On-line: <http://www.rand.org/publications/MR/MR976/mr976.pdf>.

## ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
CATV	Cable TV
CERT	Computer Emergency Response Team
GPRS	Generic Packer Radio Service (packet mode communication via GSM)
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HPM	High Power Microwave
ICT	Information and Communications Technology
IP	Internet Protocol
ISP	Internet Service Providers
OECD	Organisation for Economic Co-operation and Development
PDD	Presidential Decision Directive
PPCIP	Presidential Committee on Critical Infrastructure Protection (USA)
POTS	Plain Old Telephony System
SET	Secure Electronic Transaction
SMS	Short Message Service
TTP	Trusted Third Party
UMTS	Universal Mobile Telecommunications System
UTN	Universeel Transport Netwerk (Universal Transport Network) (KPN Telecom)
VIR	Voorschrift Informatiebeveiliging Rijksdienst (Dutch Government Information Security Regulation)
VOIP	Voice-over IP
WAP	Wireless Application Protocol
WLL	Wireless Local Loop

## THE AUTHORS

Ir. H.A.M. Luijff ([luijff@fel.tno.nl](mailto:luijff@fel.tno.nl))

Dr. M.H.A. Klaver (Mrs) ([klaver@fel.tno.nl](mailto:klaver@fel.tno.nl))

Both authors are employed as principal consultants with:

TNO Physics and Electronics Laboratory

P.O. Box 96864, 2509 JG, The Hague, The Netherlands

Phone: +31 70 374 00 00 Fax: +31 70 374 06 51