INTERNATIONAL TELECOMMUNICATION UNION

**ITU WORKSHOP ON
CREATING TRUST IN CRITICAL
NETWORK INFRASTRUCTURES**

**Document: CNI/08
20 May 2002**

Seoul, Republic of Korea — 20 - 22 May 2002

CREATING TRUST IN CRITICAL NETWORK INFRASTRUCTURES:

NETHERLANDS CASE STUDY

This case study was prepared by Michel Schut, a postgraduate student of the Faculty of Technology, Policy and Management of the Delft University of Technology, under the supervision of Ivo Essenberg, Project Manager – New Initiatives, International Telecommunication Union: <mailto:ivo.Essenberg@itu.int>. This study is part of a series of country case studies prepared for the ITU New Initiatives Workshop *Creating Trust in Critical Network Infrastructures* to be held in the Republic of Korea, from 20 to 22 May, 2002. The author is thankful to Simone Meijer, Ronald van der Luit, Klaas Bouma and Tim de Kamper of the Netherlands Ministry of Transport, Public Works and Water Management, Jaap Akkerhuis of the Stichting Internet Domeinregistratie Nederland (SIDN) and to the faculty of Technology, Policy and Management of the Delft University of Technology, in particular to Samir Daskapan, Rudi Westerveld and Wander van den Berg. This study has been undertaken under the auspices of ITU, however, the information contained herein does not necessarily represent the views of ITU or its membership, nor those of the Netherlands Administration.

Table of contents

1 Introduction

It is a generally acknowledged fact that our dependence on networks is growing at a rapid rate, especially in the field of computing. More and more of our daily activities use data networks, be it for transfer of information or communication between geographically diverse locations. Hence, our need for trust in critical network infrastructures increases on an almost daily basis. Attacks against our infrastructures show us how much we need these infrastructures to be available, reliable and secure.

The present case study offers an overview of the Netherlands in the area of critical network infrastructures. It was written in preparation for the ITU New Initiatives Workshop 'Creating Trust in Critical Network Infrastructures'. The study focuses mainly on data networks, including financial networks, and mainly from an infrastructure perspective, rather than from an end-user perspective. The study includes both private and public networks and looks at the environment needed to guarantee applications being available and secure. Naturally, points of view differ on which requirements are necessary, depending on the application in question.

The study aims to bring together the views of both the public and the private sector. Achieving trust in critical network infrastructures will require both sides to work together, through a combination of information, regulation and investment. As such, it is hoped that this study will serve as a catalyst for the exchange of information between the relevant parties in the Netherlands.

1.1 Country background

0 25 50 km
0 25 50 mi
North Sea
Den Helder
Delfzijl
Leeuwarden
Groningen
Assen
Zwolle
IJmuiden
Haarlem
AMSTERDAM
The Hague
Utrecht
Arnhem
Europoort
Rotterdam
Dordrecht
Nijmegen
Tilburg
GERMANY
Terneuzen
Eindhoven
BELGIUM
Maastricht

The Netherlands is a Western European country with a population of 15,981,472[1]. It covers 41,526 km^2 and, with a population density of 385 inhabitants per square kilometer, it is one of the most densely populated countries in the world. Its capital is Amsterdam, while The Hague is the seat of Government. Rotterdam is home to the largest port in the world, with a 2000 throughput of 322 million metric tons[2]. Table 1.1 provides an overview of some relevant social and economic indicators for the country.

The Netherlands is an open economy depending heavily on foreign trade and is known for its role as a European transportation hub, in part due to its large road transport sector. In 1999, its trade revenue represented 116 per cent of the

[1] July 2001 estimate, CIA World Factbook

[2] Port of Rotterdam authority

country's gross domestic product[3] and was growing at a rate of over six per cent per annum. In the same year, services formed 74 per cent of the GDP of the country[4].

The Netherlands have always been active on the international scene, and especially in the area of regional or international cooperation. In 1944, the Netherlands formed an economic union with Belgium and Luxemburg, BENELUX. In 1949, it was one of the founding members of NATO.

In 1951, the country was one of the founders of the predecessor to the European Union, the European Coal and Steel Community. After joining the Euro zone in 1999, the Netherlands was one of the first countries to completely phase out its national currency, the Guilder, in January 2002.

1.2 Information society in the Netherlands

The Netherlands is very active in developing its telecommunications infrastructure. In 1999, the country invested almost USD 3.5 billion in telecommunications infrastructure[5], an increase of 67 per cent over the previous year. In the year 2000, there were 10.7 million cellular subscribers and over 3.8 million Internet users[6]. With 2,155,635 Internet hosts in July 2000, the Netherlands ranks sixth in the world with a host density of 1,360 per 10,000 inhabitants[7].

Table 1.1: Basic economic and demographic indicators for the Netherlands

	1995	1996	1997	1998	1999
Population (000s)	15'500	15'600	15'642	15'745	15'839
Gross Domestic Product (GDP) (Million EUR)	290'302	300'323	319'814	340'585	372'600
GDP (million USD)	398'593	392'565	360'478	378'359	396'668
GDP per capita (USD)	25'716	25'164	23'045	24'031	25'043
Annual investment in telecommunication (million USD)	1'710	1'606	1'627	2'068	3'447

Source: ITU World Telecommunication Indicators

Note: Exchange rate used Dutch Guilders to Euro conversion: 2.20371

There are many factors which have made the Netherlands into one of the major network hubs in Europe. The availability of highly skilled labor, a population whose vast majority speak English as a second language and its favorable tax environment are just some of the advantages that the country offers. As a result, in 2000, the Netherlands was home to seven of the 78 Internet Exchange points in Europe, compared to 12 in the United Kingdom, six in France and just one in Germany[8].

[3] 2001 World Development Indicators, The World Bank

[4] Id.

[5] Source: ITU World Telecommunication Indicators

[6] Id.

[7] ITU Internet Reports 2001

[8] ITU Trends in Telecommunication 2000-2001

Of the top ten international Internet routes, five connect to Amsterdam[9]. In 2000, Amsterdam was the second largest international Internet hub and one of the five European cities with five or more Metropolitan Area Networks[10]. In terms of international backbone routes, 13 of the top 50 routes in Europe connect to Amsterdam[11].

In 2002, the Information Society Index, a composite index based on computer, Internet, information and social infrastructure, ranks the Netherlands as sixth in the world[12], up from tenth in 2000. The Netherlands score especially high in the area of information infrastructure which provides a score for the number of phone lines per household and their quality, the cost of local calls, television, radio, fax and cellular phone ownership and access to cable television.

1.3 Telecommunication market

The Netherlands has a highly active telecommunication market. The Dutch government started the path towards liberalization by its partial privatization of the incumbent operator, KPN, in 1994. In 1996, the Fixed Telecommunications Infrastructure Licences Act started the liberalization of fixed telecommunications infrastructure.

1997 saw the introduction of the Competition Act and the OPTA law which established an independent regulatory authority, OPTA, and opened the market to competition. At this date, all telecommunication services[13], except for local calls and telex, were open to competition. At the end of 1999, there were 95 licensed operators for fixed services[14]. In July 2000, there were 60 authorized international carriers, ranking the Netherlands eighth in the world[15]. In 1999, the country was home to 130 Internet service providers[16]. In the fixed line market, the Netherlands offers high quality connections with a very low number of faults per year (27 per 1000 lines in 2000[17]) and competitive rates compared to most countries.

The Dutch government is also highly active in the development of network security in such areas as emergency response networks, security of transactions and security of actual networks. A national emergency network, the "Nationaal Noodnet", has been put in place, consisting of 17 digital phone switch offices, with a capacity of 7,000 to 10,000 connections. The targeted availability of this network is 100 per cent through a combination of technical measures[18].

Aside from these activities at national level, the Dutch government is also closely tracking a number issues at international level, such as Internet management and European network security activities. The country actively participates in such policy forums as the European Conference of Postal and Telecommunications Administrations (CEPT), the European Union and the International Telecommunication Union (ITU).

[9] Telegeography, 2001. Of the top 50 routes, 11 connect Amsterdam.

[10] Telegeography, 2001.

[11] Id. 5 of these routes are in the top 10 routes in Europe.

[12] http://www.worldpaper.com/2002/feb02/isi.jpg

[13] including the provision of cable television

[14] http://www.eu-sis.org/Basic/NLbasic00.htm

[15] Telegeography 2001.

[16] ITU Internet Reports 2001

[17] "Netwerken in cijfers", Ministry of Transport, Public Works and Water Management, The Netherlands

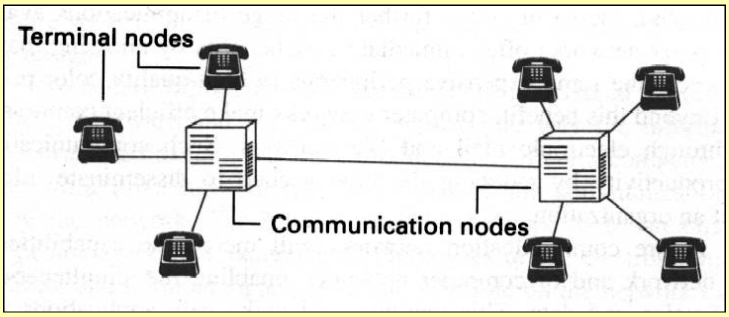
[18] Id.

2 Networks

2.1 Organization of networks

In order to be able to define the problem area and provide an accurate description of networks involved, it is necessary to understand the concept of networks and how they are used. Walrand[19] defines communication networks as:"A communication network is a set of nodes that are interconnected to permit the exchange of information."

Figure 2.1: Network nodes
"A communication network is a set of nodes that are interconnected to permit the exchange of information."



So a network consists of nodes and interconnections. Nodes can be of two types, terminal nodes and communication nodes. Terminal nodes generate or use information on the network.

Communication nodes are used to receive and transfer information. These terminal nodes can be telephones, but also personal computers, televisions, servers and so on. Examples of the communication nodes are hubs, telephone centrals and switches. The physical interconnection can be copper wire, radio waves, optical fiber and cable. Information may be voice, sound, graphics, pictures, video, text or data.

This information can be used between nodes using different kinds of transmission technology, broadcast networks and point-to-point networks.[20] Information that is broadcasted uses a single communication channel that is shared by all the machines on the network. Point-to-point networks use individual connection between pairs of machines. Often the type of information and its purpose define which kind of medium is used. Television signals are broadcasted while telephone signals use point-to-point connections.

But today a lot of systems are connected to each other and converging to more general systems. Almost all information can be converted to packages and sent over the same networks. Most data, video and phone services can be transmitted over the Internet. But the Internet can also use cable, phone or satellite networks.

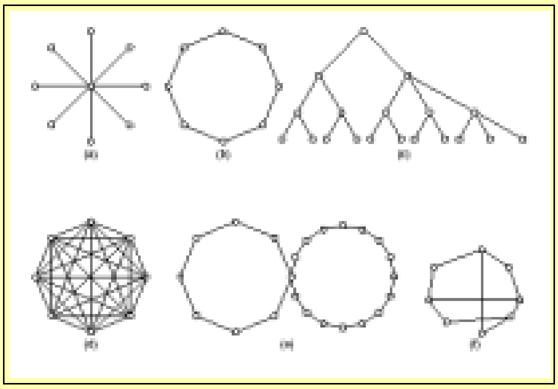
[19] Jean Walrand, Communication Networks: A first course, Homewood, IL: Irwin, 1991

[20] Andrew S. Tanenbaum, Computer Networks (Third editition) Prentice-Hall, 1996

2.2 Internet networks

The Internet is a worldwide network of networks, consisting of an amalgam of many different types of networks, connected together using the Internet protocol (IP). These networks are interconnected by various arrangements. The traffic that goes over the Internet can be part of a provider/customer relationship, in which case it is called transit traffic or can be part of a peering arrangement. Often these interconnections take place at an Internet exchange (IX), a central, neutral, point where various Internet service providers exchange (peering) traffic. Peering agreements are usually based on an agreement to carry an equivalent reciprocal quantity of traffic from the peering network.

Figure 2.2: Shapes of networks



Network types include local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). LANs are mostly used within a 1 km radius. They can be found within an office or on a campus. LANs often use broadcast technology and have simple topologies, usually either ring or bus topologies. MANs use broadcasting technology similar to LANs. Although LANs and MANs are extremely efficient, it's hard to scale them up across a whole country or continent. That is because the wire must do all the work and all packets are broadcasted all over the network. In a WAN hosts are connected to a subnet, which in turn consists of switching computers (routers) and transmission lines (trunks). Routers receive packets from a host. First they buffer the packet and then decides where the packet has to go and forward it across the selected line. WANs subnets can have all kinds of topologies. Often, WANs are again interconnected with each other to a global network whereto every computer is connected.

2.3 Internet hierarchy

A user who is online using Internet will most likely connect to the network of their Internet service provider (ISP) and thus become part of that network. Connection is possible through a standard telephone, but can also be made via a company network with a private line or cable network. Local ISP's can be interconnected with each other. The ISP may also then join to a lager network of other ISPs. This is often called a backbone ISP or transport provider(TP)[21]. Using these ISPs, a user is able to reach others who are connected to the same backbone ISP. Nearly all ISPs and TPs are linked to a national switch. These switches are usually known as Internet exchanges. International consortia have connections with these Internet Exchanges and connect these with other countries as well as with their own network. Some ISPs, like UUNet for example, have their own local networks and backbone facilities. So they can operate regionally, nationally, and even internationally.[22]

2.4 Vulnerability and reliability of networks

First, it is important to get an idea of what is meant by vulnerability. The Ministry of Internal Affairs of the Netherlands uses the following definition for vulnerability of information systems:

"The manifestation of threats to the functionality of an information system or responsibility area".[23]

There are two aspects to this definition. The first is that a system is considered vulnerable if the likelihood of a negative event is high. The second is the strength of the impact of such an event on the system concerned.

For instance, if a packet is lost while it is being transmitted, but it is very easy to send another one, then the vulnerability is not considered high. Even if the rate of packet loss is increased, this is not an issue, unless the system is not able to correct the problem by resending packets.

Similarly, if an event would have a serious impact on a system, but is highly unlikely to occur, the vulnerability of the system is considered to be low.

There are three basic requirements for reliability on computers and networks, namely: availability, integrity and confidentiality. If one of these requirements is in jeopardy, or compromised, a system may be considered to be vulnerable. Availability is compromised when information is lost or not available when a user requests the information. Integrity is compromised when information is incorrectly altered: inconsistent data is unreliable and has to be discarded. Finally, if information falls into the wrong hands, then confidentiality is compromised.[24]

Failures in reliability can have any number of causes, such as those shown in Table 2.1 below.

[21] http://www.howstuffworks.com/Internet-infrastructure.htm

[22] Policy paper "Internet vulnerability", Ministry of Transport, Public Works and Water Management, Netherlands, 2001, http://www.dgtp.nl/english.html

[23] Voorschrift Informatie beveiliging Rijksdienst (VIR), Ministry of Internal Affairs, Netherlands, 1994

[24] Mieke Borgers-Roozen ea, Werkplekbeveiliging, Informatiebeveiliging jaarboek 2000/2001

Table 2.1: Causes of failure in networks

Natural disasters and break-down of electricity, telephone network	Fire, storm, float etc. can result in damage to buildings, computers and infrastructure	Availability, integrity
Technical failure	Malfunction of computers leads to data loss and data corruption	Availability, integrity
Virus	A Virus causes data loss, data mutation and unwanted e-mail traffic	Availability, integrity, confidentiality
Loss-theft	When laptops or computers are stolen or lost data can fall in wrong hands.	Availability, confidentiality
Unsupervised computers	Someone unauthorized can access information	Integrity, confidentiality
Ignorance and carelessness	Errors are made by people who aren't well trained or careless	Availability, integrity, confidentiality
Purpose	People with access to computer can access data in order to commit fraud or sabotage.	Availability, integrity, confidentiality

Viruses

Viruses are programs intended to inflict damage on computer and network systems. A computer virus will infiltrate the system and execute all kinds of actions. The most common types of viruses are worms, "Trojan horses", common executables, boot viruses and macro viruses.

Viruses may be developed for the sole purpose of causing damage to systems, but may also be used for a hacker to gain access. Hoaxes are new form of pseudo-virus that work by means of an alarmist e-mail which causes users to delete critical system files, thus rendering their systems unusable.

2.5 Denial of service attacks

In addition to viruses, computer systems are vulnerable to so-called "denial of service" (DoS) attacks. In a DoS attack, the criminal attempts to bring down a service by overflowing it with bogus traffic. For example, a domain name server can be bogged down with faulty requests for information, causing such excess loads on the server that it will not be able to respond to legitimate queries.

Viruses can also be written to install software on remote computers which will enable the hacker to control the victim's computer. An example of this is the "Sub7" virus which opens a backdoor into a victim's computer, enabling the sender of the virus to control the computer remotely. This tactic is widely used to gain control of a large number of computers which can then be used to attack a specific target in what is called a "distributed denial of service" (DDoS) attack. In a distributed attack, the attacker uses many different computers to attack the target, instead of generating all attacks from a single machine. This has the "advantage" of being more difficult to halt, since many attackers coming from many different locations need to be blocked, instead of being able to focus on a single machine.

3 Networks in the Netherlands

The purpose of this chapter is to give a global description of network infrastructures in the Netherlands, not only in respect of their structure and architecture, but also in respect of the various organizations behind the technology and the roles these play. Furthermore, some of the weaknesses of the Internet in the Netherlands are described, and some possible solutions proposed. Finally, there is a description of current measures for the dissemination of information regarding network issues.

3.1 Network infrastructure

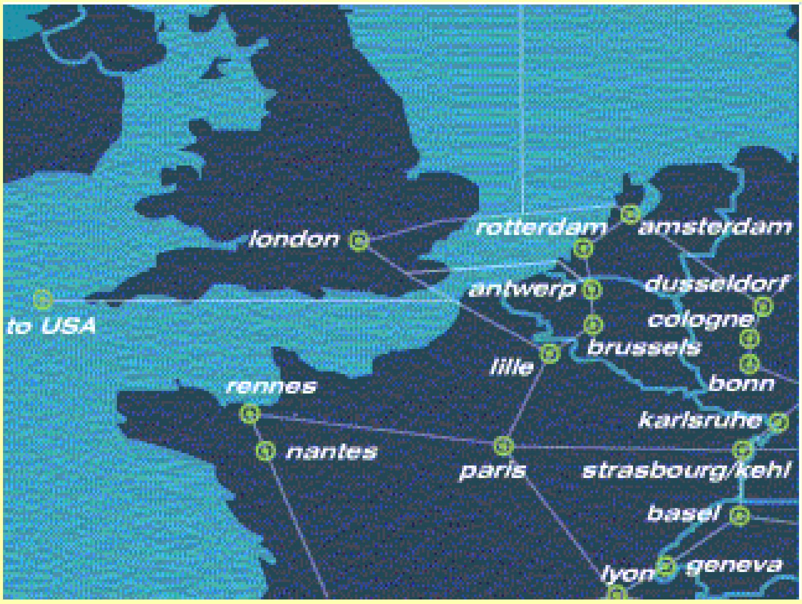
The telecommunications infrastructure in the Netherlands consists of a variety of networks. At the present time, most of these can be used to transmit data.

The cable network in the Netherlands is primarily used for broadcasting television and radio signals. A cable company broadcasts an average of 30 television stations and 34 radio stations. Due to the high population and limited size of the country, it has been possible to achieve a high level of cable penetration. In 2000, the Netherlands comprised approximately 6.6 million households. Of these, approximately 6.2 million were subscribers to cable TV. [25] This represents a cable penetration of over 94 per cent. As of January 1999, 43 per cent of the main cable networks consisted of optic fiber cables, thus enabling cable companies to prepare their networks for two-way broadband traffic. In recent years, most cable companies have started offering high-speed Internet access through the use of cable modems and, more recently, have additionally started offering telephone service.

Five operators offer mobile telephone services. KPN and Vodafone (formally known as Libertel) both have 900Mhz networks with proven national coverage. Apart from these two 900Mhz networks, all five operators, KPN, Vodafone (formerly known as Libertel), Dutchtone, Ben and O2 (formerly known as Telfort) offer services via 1800Mhz networks. All the operators have interconnection agreements with the KPN fixed network so that their customers can reach fixed-network customers. Currently, most operators also have mutual interconnection agreements.

[25] http://www.vecai.nl/facts.asp

Figure 3.1: ***(c)*** **KPNQwest**



KPN has monopoly status as the incumbent fixed-network telephone line operator in the Netherlands, operating more than eight million fixed-network telephone lines. The KPN network is its *Lambda*-network, a fiber-optic network which interconnects the main conurbations in the Netherlands.[26] Even though the last mile connections are now open to competition, KPN still has a dominant position in this market.

Finally there are leased line operators. These operators offer high quality network connections. These include Worldcom(formerly UUNet), Infonet and KPNQwest. These operators use their own pan-European or global networks connecting major cities around the world.

The Netherlands host a number of Internet exchanges. The most important one is the Amsterdam Internet Exchange (AMS-IX)[27]. It is one of the biggest in Europe, comparable with the London Internet Exchange (LINX). Currently there are some 130 companies connecting 132 autonomous systems (AS) through 181 different ports. The average traffic is about 5 Gbits/sec and is still growing (figure for January 2002). Apart from the AMS-IX, operators use a variety of other interconnection points throughout the Netherlands.

The AMS-IX is based at four different locations in Amsterdam. Each location has links to at least two of the others, thus ensuring connectivity in case of failure of a link.

AMS-IX is unique in that it also has a function for the upcoming UMTS and GRPS operators. Many of these operators are already connected to AMS-IX. These operators will maintain private networks to support the mobile Internet services. To enable shared

[26] http://www.kpn.com

[27] http://www.ams-ix.net

roaming, a dedicated virtual exchange network (VLAN) is maintained by the AMS-IX, known as the GRX Peering Amsterdam (GP-A). AMS-IX will also offer naming services for these private networks. Note that there is no connection with the Internet; the GRX networks use private network IP numbers which cannot be routed on the Internet.

Recently, the Dutch-German Internet eXchange (NDIX) became active. This is an Internet switch in the east of the Netherlands located between the main economic center of the Netherlands (the area between Amsterdam, Utrecht, Rotterdam and the Hague, also known as the Randstad) and the German Ruhr-area.[28] Other Internet exchanges are located in The Hague, Groningen and Maastricht. The Internet exchange of the Hague is allied with the Ebone-consortium, and the NDIX is an important connection point in the Teleglobe network.

3.2 Organizations currently involved in networks

In the light of the above description of how networks are organized in the Netherlands, a look can now be taken at the organizations behind it.

Since 1998, an independent regulator[29], the OPTA, was established to provide oversight of all telecommunication networks. Its task is to oversee such issues as interconnection tariffs, frequency allocation and many other matters related to telecommunications.

The Dutch domain-registry authority, SIDN[30], is a non-profit foundation responsible for registration and issue of (.nl)-top level domain names. Its goals are quick and reliable issuing of domain-names, the maintenance of registrations, and promoting cooperation between its members and the local and international Internet community. SIDN is member of the Council of the European National Top-level Domain Registries (CENTR)[31] and is an active contributor in forums such as the Internet Corporation for Assigned Names and Numbers (ICANN) .[32] SIDN defines policy on the registration of domain names in consultation with the Dutch Internet community, carries out registration of the .nl domain names and runs the .nl name servers.

Around 55 ISPs are members of the NLIP[33], the Dutch Internet providers Union. NLIP represents its members in deliberations. Furthermore, NLIP has a code of conduct on quality and complaint settlements, with which members are obliged to comply. Members can be access providers, backbone providers or content providers. Access providers offer access to network backbones by ADSL, cable or telephone. Backbone providers offer connections between access providers to each other and with the Internet exchange points as discussed above. Content providers host services like e-mail, web hosting, and so on.

Approximately 40 cable operators, representing 98.5 per cent of the market, belong to VECAI[34]. VECAI represents cable operators and tries to influence government policy in the area of cable networks. VECAI is also trying the expand the possible uses of cable and obtain the necessary legal changes to allow these new opportunities.

[28] http://www.ndix.net/

[29] Further information on the creation of OPTA can be found in section 4.2

[30] http://www.sidn.nl/

[31]http://www.centr.org/

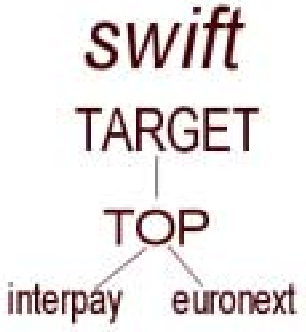
[32] http://www.icann.org/

[33] http://www.nlip.nl/

[34] http://www.vecai.nl/

3.3 Financial networks

Financial transactions within the Netherlands are carried out trough the Interpay[35] network. Interpay is a cooperation of Dutch banks, which was created after the merging of the Bank-girocentrale (BGC), MasterCard Nederland and Beanet.



"Each day, a large number of payments are processed between banks, businesses and consumers. Interpay Nederland was founded as a subsidiary of Dutch banks for the purpose of establishing, managing and developing an efficient payment infrastructure."

Interpay extensively modified its processing system on 1 October 2001. Throughout each day, Interpay compiles sub-batches of the payment traffic, by which the sums the banks owe one another are determined per sub-batch. This is known as "clearing". About every half hour, this information is submitted to De Nederlandsche Bank (DNB)[36], where all banks have an account. DNB is the Dutch national bank, which is authorized to debit and credit these accounts. This process is known as "settlement", and under the new arrangements it is performed throughout the day, while formerly settlement occurred only once each day. Since October 2001, the banks can also receive information regarding clearing and settlement more frequently. The banks may receive their information once every half hour or even less if the number of transactions exceeds a maximum to be determined per bank. With the new system, Interpay is the first clearing house in Europe to settle bulk payment traffic directly.

DNB processes the messages it receives from Interpay and Euronext (the stockmarket) by using the TOP paying system. On the top of the Dutch financial network, top acts as a real-time gross settlement system. All payments made by TOP are carried out in real-time and may not be recalled. A further possibility offered by the TOP system is real-time information on these transactions. Clients can acquire this information by using the Swift network or through the Internet. TOP is connected with other European countries through TARGET.[37] Target is a real-time gross settlement system for the clearing in the EURO zone. Target is part of the European Central Bank.

International financial transactions are handled through the Swift network.[38]. Swift is the Society for Worldwide Interbank Financial Telecommunications. It is an industry-owned cooperative supplying secure messaging services and interface software to over 7,000 financial institutions in 196 countries. Annually, 1.5 billion messages are processed. The daily value of payment messages on Swift is estimated to be above USD 6 trillion. These messages are carried over an X.25 network. Only firms connected with Swift have access.

At the present time, Swift is being transferred to IP technology. Recently, Swift signed an exclusive agreement with Global Crossing to provide secure IP connectivity for the Swift network (as well as the current X.25 network also run by Global Crossing). However, with the bankruptcy filing of Global Crossing, Swift has reassumed ownership of its networks. In May 2002, Swift entered into an agreement with Global Crossing to provide network operation activities. Swift will continue to roll out a highly secure, extremely reliable IP network to support their new generation of products and services. With standardized end-to-end automated communications, Swift standards are the accepted norm for financial messaging worldwide. Interpay, Euronext, TOP and Target all use the

[35] http://www.interpay.nl/

[36] http://www.dnb.nl/

[37] http://www.ecb.int/

[38] http://www.swift.com/

Swift standards. Swift is also the messaging hub for a growing number of high-value payment systems, securities infrastructures and foreign exchange settlement systems. These market infrastructures need a trusted third party to provide secure, reliable and proven messaging solutions to their diverse users. Banks and regulators are turning to Swift to fulfill that role.

Trust is also essential when trading over the Internet. Swift's standardized web-based products enable financial institutions to offer trust services and e-payments to corporate customers active in B2B e-commerce. Swift's trusted third-party status extends beyond market infrastructures and the Internet. The international nature of the Swift shareholders and the industry-owned cooperative structure has shaped best practice in the financial industry and act as a forum to advance critical dialogue on industry-level issues and opportunities.

3.4 Vulnerabilities in the Netherlands

In 2000, the Ministry of Transport, Public Works and Water Management commissioned a study from the Stratix Consulting Group and TNO-FEL aimed at identifying current weaknesses and vulnerabilities of the Internet in the Netherlands. The report[39], known as the "KWINT report", provided a good analysis of the vulnerabilities of networks in the country. Based on the recommendations of this report, a number of actions have been taken both by the private sector and the government to remedy these issues.

The KWINT report[40] on the vulnerability of Internet describes vulnerabilities at different levels. First and foremost of these is the information and general application layer. In order to get a good picture of vulnerabilities of this layer, CERT-NL has made a list on how many times incidents occur[41]. These statistics help to gain insight into the incidents that are reported each month, and on which problems CERT-NL[42] should focus its attention. It must be noted that the Netherlands has a number of CERT organizations for various networks, such as academic networks, the KPN network and government networks.

[39] Policy paper "Internet vulnerability", Ministry of Transport, Public Works and Water Management, Netherlands, 2001, http://www.dgtp.nl/english.html

[40] id.

[41] http://www.cert-nl.nl/statistics.shtml

[42] Further discussion of CERT-NL can be found in section 3.5

Table 3.1: Vulnerabilities in the Netherlands

Number and type of incidents occurring monthly

	2001	2000	1999
Abusive communication	10	16	9
Administrative	68	71	11
Denial of service	32	30	22
Lan sniffing	3	3	2
Other	10	43	10
Probe	227	204	132
Root compromise	48	31	19
Spam	40	82	45
Trojan	2	4	18
Unauthorized use	24	26	11
Virus	18	5	0
Warez	8	6	2
Total:	**481**	**521**	**332**

Vulnerabilities can lead to loss of confidence in e-commerce, fraud and loss of privacy or other important data.

On the network layer, there is a danger of the crashing of critical components, denial of service attacks, hacks on ISPs and poorly-secured networks. A well-aimed attack at an Internet exchange can completely knock out the exchange, collapsing the Internet in the Netherlands or even affecting international backbones.

Vulnerabilities in the transmission layer can result in failure where there is just one line between two points and this line is broken. A second, backup line can be a means to avoid failure in such cases. However, this may still not solve the problem as these redundant lines are often located in the same tube, or both lines may run through the same transmission point and are vulnerable if that point is put offline.

Other problems include physical attacks by terrorists, or the disruption of facilities such as the electricity supply. Facilities such as these are also subject to terrorist attacks, or to natural disasters. Even a shortage in the electricity supply can present a risk to networks.

Finally there are problems with the convergence and coordination between different systems. If there are different kinds of services using the same hardware, and different persons are responsible for this hardware, this can result in loss of coordination of the system.

Although most weak points are dealt with as soon as they are discovered, there are still some points where things can go wrong.

Internet exchange points and other points where networks are interconnected are vital points: one of these points failing as a result of natural or human causes can spell disaster. If there is just one connection between different networks, this leads to total loss of connection between the networks. At the present time, there is usually more than one connection point. With the growth in communications systems however, the possibility of other points becoming overloaded is increasing. At best, the amounts of data transmitted will have to be reduced, but in the worst case a chain reaction could occur, leading to total network failure.

Another problem is that redundant communication lines are sometimes run along in the same gutter because this is less expensive.

Another problem is chain dependencies. Because most mobile telephone operators use KPN for connections to other networks, failure at KPN will compromise the other operators too. Most emergency plans are made to function within its own organization. Where there are emergency plans between companies, these are the result of voluntary cooperation. NACOTEL is an example where there is some cooperation.

Problems are sometimes caused by dependencies at service level. When there was a blackout in Noord-Holland in 2001, the AMS-IX had serious problems during most of the day. Because AMS-IX is the most important Internet exchange in the Netherlands, this leads to problems all with Internet over the Netherlands.[43]

Uncertainties in the market present further threats to reliability of services for users. Currently, cable operator UPC is trying to overcome its financial problems. If UPC goes bankrupt however, its customers run the risk of loosing telephone, cable and Internet access.

Other problems include bugs and other software errors. As well as the well-known Y2K bug, a great number of unknown bugs may be present in new technology such as wireless LAN and i-mode. These technologies are often driven onto the market by economic motives and are not always well tested before they are taken up in business. These bugs will require patches, but because there are so many of these patches, and patching takes much time, there is already some patch fatigue.[44]

3.5 Information initiatives

It is assumed that Internet users have a heavy personal responsibility for the security of their systems and communications. Knowledge of the risks and of the means of controlling risks is a precondition for Internet users to venture onto the "electronic highway" with confidence. Objective and widely accessible information is therefore necessary, and needs to be geared towards the different users (e.g. consumers and business community, would-be, novice, and experienced Internet users).

A recent resolution of the Council of the European Union on a common approach and specific actions in the area of network and information security (15 January 2002) asks the member states "to launch or strengthen information and education campaigns to increase awareness of network and information security, and to encourage private sector-led initiatives".

surfopsafe

Already in 2001, the Dutch Government started an awareness and information campaign about information security, with a focus on the

[43] http://www.en.nl/994396857602.html

[44] http://www.webwereld.nl/nieuws/9400.phtml

Internet. This campaign is called SurfopSafe (http://www.surfopsafe.nl/) and is aimed at end-users (households and small companies). The focus of http://www.surfopsafe.nl/ is e-mail, web surfing, Internet shopping, chatting, continuous online, securing company information and the use of mobile Internet.

In addition, more static and dynamic information about vulnerabilities is also important to enable users of the Internet to take countermeasures. Information on network security and on how to respond to emergencies is given by so-called CERTs. A CERT is a team that handles security breaches that occur inside its area of support. The area of support can consist of all workers in a company, of the customers of a given ISP, or users of a certain piece of software. Not every CERT has the same objectives. Some have are more oriented towards informing people than others. In the Netherlands, several CERT's exist, such as CERT-NL for Dutch universities . At the moment, the government is setting up a CERT for it's own area network, but also to inform the public.

4 Regulatory Climate

4.1 Regulation at European level

The market for telecommunication networks and services in Europe has been liberalized for quite some time now. In 1998 the European Parliament adopted a set of 18 directives—the so-called Open Network Provision directives, better known as "ONP". The aim of these directives was to open the market to new entrants and at the same time give these new start-ups some "backing" by providing a set of rules that would grant them extra privileges compared to the incumbent operators. It was generally felt that applying "common competition rules" in a under-developed market would, from a competitive point of view, hamper the chances of survival of the new companies.

A revision of this set of rules was foreseen last year. Currently, four new directives are on their way to being implemented under national legislation, a fifth directive on data protection in electronic communication networks, is still under negotiation.

Apart from these directives, the European Commission stimulates several initiatives on promoting the use of electronic networks and new media. More information on EU initiatives can be found at: http://www.europa.eu.int.

4.2 Regulation at national level

Legislation at national level is heavily influenced by the implementation of European directives under national legislation. Most of the regulation can be found in the 1998 Telecommunications Law.

Furthermore, due to the liberalization of the telecommunication market, an independent regulator for telecommunications and post (OPTA), was created in 1998 by the law on OPTA. The independent regulator has to ensure fair competition in the market and to see that all parties abide by the rules set by the government. As a result of the European directive on electronic signatures[45], OPTA also received the function of supervisor of Trusted Third Parties (in Europe also known as Certificate Service Providers). These are private parties that provide services in order to enhance the reliability of electronic data exchange.

Generally speaking, Dutch legislation has no specific provisions on the regulation of the Internet. However, certain acts, such as e.g. hacking, computer sabotage or data destruction, are considered criminal offences under Dutch law. Offenders can be prosecuted under the Dutch penal law code.

[45] Directive 1999/93/EG of the European Parliament and the Council of 13 December 1999

5 Current initiatives

5.1 International level

A number of initiatives are currently ongoing at international level to improve the security of network infrastructures and to provide law enforcement agencies with better tools to combat cybercriminality. The Netherlands is an active participant in many international activities aimed at improving global cooperation in the area of networking. For example, the Ministry of Transport, Public Works and Water Management is an active participant in the Governmental Advisory Committee of ICANN. The Netherlands is also home to the headquarters of the Network Coordination Centre of RIPE, the Réseaux IP Européens.

5.1.1 The European Commission

In December 1999, the European Commission launched its e-Europe initiative.[46] In elaborating the main theme, a cheaper, faster and more secure Internet, priority has been given to the element secure networks and other subjects relating to security of information. The Council of the European Union issued a resolution[47] on a common approach and specific actions in the area of network and information security. This resolution includes, *inter alia*, information and education campaigns to increase awareness of network and information security, the setting up of CERT's and the development of standards.

Results of a different kind have been sought under the action plan e-Europe 2002 communication about 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'[48]. In this communication, the Commission announces its intention to set up an EU forum in which various parties can improve their mutual understanding and cooperation at EU level. The forum includes law enforcement authorities, Internet service providers, telecommunication providers, civil rights organizations, consumer organizations and data protection bodies.

5.1.2 DNSSEC

It has been known for quite some time that there are vulnerabilities in the Domain Names System (DNS) protocol, such as spoofing of information. In the Internet Engineering Task Force (IETF)[49] is work going on which will add to this protocol a security layer making use of digital signatures. Various individuals from european organizations are actively involved in this work . The Council of European Top-Level Domain Registries (CENTR) has a technical workgroup to study the ramifications for registers. SIDN is working together with NLnetlabs[50] to study the technical details of this protocol. NLnetlabs was instrumental in stimulating work in the IETF and proposing solutions for some hard problems related to the proposed protocol extensions.

5.2 National level

The Dutch government is taking several initiatives to improve networks security and availability.

In 2001, the Ministry of Transport signed an agreement with the telecom operators operating countrywide. This agreement is called NACOTEL (NAtional COntinuity plan

[46] http://www.europa.eu.int/information_society/eeurope/action_plan/index_en.htm

[47] http://www.europa.eu.int/information_society/eeurope/action_plan/safe/index_en.htm

[48] http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html

[49] http://www.ietf.org/

[50] http://www.nlnetlabs.nl

TELecommunication) and has the objective of implementing "best practice" continuity policies and manage crises if, despite the preventive measures, (part of) the network should fail.[51]

Since 2000, special attention has been paid to the Internet. Computer break-ins, viruses, and deliberate sabotage of computer systems are problems that already existed before the Internet era. However, with the advent of Internet, these incidents occur more frequently and on a much larger scale. Private individuals, companies, and institutions, are now connected with each other more strongly by means of information and communication networks. The increasing use of information and communication technology (ICT) in general, and the Internet in particular, also means that society is becoming ever more dependent on this technology. Because of this, such incidents can cause alarming social and economic damage. At the same time, if the number of incidents increases, individuals and companies will begin to lose confidence in the Internet. And confidence in Internet forms an important foundation of the information society. For this reason, the Dutch Government carried out its investigation into the nature and extent of the vulnerability of Internet in the Netherlands.

In its policy paper on Internet vulnerability[52], the government presents the result of this investigation. It also shows how the government wishes to make a contribution to the reliability of the Internet. This government policy is based on the principle of coordinated self-regulation. This means that the government wants to bring the parties involved together to work on solutions contributing to increased Internet security and reliability. At the beginning of 2002, a public-private project, KWINT, was launched to implement the policy lines as described in the paper on Internet vulnerability.

The two initiatives presented above aim at keeping the communication networks more or less on the level to which we are accustomed, and which we need in daily life. Despite these efforts however, should something happen that means that communication over this networks is not longer possible, there is a fallback network in the Netherlands. The National emergency networks (Nationaal Noodnet) has existed for ten years.[53] This is a closed network that connects 17 digital telephone exchanges. Two-way, geographical separated transmission lines connect these exchanges. In case of an emergency, it makes sure that most important parties have access to telecommunications (telephone). Currently, a study is under way on the Noodnet in order to find how it can be upgraded to meet present and future demands.

[51] NACOTEL, ministry of transport, public works and water management

[52] Policy paper "Internet vulnerability", Ministry of transport, public works and water management, Netherlands, 2001, http://www.dgtp.nl/english.html

[53] Nationaal noodnet, ministry of transport, public works and water management

[54] Policy paper "Internet vulnerability", Ministry of transport, public works and water management, Netherlands, 2001, http://www.dgtp.nl/english.html

[55] Nationaal noodnet, ministry of transport, public works and water management

6 Conclusion

Although the Netherlands is a small country, it is one of the front-runners in the development of the information society. Through its active participation in international organizations at both European and worldwide level, it has been instrumental in the development of many instruments on the legal and technical aspects of network implementation.

By virtue of being a member of the European Union, the Netherlands has implemented a large number of European directives in the area of telecommunications. This limits the freedom of action of the country as far as creating its own rules on such topics as network security. However, the Netherlands compensates for this by being an active participant within the European Union and thus stimulating the timely development of the necessary directives to promote the development of new applications and protect infrastructure and applications.

As a result of the implementation of European directives and a generally open-minded approach to law, the Netherlands has a liberal telecommunications environment, leaving the door open for self-regulation within the private sector. Instead of following an approach whereby new technologies need new laws, the Dutch Constitution leaves a certain margin of freedom to the judicial system, thus enabling the government to regulate new applications and systems using existing laws. This enables a faster response to change in society, as there is no immediate need to develop new laws to keep pace with the evolution of technology.

The same applies to criminal law. Dutch lawmakers tend to use a rather general approach to regulation instead of focusing on each and every detail. This is reflected in the approach to Internet criminality where most problems are handled through the use of existing penal law. By applying existing laws to new issues, the Ministry of Justice is able to respond to the changes in society without being constrained by outdated laws.

The Ministry of Transport, Public Works and Water Management is quite aware of the possible vulnerabilities of telecommunication networks. In order to study this topic, it commissioned a study in 2001 to identify the potential problem areas. The report of this study was implemented as a policy paper[56] which will serve as a lead to improve reliability of information systems in the Netherlands.

One of the first visible improvements resulting from the policy paper is the multi-homing of the Amsterdam Internet Exchange, thus removing the single point of failure of Internet connectivity in the Netherlands. Thus, by taking a proactive approach to the security of network infrastructures, the Netherlands government prevents mishaps, through an early identification and resolution process.

The private sector has been active in self-regulation. An example of this is the Stichting Internet Domeinregistratie Nederland (SIDN), the organization responsible for the registration of Internet domain names within the .nl country domain. By following developments in a proactive manner, SIDN has addressed aspects such as intellectual property and domain name ownership without the need for laws to be developed, thus promoting further growth of the Internet in the Netherlands.

Another example of the activity of the private sector is the active role of SIDN in the implementation of the new security standard for Internet domain names, DNSSEC. Even though no major problem has yet been experienced due to vulnerabilities in the domain name system, the Dutch Internet community has identified the issue and is working at preventing possible attacks.

[56] Policy paper "Internet vulnerability", Ministry of transport, public works and water management, Netherlands, 2001, http://www.dgtp.nl/english.html

Overall, one can say that, through the use of flexible laws and a positive cooperation between government and the private sector, the Netherlands is able to resolve many vulnerability issues before they become a real threat. Through the effective exchange of information, the various entities involved in networking are able to work together to provide the Netherlands with a stable and reliable collection of networks.

Appendix 1: References

- CIA World Factbook, http://www.cia.gov/cia/publications/factbook/
- Telegeography, 2001
- 2001 World Development Indicators, The World Bank
- ITU World Telecommunication Indicators
- ITU Internet Reports 2001
- ITU Trends in Telecommunication 2000-2001
- "Netwerken in cijfers", Ministry of Transport, Public Works and Water Management, The Netherlands
- Jean Walrand, Communication Networks: A first course, Homewood, IL: Irwin, 1991
- Andrew S. Tanenbaum, Computer Networks (Third editition) Prentice-Hall, 1996
- Stratix, Eindrapport "Kwetsbaarheid van het Internet", ministry of transport, public works and water management, Netherlands, 2000
- Voorschrift Informatie beveiliging Rijksdienst (VIR), Ministry of Internal Affairs, Netherlands, 1994
- Mieke Borgers-Roozen ea, Werkplekbeveiliging, Informatiebeveiliging jaarboek 2000/2001