CIIP Country Surveys

The Netherlands

The Country Survey 2004 of the Netherlands was written with the help of Eric Luiijf, TNO Physics and Electronics Laboratory, and Roland de Bruin, KWINT, ECP.nl.

The Netherlands

Critical Sectors

With the *Quick Scan* method (see Part II for more details) and in consultation with the industry and government, it was determined that the Netherlands' critical infrastructure comprises 11 sectors and 31 products and services. Infrastructures are deemed critical if they constitute an essential, indispensable facility for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term. In the Netherlands, critical sectors and (products and services) include the following:[255]

- Drinking Water (Drinking Water Supply),
- Energy (Electricity, Natural Gas, and Oil),
- Financial (Financial Services and Financial Infrastructure both Public and Private),
- Food (Food Supply and Food Safety),
- Health (Health Care),
- Legal Order (Administration of Justice and Detention, Law Enforcement),
- Public Order and Safety (Maintaining Public Order, Maintaining Public Safety),
- Retaining and Managing Surface Water (Management of Water Quality, Retaining and Managing Water Quantity),
- Telecommunications (Fixed Telecommunication Network Services, Mobile Telecommunication Services, Radio Communication and Navigation, Satellite Communication, Broadcast Services, Internet Access, Postal and Courier Services),
- Public Administration (Diplomacy, Information Provision by the Government, Armed Forces and Defense, Public Administration),
- Transport (Road Transport, Rail Transport, Air Transport, Inland Navigation, Ocean Shipping, Pipelines).

The Critical Information Infrastructure (CII) of the Netherlands consists mainly of the internal supporting infrastructure of critical sectors like the energy, transport, and financial sectors, and is supported by a set of

[255] Ministry of the Interior and Kingdom Relations. The Netherlands, April 2003: Critical Infrastructure Protection in The Netherlands, p. 13–14.

services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, Internet access, electricity). It is explicitly not considered as an infrastructure in its own right. However, the KWINT program (see below) is targeted at the protection and safe use of the Internet.

Initiatives and Policy

In the Netherlands, CIP/CIIP is perceived increasingly as a crucial issue of national security. Since the end of the 1990s, several efforts have been made to better manage CIP/CIIP.

"The Digital Delta"

The publication "*The Digital Delta*" (June 1999) offers a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years.[256] This memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructure and of mastering the growing complexities of advanced IT applications.[257]

Defense Whitepaper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the *Dutch Defense Whitepaper 2000*: "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."[258]

Infodrome Initiative and BITBREUK

In March 2000, the key essay *BITBREUK* (English version "In Bits and Pieces") was published by the government-sponsored think tank *Infodrome*

[256] http://www.gbde.org/egovernment/database/netherlands.html.

[257] Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society.* (Translation of he Dutch Infodrome essay "BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij). (Amsterdam, March 2000), p. 5.

[258] Ministerie van Defensie, *Defensienota 2000*, (1999), p. 59.

to stimulate the discussion on the need to protect CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in co-operation with the appropriate national public and commercial organizations.[259] In mid-2001, this document was used as a starting point for a so-called 24-hour cabinet session. This was a 24-hour workshop with a selected group of experts that created a manifesto on CI/CII issues with a set of recommendations for all political parties. This KWINT-manifest document is available only in Dutch.[260]

KWINT Report and Memorandum

The report entitled *Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid* (KWINT), written by Stratix/TNO[261] for the *Ministry of Transport, Public Works, and Water Management* (V&W), was completed in 2001. The report concluded that the Dutch Internet infrastructure is extremely vulnerable. Final recommendations on policy measures were made with regard to awareness and education, coordination of incidents, protection, security. It was concluded that the measures should be taken within a public private partnership approach, while the government should play a facilitating and coordinating role.[262]

The findings and recommendations of this report triggered the implementation of an interdepartmental working group of members of the *Ministries of Economic Affairs, Defense, Finance, the Interior, Justice,* and *Transport* (Telecom and Post Directorate) [263]. As a result, the KWINT government memorandum (*Vulnerability of the Internet*) was endorsed by the cabinet on 6 July 2001. It includes a set of recommendations for action. A government-wide computer emergency response team (GOVCERT.NL) was established and a malware alerting service for SMEs and the public was set

[259] Luiijf, Eric, M. Klaver. *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society* (Translation of the Dutch Infodrome essay "BITBREUK, de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij") (Amsterdam, March 2000).

[260] http://www.infodrome.nl.

[261] TNO is the Netherlands' Organization for Applied Scientific Research.

[262] De Bruin, Ronald. "From Research to Practice: A Public Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". *Dependability Development Support Initiative (DDSI) Workshop* (28 February 2002).

[263] The Telecom and Post Directorate (DGTP) became part of the Ministry of Economic Affairs as of 1 January 2003.

up. Other actions were tasked to ECP.NL, the public private platform for e-Commerce in the Netherlands.

The Dutch CIIP policy as laid out by KWINT is based on three premises: measures should not decrease innovation, the dynamic character of threats should be taken into account, and there is no 100 per cent reliability.[264] The government policy is aimed at fostering wider application of ICT and an understanding of the consequences. In its report, entitled "Government losing ground", the WRR,[265] a government advisory body, analyzed some of the political aspects of the further advance of ICT across society.[266]

Anti-Terrorism Plan

In the aftermath of 11 September 2001, the Minister of the Interior was tasked by the Cabinet in early October 2001 with developing a coherent set of measures to protect CI/CII as part of the nation's anti-terrorism plan.[267] The *National Co-ordination Center* (NCC), which is part of the *Ministry of the Interior and Kingdom Relations*, has been tasked with developing an integrated set of measures to protect the critical infrastructure within a multi-step project, called "Bescherming Vitale Infrastuctuur" (*Protection of the Dutch Critical Infrastructure*). This project will run until 2004 and comprises the following steps:[268]

- Quick Scan (see below),
- Public private partnership kick-off workshop,
- Investigation of vital nodes,
- Risk analysis generating a list of measures, which is compared to the list of measures already taken generating a balanced set of actions by government and industry.

In June 2002, 11 working groups were formed, one for each vital sector. In April 2003, the findings of the Quick Scan, performed in close collaboration with the *Netherlands Organization for Applied Scientific Research* (TNO) were published by the *Ministry of the Interior*.[269] The objective of Quick Scan was to give an overall view of the essential products and services that comprise the Netherlands' CI, to determine their interdependencies and to

[264] De Bruin, From Research to Practice.

[265] Wetenschappelijke Raad voor het Regeringsbeleid.

[266] http://www.infodrome.nl/english/missie-eng.html.

[267] House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.

[268] Ministry of the Interior and Kingdom Relations. The Netherlands, April 2003: Critical Infrastructure Protection in The Netherlands, p. 9.

[269] Ibid, p. 7.

consider the consequences of their possible breakdowns. (→ for details, see Part II, chapter 1 on Sector Analysis, Example 2).

In December 2002, the following main conclusions could be drawn from the Quick Scan results:

- The Dutch government and industry now have a clear understanding of the critical products and services that comprise the Netherlands' critical infrastructure, and of their (inter-) dependencies,
- The direct and indirect vitality of critical products and services have been elaborated,
- It became clear that actors responsible for critical products and services have merely a limited understanding of other critical products and services depending on them, and of the extent of this dependence.[270]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP will include risk and vulnerability analyses by sector, scenarios to test the effectiveness of CIP/CIIP measures, and international interdepartmental exchange of information and coordination.[271]

Hacking Emergency Response Team (HERT)

In June 2002, the cyber-crime unit of the Dutch police (KLPD) founded a special response group to be activated if the ICT part of a CI were attacked. The priorities of the *Hacking Emergency Response Team* (HERT) will be to restore CI services and assist in recovery and logistics while collecting evidence. The intention is to have public private co-operation in this area, bringing in experts from other organizations in order to analyze and mitigate the problem. HERT will be fully operational in a few years.

Organizational Overview

Public Agencies

As stated above, responsibility for the Dutch CII lies with various actors and involves both public and private sectors as well as multiple ministries. In particular, the *Ministry of Economic Affairs/Telecom and Post Directorate* is responsible for the protection policy for telecommunications and the

[270] Ibid, p. 23.
[271] Ibid., p. 25.

Internet. Other parts of the same ministry are responsible for CIP/CIIP policies regarding the energy sector and private industry, including SMEs. The *Ministry of the Interior* is responsible (in terms of policy) for the protection of government information infrastructures and coordinates CIP policy across all sectors and responsible ministries.

Ministry of the Interior (BZK)

The duties of the *Ministry of the Interior* include the promotion of public order and safety and the administration of the national police forces. It includes the *National Co-ordination Center* (NCC), which is in charge of coordination activities at policy level in case of emergencies with nationwide impact.

Ministry of Economic Affairs

The *Directorate-General for Telecommunications and Post* was subordinate to the *Ministry of Transport, Public Works, and Water Management* (V&W) until mid-2002. The directorate is now subordinate to the *Ministry of Economic Affairs*. The two most important goals are the strengthening of the Netherlands' competitive position in the field of telecommunications, telematics, and postal services, and to ensure that these facilities remain available to citizens and companies.[272]

Furthermore, this ministry is responsible for C(I)IP policy in the energy sector and within the private industry, including SMEs.

Ministry of Transport, Public Works, and Water Management (V&W)

The *Ministry of Transport, Public Works, and Water Management* (V&W)[273] is responsible for CI in transport and water management (quantity). The biochemical quality of the surface water lies within the responsibility of the *Ministry of Health* (VWS).

General Intelligence and Security Service (AIVD)

The *General Intelligence and Security Service* (Algemene Inlichtingen- en Veiligheidsdienst, AIVD, formerly called BVD[274]) is a division of the *Ministry of the Interior* and is tasked with information security and the protection of vital sectors of Dutch society.[275] The AIVD´s focus shifts in accordance

[272] http://www.minez.nl/default_bel.asp?pagina=english.

[273] http://www.minvenw.nl/cend/dco/home/data/international/gb/index.htm.

[274] In December 2000, a total of 594 personnel were employed by the BVD.

[275] http://www.fas.org/irp/world/netherlands/bvd.htm.

with social and political changes. One of its tasks is to uncover forms of improper competition such as economic espionage that could harm Dutch economic interests.[276] Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere.[277] The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

Public Private Partnerships

In general, public private partnerships in the Netherlands are organized by agreement between the actors.[278] The government is usually a facilitator bringing together the actors concerned.[279]

The above-mentioned KWINT study of 2001 has led to a flurry of policy recommendations, which are elaborated in further detail in the public private partnership platform ECP.NL. These recommendations include awareness-raising, research and development, alarm and incident response, and integrity of information.

Public private co-operation within the project 'Bescherming Vitale Infrastuctuur' (Protection of the Dutch Critical Infrastructure) also involves the *Confederation of Netherlands Industry and Employers* (VNO-NCW) in a coordinating private-sector role.

Platform Electronic Commerce in the Netherlands (ECP.NL)

ECP.NL[280], the platform for *e*Netherlands, has been tasked by the *Ministry of Economic Affairs* with setting up a public private partnership program to implement the action guidelines of the KWINT Memorandum

The objective of the KWINT program[281] is to define concrete protective measures against the risks of Internet usage for businesses, consumers, the government, and citizens. A second objective is to provide a platform for public private partnership, and in this way provide a sounding board for government policy-making. The steering board and the various working groups consist of representatives of the government and the private sector.

[276] http://www.minbzk.nl.

[277] http://www.minbzk.nl.

[278] This has been common practice in the Netherlands since the 13th century in the continuous struggle against flooding by rivers and the sea.

[279] Interview with a representative of Netherlands' Organization for Applied Scientific Research (TNO), April 2002.

[280] http://www.ecp.nl/ENGLISH/index.html.

[281] http://www.kwint.org.

Acting on the recommendations of a risk analysis, the program is currently focused on the following aspects: continuity of the Internet infrastructure in the Netherlands, viruses, denial of service attacks, hacking, transparency of Internet services, integrity and confidentiality of information, and misuse by personnel.

Within the program, a best practice has been developed for defining solutions, creating commitment, and communicating solutions to end-users who will be implementing them. The program has delivered many different results, varying from complex risk analyses to practical tools. Commitment has been created not only among participants, but also among many stakeholders. To this end, public stakeholder debates are organized involving politicians, researchers, business executives, and users. KWINT Marketplaces are organized to present solutions to intermediary organizations that play a key-role in disseminating them to their members. These intermediaries also provide feedback to the KWINT program on the actual implementation of the solutions by their members. Finally, the program also actively anticipates and works in close co-operation with government on international developments, for example within the OECD and the European Union.

As stated above, the KWINT program also focuses on the continuity of the Internet infrastructure in the Netherlands. Since the Internet is regarded as one of the critical infrastructures, any results within this area of activities are also delivered to the CIIP initiative of the Dutch government. Apart from that cooperation, a liaison with the steering board and the government CIP initiative has been established.

Infodrome

Infodrome[282] is a think-tank founded in 1999 and sponsored by the Dutch government. Infodrome serves a threefold objective: (1) to develop an understanding of the social implications of the information revolution (this requires the gathering of empirical, quantitative knowledge and data on IT-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the importance of having a government policy that meets the requirements of the information society, and (3) to examine the priorities given by parties and interest groups to activities (public or private) undertaken in relation to the information society. This requires an understanding of the political and social value of knowledge, experience, and insights.

The organizational structure of *Infodrome* reflected the program's ambitious targets. The program was conducted under the direction of a steering

[282] http://www.infodrome.nl/english/missie_eng.html.

group and presided over by a member of cabinet. In addition, participants included members of important policy think-tanks. All ministries were represented in the supervisory committee. The structure ensured that politicians, (political) scientists, and representatives of the administrative system were actively engaged in the development of government strategy vis-à-vis the information age.

Early Warning Approaches

CERT-NL (part of SURFnet)

CERT-NL is the *Computer Emergency Response Team* of SURFnet, the Internet provider for institutes of higher education and many research organizations in the Netherlands. CERT-NL handles all computer security incidents involving SURFnet customers, either as victims or as suspects. CERT-NL also disseminates security-related information to SURFnet customers on a structural basis (e.g., distributing security advisories) as well as on an incidental basis (distributing information during disasters).[283] CERT-NL disseminates information coming from CERT-CC/FIRST.

NLIP Security Coordination Group

Some 55 ISPs are organized within the NLIP (Branchevereniging van Nederlandse Internet Providers), the Netherlands Internet Providers' trade association. This independent association has existed since 1997.[284]

GOVCERT.NL

A computer emergency response team for government departments (CERT-RO) was established in June 2002. In February 2003, it was renamed GOVCERT.NL.[285] It is operated under the responsibility of the *Ministry of the Interior*[286] under its ICT agency ICTU. GOVCERT.NL is co-located and co-operates with "Waarschuwingsdienst.nl",[287] a group that is responsible for issuing alerts and advice memoranda to the public and SMEs about

[283] http://cert-nl.surfnet.nl/home-eng.html.
[284] http://www.nlip.nl.
[285] http://www.govcert.nl.
[286] http://www.minbzk.nl.
[287] http://www.waarschuwingsdienst.nl.

viruses, Trojan Horse codes, and other malicious software, or "malware". Warnings are disseminated via e-mail, web services, and SMS, will soon be issued via public radio and TV channels as well. The Waarschuwingsdienst was founded in early 2003 and is funded by the *Ministry of Economic Affairs/Telecom and Post Directorate*.

At the tactical level, the KWINT program focuses on improving general awareness of ICT security through best-practice procedures. This includes, for example, the free provision of the Dutch version of ISO/IEC 17799:2000 (or BS 7799), the "Code voor Informatiebeveiliging". Currently, no early-warning or incident-analysis capability is planned at the strategic national level. This is because CII is mainly considered to be a subsidiary of the individual CI sectors.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger