CIIP Country Surveys

The Netherlands

The Netherlands

Concept of CIIP and Description of System

In the Netherlands, CIIP is defined as the measures to protect the country, its society, its international allies, and its economic (inter)national interests against the effects of deliberate or inadvertent disturbances or intrusions of CII.[1] The following are the critical sectors in the Netherlands:

- Banking and finance,
- (Tele) Communication,
- Defense,
- Drinking water,
- Energy and utilities,
- Food,
- Government,
- Justice,
- Objects with high risk in case of emergency,
- Public health,
- Public order and safety,
- Social sector,
- Transport,
- Water management.

Given their vital role for the Dutch and international society, for most of these sectors, CIIP is of high importance.

CIIP Initiatives and Policy

CIIP Initiatives

CIIP is being perceived more and more as a crucial issue of national security in the Netherlands. Since the end of the 1990s, several efforts have been made to better manage CIIP.

1 Interview with a representative of the Netherlands' Organization for Applied Scientific Research (TNO), April 2002.

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 to stimulate the discussion on CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in cooperation with the appropriate national public and commercial organizations.[2] 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 KWICT-manifest document is available only in Dutch.[3]

KWINT Report and Memorandum

The report entitled "Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid" (KWINT), written by Stratix/TNO[4] 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, etc. 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.[5]

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, Interior, Justice, and Transport (Telecom and Post Directorate). As a result, the KWINT government memorandum (Vulnerability of the Internet) was endorsed by the cabinet on 6 July 2001. It includes a number of recommendations for action.

2 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).

3 http://www.infodrome.nl.

4 TNO is the Netherlands' Organization for Applied Scientific Research.

5 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).

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.[6] A ministerial steering group including all ministers responsible for aspects of CI/CII will investigate the extent of the vital sectors first. In a second step, the critical parts of the sectors will be defined. Current measures will be assessed and additional measures proposed where necessary. Interdependencies and cross-sector aspects will be taken into account. The six-step project will last till 2004 and is scheduled to proceed as follows:

- Quick scan,
- Public-private partnership kickoff workshop,
- Formulation of availability band integrity requirements,
- Risk analysis generating a list of measures,
- List of measures already taken,
- Plan for measures to be taken. This includes ICT/information infrastructure of all sectors.

In June 2002, 17 working groups were formed, one for each vital sector and three for international, legal, and cross-sector dependencies.

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 is 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 cooperation in this area, bringing in experts from other organizations in order to analyze and mitigate the problem. HERT is to be fully operational in a few years. The 2002 initial phase is called "Bambi".

CIIP Policy

The Dutch CIIP policy 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.[7] The government policy is aimed at fostering wider application of ICT and an understanding

6 House of Parliament (Tweede Kamer). Dossier 27925 – action line 10.
7 De Bruin, From Research to Practice.

of the consequences. In its report, entitled "Government losing ground", the WRR,[8] a government advisory body, analyzed some of the political aspects of the further advance of ICT across society.[9]

"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.[10] This memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructure and of mastering the growing complexities of IT-applications that are already advanced in nature.[11]

Defense White Paper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the Dutch Defense White Paper 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."[12]

Law and Legislative Action

Penal Code

The Penal Code prohibits attacks against (non-ICT) CI (e.g., sabotage, intervening with water management systems, electricity, railways, etc.).

Cyber Crime Law I and Cyber Crime Law II

Both laws are under development and will include all the provisions of the EU Cyber Crime Treaty.[13]

8 Wetenschappelijke Raad voor het Regeringsbeleid.
9 http://www.infodrome.nl/english/missie-eng.html.
10 http://www.gbde.org/egovernment/database/netherlands.html.
11 Luiijf, Klaver, In Bits and Pieces, 5.
12 Ministerie van Defensie, *Defensienota 2000*, (1999), 59.
13 See http://www.minjust.nl/DOWNLOAD/COMPCRIM.DOC.

Telecommunications Law

This law states requirements of the public telecommunication operators regarding capacity, quality, and other properties of the services offered (e.g., free access to the 112 emergency number), as well as regulations with respect to safety and privacy precautions regarding their network and services.[14]

Organizational Analysis

Public Agencies

Ministry of the Interior and Kingdom Relations (BZK)[15]

The duties of the Ministry of the Interior include the promotion of public order and safety and the provision of centralized management of the countries' police forces. It includes the National Coordination Center (NCC), in charge of emergencies with nationwide impact.

Directorate General Telecommunications and Post[16]

The Directorate-General for Telecommunications and Post is subordinated to the Ministry of Transport, Public Works, and Water Management (V&W). The two most important goals are the strengthening of the Netherlands' competitive position in the field of telecommunications, telematics, and postal services, and to make sure that these facilities remain available to citizens and companies.[17] Other parts of the same ministry are responsible for the CI of transport and water management.

General Intelligence and Security Service

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) is a division of the Ministry of Interior and is tasked with information security and the protection of vital sectors of Dutch society.[18] The focus areas of the AIVD change in accordance with social and political changes. One of its new tasks is to uncover forms of improper competition such as economic espionage, which could harm

14 http://www.minvenw.nl/dgtp/home/data/tweng.doc.
15 In December 2000, a total of 594 personnel were employed by the BVD.
16 http://www.minvenw.nl/cend/dco/home/data/international/gb/index.htm.
17 http://www.minvenw.nl/cend/dco/home/data/international/gb/brief.htm#dgtp.
18 http://www.fas.org/irp/world/netherlands/bvd.htm.

Dutch economic interests.[19] Another new task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere.[20]

Cooperation between Public and Private Sectors

In general, public-private partnerships in the Netherlands are organized by agreement between the actors. The government is usually a facilitator bringing the respective actors together. The other actors cooperate according to their responsibility.[21]

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

Platform Electronic Commerce in the Netherlands (ECP.nl)[22]

ECP.nl (the Platform for Electronic Business in the Netherlands) has been asked to set up a public-private partnership program. Its activities cover six major areas: awareness, trust, interoperability, national projects, research and development, and international coordination. The first duty of ECP.nl is to inform a broad public about the application of electronic commerce for congresses, seminars, conferences, the own website, helpdesks, training, and electronic newsletters. ECP.nl also works on building trust. To this end, it is involved in several projects, including the implementation of various KWINT action lines.

Infodrome[23]

Infodrome is a think tank sponsored by the Dutch government. Started in 1999, it will run for three years. 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 information on information-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the

19 http://www.minbzk.nl.
20 http://www.minbzk.nl.
21 Interview with a representative of Netherlands' Organization for Applied Scientific Research (TNO), April 2002.
22 http://www.ecp.nl/ENGLISH/index.html.
23 http://www.infodrome.nl/english/missie_eng.html.

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 reflects the program's ambitious targets. The program is conducted under the direction of a steering group and presided over by a member of cabinet. In addition, participants include members of important policy think tanks. All ministries are represented in the supervisory committee. The structure ensures that politicians, (political) scientists, and representatives of the administrative system are actively engaged in the development of government strategy vis-a-vis the information age.

Early Warning

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 in which a SURFnet customer is involved, either as a victim or as a suspect. 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 calamities).[24] CERT-NL disseminates information coming from CERT-CC/FIRST.

NLIP Security Coordination Group[25]

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

CERT-RO

A computer emergency response team for government departments (CERT-RO) was established in June 2002. It is operated under the respon-

24 http://cert-nl.surfnet.nl/home-eng.html.
25 http://www.nlip.nl.

sibility of the Ministry of Interior (BZK[26]) under its ICT-agency ICTU. CERT-RO will be co-located and co-operating with an entity that is responsible for issuing alarms and advice memoranda to the public and SME about viruses, Trojan Horse codes, and other malicious software, or "malware". Public radio and TV channels will used for communication. This body will become operational at the end of 2002 and is funded by the Ministry of Transport, Public Works, and Water Management (V&W).[27]

Research and Development

The government of the Netherlands aims to engage the business community more actively in European research initiatives. This goal is to be reached through the provision of information on these initiatives and support for the submission of project proposals. The government will give more encouragement to systematic research. Some research has already been carried out at TNO (the Netherlands Organization for Applied Scientific Research).[28] Research at the universities in the field of Internet dependability and security should also be intensified.[29] The overall aim is to promote research into and development of new methods and aids for ensuring the security of information. Further important actors involved in CIIP research and development are the Dutch Ministry of Defense and the think tank Infodrome, as well as the Rathenau Institute.[30]

26 http://www.minbzk.nl.
27 Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs. Internet Vulnerability. (July 2001).
28 http://www.tno.nl/homepage_nl.html.
29 Dutch Ministry of Transport, Public Works and Water Management / Dutch Ministry of Economic Affairs, Internet Vulnerability.
30 http://www.rathenau.nl.