The Netherlands

Critical Sectors

Using the so-called Quick Scan method[1] and in consultation with the industry and government, it was determined in 2002 that the Netherlands' critical infrastructure comprises 11 sectors and 31 critical products and services.[2] That result was adjusted in the ensuing risk analysis phase. Since April 2004, the list comprises 12 critical sectors and 33 critical products and services. Infrastructures are deemed critical if they constitute an essential, indispensable service 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:[3]

.....

* This chapter was reviewed by Eric Luiijf, TNO Defense, Security and Safety; Williët Brouwer, Programme Manager Critical Infrastructure Protection, Ministry of the Interior; and André Griffioen, Deputy Programme Manager Critical Infrastructure Protection, Ministry of the Interior.

1 For more information on "Quick Scan", see the chapter on Past and Present Initiatives.

2 Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands", (April 2003). http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.

3 Ministry of the Interior and Kingdom Relations. "Report on the Netherlands", September 2005: Critical Infrastructure Protection, September 2005, p. 72.

- Drinking Water Supply,
- Energy (Electricity, Natural Gas, and Oil),
- Financial Sector (Financial Services and the Financial Infrastructure, both Public and Private),
- Food (Food Supply and Food Safety),
- Health (Urgent Health Care/Hospitals, Sera and Vaccines, Nuclear Medicine),
- 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 (Diplomatic Communication, Information Provision by the Government, Armed Forces and Defense, Decision-making by Public Administration),
- Transport (Mainport Schiphol, Mainport Rotterdam, Main Highways and Waterways, Rail Transport),
- Chemical and Nuclear Industry (transport, storage, and production/processing).

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 services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, internet access, electricity).

Past and Present Initiatives and Policies

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 manage CIP/CIIP better. The early initiatives and policies were aimed at information security in general, because there was no clear definition of critical infrastructures. This changed with the Critical Infrastructure Protection Project, which started in 2001 and formulated dedicated policies for CIP and CIIP.

Early Efforts to Protect Information and Communication Infrastructure

The Digital Delta

The publication The Digital Delta of June 1999 offered a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years.[4] This memorandum noted the increasing importance of ensuring the security of information systems and the communications infrastructure, and of mastering the growing complexities of advanced IT applications.[5]

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."[6]

4 http://www.gbde.org.

5 Eric Luiijf and Marieke Klaver. "In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society", (Amsterdam, March 2000); translation of the Dutch Infodrome essay 'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij, p. 5.

6 Ministerie van Defensie. "Defensienota 2000", (1999), p. 59.

Infodrome Initiative & BITBREUK

In March 2000, the key essay BITBREUK (English version In Bits and Pieces) was published by the government-sponsored think-tank Infodrome[7] 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.[8] 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 (KWINT-manifest) with a set of recommendations for all political parties. These recommendations provided the basis for the KWINT program to improve information security.

KWINT Report and KWINT Program

The report entitled Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid (KWINT),[9] written by Stratix Consulting/TNO[10] for the Ministry of Transport, Public Works, and Water Management (V&W), was completed in 2001. The report concluded that the Dutch internet infrastructure was extremely vulnerable. Final recommendations were made on policy measures with regard to awareness and education, coordination of incidents, protection, and security. The report concluded that the measures should be realized within

7 Infodrome was a think-tank founded in 1999 and sponsored by the Dutch government that served 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 Infodrome project ended in 2002.

8 Luiijf/Klaver, op. cit.

9 Vulnerability of the Internet – Working Together for Greater Security and Reliability.

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

a public-private partnership framework, while the government should play a facilitating and coordinating role.[11]

The findings and recommendations of this report triggered the formation of an interdepartmental working group of members of the Ministries of Economic Affairs, Defence, Finance, the Interior, Justice, and Transport (Telecom and Post Directorate).[12] 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. The government-wide computer emergency response team, GOVCERT.NL, was established, and a malware-alerting service for Small and Medium Enterprises (SMEs) and the public was set up.[13] Other KWINT tasks were given to the Platform Electronic Commerce in the Netherlands (ECP.NL), the public-private platform for e-commerce in the Netherlands.

The KWINT Program 2002–2005 was especially targeted towards the protection and safe use of the internet. The 2005 report to the Dutch parliament recognizes the need to address the security of ICT that is used across critical sectors. The dependency and vulnerability of Supervisory, Control, and Data Acquisition (SCADA), for instance, is a cross-sector ICT area that will be analyzed in detail.

Veilige Elektronische Communicatie (VEC)

The successor of the KWINT program is called Veilige Elektronische Communicatie (VEC).[14] The program started in January 2006 and will run for at least three years. The program is designed as a public-private partnership under the responsibility of the Ministry of Economic Affairs. It aims to raise

11 Ronald De Bruin. "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).

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

13 http://www.waarschuwingsdienst.nl.

14 Safe Electronic Communications.

general awareness of information security and will implement a pilot project to support SMEs in the fight against cybercrime.[15]

The Critical Infrastructure Protection Project

In early 2002, the Dutch government initiated the critical infrastructure protection project Protection of the Dutch Critical Infrastructure,[16] with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT.[17] The project includes four steps: 1) A quick-scan analysis of the Dutch critical infrastructure to identify products and services vital to the nation, the (inter-) dependencies of these products and services, and underlying essential processes; 2) stimulation of a public-private partnership; 3) threat and vulnerability analysis; and 4) a gap analysis of protection measures.

To identify sectors, products, and services comprising the national critical infrastructure, a Quick-Scan Questionnaire was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were augmented and refined in 17 workshops with the vital public and private sectors. In parallel, damage experts

15 http://www.minez.nl/dsc?c=getobject&s=obj&objectid=136886&!dsnameEZInternet&isapidir=/gvisapi/ (in Dutch). Cf. also: Marjolijn Durinck and Willem Boersma. "Public-Private Partnership in Awareness Raising: Internet Safety Awareness in the Netherlands". http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_public_awareness_raising_in_the_netherland_boersma_durincks.pdf.

16 Bescherming Vitale Infrastuctuur.

17 Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands", (April 2003). http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.

evaluated the potential damage impact of loss or disruption of vital products and services.[18]

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 and Kingdom Relations.[19] The following main conclusions were 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 has been elaborated;
- It became clear that actors responsible for critical products and services only have a limited understanding of other critical products and services that depend on them, and of the extent of this dependence.[20]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP included pinpointing the vital nodes for each of the critical services, risk and vulnerability analyses for each critical sector, scenarios to test the effectiveness of CIP/CIIP measures, and an international exchange of CIP/CIIP information and coordination.[21] In addition, the CIP project has been established as a regular policy file under the responsibility of the Ministry of the Interior

18 To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are "merely" very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society. Eric Luiijf, Helen H. Burger, and Marieke H.A. Klaver, "Critical Infrastructure Protection in the Netherlands: A Quick-scan". In: Urs E. Gattiker, Pia Pedersen, and Karsten Petersen (eds.): EICAR Conference Best Paper Proceedings 2003.

19 Ibid., p. 7.

20 Ibid., p. 23.

21 Ibid., p. 25.

and Kingdom Relations. In 2005, the ministry outlined the Report on Critical Infrastructure Protection for the attention of the Dutch parliament. The report contained a review of the achievements of the CIP Project and defined a new set of actions.[22]

- Intensifying critical infrastructure security policy: CIP is a collective task, and it is important that all relevant stakeholders pull together to improve the security of national infrastructures. Therefore, a Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was created (for more information, see the chapter on Organizational Overview);
- Analyzing CIP dependency: fostering cross-critical sector communication is also the goal of the CIP Dependency project. Critical sectors must be able to get in touch with each other – not only to determine the extent of the crisis, but also to assess its likely duration. The project is underway and will determine whether the affected critical sectors will have to take additional measures in order to guarantee continuity;
- Improving protection of critical infrastructures against human threats: protection against willful disruptions of vital services is a high priority. Such attacks may be conducted by hackers, activists, frustrated employees, ordinary criminals (who are motivated by financial gains), and terrorists. In order to prevent such attacks, cooperation between law enforcement units, the intelligence services, CERTs, and private parties is indispensable. The National Advisory Centre Critical Infrastructures (NAVI)[23] provides a platform for mutual exchange among these organizations;
- Awareness-raising: Scenario exercises will be implemented involving distribution plans for CI products/services in the event of scarcity of supply, both at the national and regional levels.

Progress reports on these activities were published in 2006 and 2007.[24]

22 House of Parliament (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex "Rapport ter Bescherming Vitale Infrastructuur", dated 1 September 2005.

23 http://209.85.135.104/search?q=cache:ghBixn6L-noJ:www.fbiic.gov/reports/neth_2.pdf+%22govcert%22+%22aivd%22&hl=de&ct=clnk&cd=7&gl=ch.

24 Kamerstuk 2006–2007, 26643, nr. 83, Tweede Kamer and Kamerstuk 2007–2008, 29668, nr. 18, Tweede Kamer.

National Security Strategy and Work Programme 2007-2008

In order to cope with emerging risks, the Dutch cabinet has drawn up a National Security Strategy and Work Programme for the years 2007–2008.[25] The strategy defines the goals of Dutch security policy, analyzes and assesses threats and risks, and develops methods for strategic planning. The strategy pursues an all-hazard approach and aims to provide for a more coordinated and integrated approach to national security.[26]

Accordingly, the strategy will serve as a framework for the future protection policies for critical infrastructures.[27] The document states that there are many potential threats to the country and that each of these threats puts a strain on national security. National security is conceived as being under threat when vital interests of the Dutch state and society are harmed to the extent that society can become destabilized. These vital interests, and examples thereof, include the following:[28]

- Territorial security: the threat or occurrence of (terrorist) attacks on Dutch soil;
- Economic security: the breakdown of overseas trade or an ICT malfunction;
- Ecological safety: an environmental disaster or disruption of the drinking water supply;
- Physical safety: a dyke breach or epidemic;
- Social and political stability: tension between various ethnic groups.

25 "National Security Strategy and Work Programme 2007–2008". http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/88474/natveiligh.bwdef.pdf.
26 Dick Schoof. "National Security Strategy – The Netherlands", Presentation, 25 September 2007. http://www.hightechconnections.org/files/HTC_homeland_security_Dick_Schoof.pdf.
27 "National Security Strategy and Work Programme 2007–2008" op. cit., p. 18.
28 http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security.

In the Netherlands, national security encompasses both breaches of security by intentional human actions (security) and breaches due to disasters, system or process faults, human failure, or natural anomalies such as extreme weather (safety).

The new approach aims at allowing signals of potential threats to be identified at an earlier stage, by systematically linking information streams and cross-referencing developments (e.g., to what extent will energy requirements change if summers become warmer and more air conditioning and refrigerators are needed). The strategy formulates a method of weighing various interests and strives to prioritize among them.[29] Clearly, critical infrastructure protection is intimately linked with the National Security Strategy and planning. One of the capabilities named to be strengthened according to the national risk assessment (part of this programme) is business continuity.[30]

In 2008 one of the issues addressed within the National Security Strategy is ICT failure. A project called "ICT-verstoring" was initiated in which relevant private and public parties co-operate in a government-wide analysis and risk assessment of ICT. In this project, short, medium, and long-term ICT threats to the Netherlands are identified and analyzed in terms of their likelihood and potential impact. The insights gained from this process are used to assess whether preventative capabilities and preparation are sufficient to cope with these threats.

Organizational Overview

Responsibility for the Dutch CI and CII lies with various actors and involves public and private sectors as well as several ministries, including the Ministry of the Interior and Kingdom Relations, the Ministry of Economic Affairs, the Ministry of Transport, Public Works, and Water Management, the Ministry of Housing, Spatial Planning, and the Environment, and the Ministry of Health,

29 http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security.

30 http://www.minbzk.nl/onderwerpen/veiligheid/veilige-samenleving/nationale-veiligheid/publicaties/112985/item-112985.

Welfare and Sport. The General Intelligence and Security Service is also involved in protecting information security in the Netherlands.

Moreover, public-private partnerships play a crucial role in CIP and CIIP in the Netherlands. As mentioned above, the KWINT program and the Critical Infrastructure Protection Project are both based on public-private collaboration. The KWINT program led to a flurry of policy recommendations that are elaborated in further detail in the public-private partnership Platform Electronic Commerce in the Netherlands (ECP.NL). These recommendations refer to awareness-raising, research and development, alarm and incident response, and the integrity of information.

Public-private co-operation within the project Critical Infrastructure Protection Project gained further importance with the official establishment of the Strategic Board for CIP (SOVI). With regard to the protection of critical information infrastructures, the National Continuity Consultation Platform Telecommunication (NCO-T) is of special interest, because it enables public-private collaboration between the government and telecommunication companies on continuity planning and crisis response. Furthermore, the National Advisory Centre Critical Infrastructures is an initiative of the government striving to enhance information exchange on security issues between critical sectors, critical sector enterprises, and government agencies. Finally, the National Infrastructure against Cyber-Crime is a cyber-crime information-sharing model organized as a private-public partnership program.

Public Agencies

Ministry of the Interior and Kingdom Relations (BZK)

First of all, the Ministry of the Interior and Kingdom Relations (MoI) is responsible for the general C(I)IP policy, the co-ordination of the national activities across all sectors and responsible ministries, and international policy (e.g., EPCIP) and co-ordination. Additionally, the MoI is responsible for the protection of government information infrastructures (government CIIP), national emergency management, and the CIP aspects of emergency response services. The national emergency management includes the National Crisis Centre (NCC), which is

in charge of co-ordination activities at the policy level in case of emergencies and disasters with a nation-wide impact.

Ministry of Economic Affairs (EZ)

Some other key C(I)IP areas are the responsibility of the Ministry of Economic Affairs (EZ). EZ is responsible for C(I)IP coordination with the private sector in the areas of energy and telecommunications, including the internet.[31] Other parts of the same ministry are responsible for CIP/CIIP policies regarding 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)[32] is responsible for the public-private C(I)IP co-ordination for the critical infrastructures related to transport (road, rail, air, harbors, and inland shipping) and water management as well as the biochemical quality of the surface water.

Ministry of Housing, Spatial Planning, and the Environment (VROM)

The Ministry of Housing, Spatial Planning, and the Environment (VROM)[33] is responsible for public-private co-ordination of the C(I)IP activities of the chemical and nuclear industries, as well as the potable water infrastructure.

31 http://www.minez.nl/content.jsp?objectid=140727.
32 http://www.verkeerenwaterstaat.nl/english.
33 http://international.vrom.nl/pagina.html?id=5450.

Ministry of Health, Welfare and Sport (VWS)

The Ministry of Health, Welfare, and Sport (VWS)[34] is responsible for the public-private coordination of the C(I)IP activities of the health sector.

General Intelligence and Security Service (AIVD)

The General Intelligence and Security Service (AIVD)[35] is a division of the Ministry of the Interior and Kingdom Relations and is tasked with protecting the information security and vital sectors of Dutch society.[36] The AIVDs focus shifts in accordance 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. Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere. The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

Public-Private Partnerships

Platform Electronic Commerce in the Netherlands (ECP.NL)

The Platform Electronic Commerce in the Netherlands (ECP.NL)[37] 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 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. As the KWINT program expired in

34 http://www.minvws.nl/en.
35 Algemene Inlichtingen- en Veiligheidsdienst. https://www.aivd.nl/.
36 http://www.fas.org/irp/world/netherlands/bvd.htm.
37 http://www.ecp.nl.

2005, ECP.NL established the Digibewust program (Digital Awareness)[38] in order to improve awareness of information security.

National Continuity Plan for Telecommunications (NACOTEL) and National Continuity Forum Telecommunications (NCO-T)

The National Continuity Plan for Telecommunications (NACOTEL) was established in 2001 in order to structure the contingency policy and crisis management in the telecommunications sector. The public-private partnership included BT (IT-services), Enertel, KPN Telecom, Telfort, Orange, T-Mobile, and Vodafone – as well as the Ministry of Economic Affairs. NACOTEL was based on voluntary cooperation. The participants discussed possibilities to strengthen the security of the telecommunication sector. The building of trust was a central goal of the process. However, it became apparent that effective crisis management could not be achieved solely on a voluntary basis of cooperation. During crisis situations, it is possible that individual operators need to implement actions that run contrary to their interests. This analysis led to the decision to make participation in the public-private partnership mandatory for all operators of critical telecommunication services.[39] Therefore, NACOTEL was dissolved in February 2006 and replaced by the National Continuity Consultation Platform Telecommunications (NCO-T).[40]

Strategic Board for CIP (SOVI)

The Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was established in September 2006 as a dedicated public-private partnership for critical infrastructure protection. All critical sectors are represented in the strategic board, which meets two or three times a year. In 2007, the SOVI initiated a study on the electric power dependency of the various critical sectors and their resilience

38 http://www.digibewust.nl.
39 http://www.minez.nl/dsc?c=getobject&s=obj&objectid=150713&!dsname=EZInternet&isapidir=/gvisapi/.
40 http://www.ez.nl/content.jsp?objectid=150712&rid=150996.

and ability to cope with longer duration power outages. It investigated issues such as secondary dependencies (e.g., dependency of various sectors on diesel oil for back-up generators) and the way in which these are prioritized amongst the critical sectors. It also studied the question of which related arrangements already exist or have yet to be made.

Nationaal Adviescentrum Vitale Infrastructuur (NAVI)

The Dutch Nationaal Adviescentrum Vitale Infrastructuur (National Advisory Centre Critical Infrastructures, NAVI)[41] was initiated by the Dutch government as part of the CIP action plan discussed above.[42] In 2006, the Dutch parliament agreed to its business plan for 2006–2009.[43] NAVI has knowledge and expertise about the security of critical infrastructures and aims to exchange these with the critical sectors, critical sector enterprises, and government agencies. It builds upon its links within the government and critical sectors, such as current information provided by the AIVD and the Dutch National Coordinator for Counterterrorism (NCTb).[44]

NAVI offers various services to its constituency such as support for risk analysis as well as security advice. NAVI's modus operandi is derived from the (physical security aspect) of the UK's Centre for the Protection of National Infrastructure (CPNI). It has established sector-specific information exchanges between critical sectors and government functions. NAVI offers various services such as a front office and advisory function for critical infrastructure enterprises, good practices, and an international contact desk (information and good practices exchange with other nations and the EU). NAVI offers products such as risk analyses and risk methodologies, critical sector-specific threat scenarios, security methodologies, and advice.[45]

41 http://www.navi-online.nl.
42 House of Parliament (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex "Rapport ter Bescherming Vitale Infrastructuur", 1 September 2005.
43 House of Parliament (Tweede Kamer) 2006–2007, 26 643, No. 85.
44 http://www.nctb.nl.
45 Information provided by an expert.

Nationale Infrastructuur ter bestrijding van CyberCrime (NICC)

The National Infrastructure against Cybercrime (NICC) was established in 2006 as a three year program.[46] The NICC infrastructure consists of several components: a contact point, a reporting unit, trend-watching, monitoring and detection, information distribution, education, warning, development, knowledge sharing, surveillance, prevention, termination, and mitigation. The NICC further strengthens this infrastructure by hosting the Cybercrime Information Exchange, where public and private organizations share sensitive information, and by developing and supporting practical projects and trials that both solve concrete problems and generate knowledge about cybercrime.

The Cybercrime Information Exchange information-sharing model is based on the one designed by the UK's Centre for the Protection of National Infrastructure (CPNI). The NICC Information Exchange function can be pictured as following a 'flower' model. The heart of the flower is made up of government bodies, like the police, intelligence services, GOVCERT.NL, and the NICC itself. Critical infrastructure sectors and some other major industrial communities that heavily rely upon ICT can be thought of as being the petals of the flower. The different sectors chair their own petal, decide which parts of the meeting can be attended by the government bodies, and decide which information is sharable outside their sector 'petal'. The confidentiality of their exchanged information is maintained by an agreed set of rules on dissemination that follow the Traffic Light Protocol.

Many of the recognized information infrastructure sectors take part in a 'petal': The financial sector; providers of drinking water, energy, and telecommunication; Schiphol Airport; Rotterdam harbor; large enterprises / multi-nationals; and the rail sector.

One of the 2007 activities was the analysis of the information security posture of the SCADA and other process control systems in the Dutch drinking

46 http://www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf.

water sector. As a result, a SCADA security good practices document has been developed.[47]

It is expected that the NICC will receive new instructions in a successor program from mid-2009. The information exchanges will either continue under another public-private partnership entity or be merged with the NAVI activities that are oriented more towards physical security.[48]

Early Warning and Public Outreach

SURFCERT (part of SURFnet)

SURFCERT, formerly known as CERT-NL, is the Computer Emergency Response Team of SURFnet, the internet provider for institutes of higher education and for many research organizations in the Netherlands. SURFCERT handles all computer security incidents involving SURFnet customers, either as victims or as suspects. SURFCERT also disseminates security-related information to SURFnet customers on a structural basis (e.g., by distributing security advisories) as well as on an incidental basis (distributing information during disasters).[49]

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.[50] It is operated under the responsibility of the Ministry of the Interior and Kingdom Relations (MoI). The GOVCERT.NL team is co-located and cooperates with Waarschuwingsdienst.nl (Alert Service),[51] a website and initiative

47 Eric Luiijf. "SCADA Security Good Practices for the Dutch Drinking Water Sector", report TNO DV 2008 C096, (March 2008).
48 Information provided by the country expert.
49 http://cert-nl.surfnet.nl/home-eng.html.
50 http://www.govcert.nl/render.html?it=41.
51 http://www.waarschuwingsdienst.nl/render.html?cid=106.

provided by the Ministry of Economic Affairs/Directorate-General for Energy and Telecom (EZ/DGET). The Waarschuwingsdienst is responsible for issuing alerts and advice memoranda to the public and SMEs about viruses, Trojan codes, and other malicious software. Warnings are disseminated to the public via e-mail, web services, and SMS. The Waarschuwingsdienst was founded in early 2003 and is funded by the Ministry of Economic Affairs.

Law and Legislation

Penal Code

The Penal Code prohibits attacks against (non-ICT) CI (e.g., sabotage and interference with water management systems, electricity, the railway network, etc.).

Computer Crime Laws

The second version of the Dutch computer crime law has been under development since 1999. It was delayed because of the need to adapt it to the European Cybercrime Convention, and several anti-terror measures have been included in this new national law. The Computer Crime Law II was introduced in September 2006, with some articles taking effect from September 2007 onwards.[52]

Telecommunications Law

This law states the requirements that must be met by public telecommunication operators regarding the 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.

52 Official publication: Staatsblad 2006, 300 and 301, 13 July 2006.

Criminal Code, Articles 138a and 138b

In summary, Article 138a states that any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, is guilty of a breach of computer peace and shall be liable to a term of imprisonment not exceeding six months or a related fine[53] if they breach security by technical intervention with the help of false signals or a false key, or by acting in a false capacity.[54]

An unauthorized person penetrating an automated system who copies the contained, processed, or transferred information for their own use or use by a third party may be punished with a maximum of four years imprisonment. The same holds for someone using public telecommunications means for accessing an automated system with the purpose of own gain or gain of a third party or for unauthorized access to an automated system of a third party.

In summary, Article 138b states that whoever deliberately and without authorization disrupts an automated system by sending information to that system shall be punishable with no more than one year's imprisonment.

The penal aspects of disrupting various critical infrastructure services have been described in specific articles of penal law for electric power, railway systems, and water management, and are covered by a cybercrime law article that raises the penalties when the safety or even the lives of people are threatened, or when people are actually injured or die.

53 http://www.cybercrimelaw.net/laws/countries/netherlands.html.
54 Information provided by the country expert.