

The Netherlands Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: Dan Cimpean, Johan Meire, and Wouter-Bas Van der Vegt

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

THE NETHERLANDS	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	9
NIS GOVERNANCE	12
OVERVIEW OF THE KEY STAKEHOLDERS	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	13
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES	18
SECURITY INCIDENT MANAGEMENT	18
EMERGING NIS RISKS	20
RESILIENCE ASPECTS	21
PRIVACY AND TRUST	22
NIS AWARENESS AT THE COUNTRY LEVEL	23
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY	25
RELEVANT STATISTICS FOR THE COUNTRY	26
INTERNET ACCESS OF POPULATION AND ENTERPRISES	26
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	27
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	28
OTHER STATISTICS	29
APPENDIX	30
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES	30
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	32
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	33
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	34
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	36
REFERENCES	38

The Netherlands

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
 - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
 - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

In the area of NIS, the Dutch government increasingly takes measures with a wider scope. Where, in the first decade of this century, measures were mainly focused on the protection of vital sectors and the combating of cyber crime, currently cyber warfare and an integral cyber security strategy are also included on the political agenda. The Dutch government has taken several initiatives from a strategic perspective that are detailed further below, in particular regarding the development of a new e-government strategy, but most of all with the development of a national cyber security strategy.

In November 2010, The Netherlands published its first National Cyber Crime and Digital Safety Trend Report¹. This report has been drawn up by GOVCERT.NL under the joint auspices of the Ministries of the Interior and Kingdom Relations (BZK), Economic Affairs, Agriculture and Innovation (ELI) and Safety and Justice (V&J). Its aim is to bundle the main trends in the field of cyber crime and digital safety and to correlate them.

The trends are based on existing reports by organisations including KLPD, NCTb, AIVD and MIVD, OPTA and GOVCERT.NL and have been extended with insights from a broad group of experts. The report has a strategic and policy-neutral character, and presents key NIS considerations to be considered for future NIS strategy development.

eGovernment strategy

A new ICT and information strategy (I-Strategy) of the Dutch central government was developed in 2010. The strategy covers all ICT facilities for the management of the national government and a number of generic ICT facilities in the primary process. The I-Strategy is part of the 'Compact government' initiative by the current Cabinet. The strategy should ensure further centralization of management and operation in the field of ICT. The ultimate goal of the I-strategy is the provision and optimization of services to citizens and businesses. It acts as a catalyst for social developments in the field of competition and innovation, safety and welfare. With the I-Strategy, The Netherlands are fully in line with the Digital Agenda set by European Commissioner Neelie Kroes, while adding a number of other key elements.

The basis of the I-Strategy of the Netherlands is built on 6 key elements to adopt ICT further as enabler:

1. A more standardized digital working environment for government departments.
2. Digitalisation of information management of core government departments and collaboration.
3. Information security, based on risks
4. Optimisation of efficiencies and centralisation
5. Appropriate consideration of sourcing strategies
6. Consideration of a closed government cloud

¹ <http://www.govcert.nl/english/service-provision/knowledge-and-publications/trend+reports/trend-report-2010.html>

New cyber security strategy

The Netherlands consider trust in the Information Society as an important condition for economic development, prosperity and social welfare. In carrying out the political demands of the Dutch Parliament and the new Government, the administrations have been preparing a national cyber security strategy. This strategy embraces combating cybercrime including illegal and harmful content, improving network and information security, cyber defense and cyber warfare. The overall direction is performed by Ministry of Security and Justice (V&J), in close cooperation with the Ministry of Economic Affairs, Agriculture and Innovation (ELI), the ministry of the Interior (BZK) and the ministry of Defense.

The main goal is to reach more coherence and that the different activities are geared to one other. Public private partnership will be a basic principle. It's important to recognize that different Ministers will stay responsible for their own (mostly legally based) policy areas. In addition the security and resilience of communication networks and services will be part of the new Dutch national Digital Agenda too, which currently is still in preparation.

The Netherlands aim to be amongst the world leaders in terms of use and deployment of ICT in society and ensuring security of the digital society. It is considered that an open and free digital society contributes to the Dutch economic development, prosperity and welfare. Important conditions to allow this are the reliability of the ICT infrastructure, to protect the safety of those who enter in the digital society. Directed by the ministry of Safety and Justice (V&J) and with significant contribution of the Ministry of Economic Affairs, Agriculture and Innovation (ELI), a national cyber security strategy has been developed.

On February 22nd 2011, the minister of Security and Justice presented the first Dutch national Cyber Security Strategy² for approval by the Dutch parliament (Second Chamber). The strategy contains an analysis of the problem, a vision presentation, as well as an action plan.

The Dutch cyber security strategy presents the Dutch vision on basic principles for investing in cyber security, including:

- Linking and reinforcing initiatives;
- Public-Private partnership;
- Individual responsibility;
- Division of responsibility between departments;
- Active International cooperation;
- Proportionality of measures;
- Self-regulation if possible, legislation and regulation if necessary.

Furthermore the key highlights of the action plan presented in the Dutch cyber security strategy are:

1. **A Cyber Security Board and a National Cyber Security Centre will be created.** The Board, in which public and private parties are represented, will aim to ensure consistency and coordination in the activities in the field of cyber security. It is a wish of the Dutch government that public and private parties, on the basis of their own tasks and within the statutory options, information, knowledge and expertise, be brought together in a National Cyber Security Centre so that insight can be gained into developments, threats and trends, and support can be offered for incident handling and crisis decision making. The cabinet

² <http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/actueel/nieuws/nationale-cyber-security-strategie-gepresenteerd/nationale-cyber-security-strategie-gepresenteerd/govcert%3AdocumentResource%5B3%5D/govcert%3Aresource>

invites public and private parties to join this Centre. A joint venture model will be developed to enable this. In the Centre, based on the current GOVCERT.nl, existing knowledge and expertise from various public and private stakeholders will be brought together to gain insight into trends and developments and to support the operational control of ICT incidents and cyber attacks.

2. Additional efforts will be put in **preparing threat and risk analyses**. By increasing this knowledge, all relevant stakeholders can take measures in the entire chain, from prevention to response and investigation and prosecution. One of the tasks of the National Cyber Security Centre is the creation of one joint and integral picture of the topical threats of ICT. The Dutch Intelligence and security services will provide knowledge for the forming of this picture. Where necessary they will reinforce their cyber capacity. Annually the cabinet will be informed via the National Risk Assessment of the threats to national security.
3. There will be a focus on **increasing the resilience of vital infrastructure**. Social unrest due to ICT disruptions or cyber attacks must be prevented, and various parties have a responsibility in this respect, from citizen to supplier.
In order to achieve this objective, several actions were identified:
 - The Dutch Telecommunications Act will be updated in 2011. A number of existing agreements with the biggest telecoms companies on the continuity of their vital telecommunications infrastructure will be converted into regulations.
 - In the coming years the Cyber Crime Information Exchange will be continued under the flag of CPNI.nl. This year it will be reviewed how the cooperation between CPNI.nl and the National Cyber Security Centre will be given shape.
 - The government will stimulate the use of the usual minimum ICT security standards on the basis of good practices. The cabinet works with vital sectors to gain insight into possible measures to combat the disruption of their vital ICT facilities. On the basis hereof the government is urging vital sectors to take the identified measures. An example of this is the Emergency Communication Facility (NCV) which will replace the current Emergency Network as of 1 May 2011. Vital organisations will have the opportunity to connect to the Emergency Communication Facility.
 - Specifically to prevent (digital) espionage the cabinet has developed a package of measures. For companies an Espionage Vulnerability Analysis Manual is available with which they can increase their resilience to espionage.
 - The government aims that 80% of the organisations in the vital sectors of Public Administration and Public Order and Security will have a continuity plan by the end of 2011, including the scenario of a large-scale disruption of ICT and electricity.
 - In the middle of 2011 the cabinet will establish one security framework for information security for national government services and will present new Information Security Categorized Information Regulation. A nationwide monitoring cycle for information security will also be established.
 - In the course of 2011 the cabinet will decide whether travel documents will include an electronic Identity card which satisfies the highest reliability level for citizens.
 - The government is implementing the European disclosure obligation for data leaks with regard to the Telecom Sector. In addition, on the basis of the Coalition Agreement a proposal for a disclosure obligation will be elaborated in the event of loss, theft or abuse of personal details for all services of the information society.
 - In 2011 the cabinet will make choices on security in relation to the processing of personal data. The European developments in the area of privacy will provide direction in this respect.

- In consultation with the ICT suppliers, the cabinet wants to look for options for improving the security of hard- and software and is also intended to make agreements on secure hard- and software at international level. In addition, the Netherlands is actively participating in the Internet Governance Forum which is facilitated by the United Nations.
 - The Dutch cabinet wants to consult with suppliers to make information on the security of ICT products and services better available for the user. The government, together with the suppliers of ICT products and services, will continue developing target-oriented national campaigns for citizens, companies and the government which are geared to current developments and vulnerabilities.
4. The Dutch government wants to invest further in the Dutch **response capability for withstanding ICT disruptions and cyber attacks**. The government will respond adequately where incidents can lead to social disruption or harming of vital objects, processes or persons. In the summer of 2011 the cabinet will publish the National ICT Crisis Plan which will include an exercise plan, which aligns both national and international exercises. An ICT Response Board (IRB) will come into operation in 2011 and will be placed as a function in the National Cyber Security Centre. Internationally the focus will be on reinforcing the cooperation in the operational response between CERT organisations in Europe and reinforcing the International Watch and Warning Network (IWWN). Furthermore a cyber education and training centre (OTC) will be founded.
 5. Regarding **intelligence services and defence**, additional measures have also been identified. The **Dutch Terrorism Combating Alerting System (ATb)** will be expanded with a cyber component and drills will be carried out. Furthermore the Ministry of Defence is developing knowledge and capacities to be able to operate effectively in the digital domain. The ultimate goal is to achieve options for the exchange of knowledge and expertise with civil and international partners. In addition, studies will be carried out on how the Ministry of Defence can make knowledge and capacities available for its third (primary) task within the ICMS (intensification of civil-military cooperation) agreements. In order to further enhance the resilience of the own networks and systems, the tasks of the Defence Computer Emergency Response Team (DefCERT) will be further expanded in the coming years. In addition, investments will be made in increasing the security awareness among the personnel and there will be accreditation of systems and processes. Finally a doctrine for cyber operations is being developed for the response to an attack to protect individual resources and units.
 6. The Dutch **government will also intensify the investigation and prosecution of cyber crime**. The **chain of investigation and prosecution will** be strengthened. In the coming years, additional capacity will be made available for the investigation and prosecution of cyber crime. Furthermore there is an increased focus on more cross-border investigations with investigation departments of countries within Europe and with other international partners. In addition, the cabinet will be focusing on further international legislation and regulations for cyber crime. At the national level a steering group will be established to tackle priority crime, and its chairman will have a seat on the Cyber Security Board. The Public Order & Safety Inspectorate will review the functioning of the police in the investigation of cyber crime.
 7. Finally **the Dutch government wants to further enhance and simulate research and education**. The **cabinet will better align research programmes** of the government and where possible of scientific research centres. A plan will be developed for the expansion of the share of ICT security in the appropriate courses. Continued effort will be put into a

study of the possibilities of certification and qualification of information security professionals. Existing budgets for research programs in the field of cyber security will be identified and will be included in an integrated research program in alignment with the Cyber Security Board.

The regulatory framework

The following current Dutch national regulations have relevance and applicability in the domain of network and information security:

eGovernment Legislation³

There is currently no overall eGovernment legislation in the Netherlands. A legal framework is however being constructed to provide for eGovernment infrastructure, products and services. The framework consists of different types of acts, some of which are more conditional:

- Legislation on public access to government information (2005);
- Legislation on Personal Data Protection (2000);
- Legislation on administrative law, in particular modification by the act on electronic administrative traffic (2004);
- Legislation on electronic signatures (2003).

Data Protection/Privacy Legislation⁴

The Personal Data Protection Act was adopted by the Dutch Parliament in July 2000 and came into force on 1 September 2001. It sets the rules for recording and using personal data and furthermore implements the EU data protection legislation. The Act is overseen and enforced by the Data Protection Authority (CBP).

eCommerce Legislation⁵

In May 2004, the Parliament passed a law on eCommerce implementing the EU eCommerce Directive (2000/31/EC). Unlike most other EU Member States, this transposition does not take the form of a horizontal eCommerce law, but rather of a series of amendments to existing laws and regulations.

eCommunications Legislation

This Act transposes in Dutch law the five directives constituting the new EU regulatory framework for electronic communications: the framework directive, the access directive, the universal services directive, the authorisation directive and the privacy directive.

Its application is overseen by the national regulatory authority OPTA. On the 1st of October of 2009, a sharpening of the Telecommunications act for spamming was realized. Furthermore legislation regarding the theft and receiving of data and Notice & Takedown will be concretised.

OPTA enforces regulations on the distribution of spam and malware. Since 2004, OPTA has issued more than 20 fines between 2,000 and 500,000 € for spam and 4 for malware (16,000 € to 800,000 €) as well as over 130 warnings. After the implementation of new conditions regarding

³ Source: <http://www.epractice.eu/en/document/288325>

⁴ Idem

⁵ <http://www.epractice.eu/en/document/288325>

spam in the Telecommunications Act, the number of complaints received from civilians strongly increased.

eSignatures Legislation

The new act ensures the transposition in Dutch law of the European Directive 1999/93/EC on a Community framework for electronic signatures and provides a firm legal basis for the deployment and use of electronic signatures in eCommerce and eGovernment.

Cybercrime legislation

In terms of cybercrime legislation, most of the current cyber-crime provisions were introduced by the Computer Crime Act of 1993. All relevant material cyber-crime provisions have been incorporated in the second book of the Dutch Criminal Code. As such, they are all classified as crimes ("misdrijven"), as opposed to transgressions ("overtredingen"), in the third book of the Criminal Code). This is important, since according to Dutch criminal law, attempts and aiding and abetting are both only punishable where crimes are concerned.

For the most part, these crimes can be described as penetration of an automated device (art. 138a Criminal Code), disrupting the processing or functioning of an automated device (art. 161sexies and 161septies Criminal Code), altering data and rendering it unusable (art. 350a and 350b Criminal Code), and interception (139c, 139d and 139e Criminal Code). Additionally, the Computer Crime Act modernized the Criminal Procedure Code, introducing e.g. network searches.

The court most likely to deal with computer crime is the general Court, criminal sector (Rechtbank, sector strafrecht). Against its decisions, appeal can be lodged with the Court of Appeal (Gerechtshof). The High Court (Hoge Raad der Nederlanden) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate⁶.

Secondary legislation

Within the Government there is a regulation regarding Information security (VIR - 'Voorschrift Informatiebeveiliging Rijksdienst'). The VIR is not a list of measures to be implemented but provides a number of key rules. It sets minimum requirements for the development of security within administrations and also regarding the requirements for measures that this policy must put practice.

The manager of the information has to make a risk assessment to show what measures are required. Based on that risk assessment, information security plans need to be made.

In addition to the VIR, there is also a regulation VIR-BI ('Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie') which addresses particular treatment of special information (e.g. regarding intelligence).

Other secondary regulation

Furthermore the telecom sector is subject to the security of electronic communication networks and services as determined in the telecommunication legislation. In the financial sector, integrity checks are performed in line with the legislation on financial supervision.⁷

⁶ See: ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

⁷ Source: <http://www.oecd.org/dataoecd/25/10/40761118.pdf>

Self-regulation

The Dutch mobile telecom operators have adopted a code of conduct⁸ that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Dutch mobile electronic telecommunications market and complies with applicable European and national legislation.

⁸ Source: http://www.gsmeurope.org/safer_mobile/national.shtml

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> • Ministry of Economic Affairs, Agriculture and Innovation (EL&I) • Ministry of the Interior and Kingdom Relations (BZK) • Ministry of Security and Justice (S&V) • Team High Tech Crime • AT (Agency for Telecoms) • CBP (Data Protection Authority) • OPTA (Independent Regulator for Post and Electronic Communications) • Logius
CERTs	<ul style="list-style-type: none"> • GOVCERT.NL - Computer Emergency Response Team of the national Government of the Netherlands • AMC-CERT - Academic Medical Centre CERT, University of Amsterdam • CERT-RU - Radboud University Nijmegen CERT • CERT-RUG - Computing Centre University of Groningen CERT • CERT-UU - Computer Emergency Response Team - Universiteit Utrecht • SURFcert - Computer Emergency Response Team of SURFnet • UvA-CERT - Computer Emergency Response Team - University of Amsterdam • ING Global CIRT - Computer Incident Response Team of ING global • KPN-CERT - Computer Emergency Response Team of KPN • RABOBANK SOC - Support Operation Centre of Rabobank • AAB GCIRT - Global Computer Incident Response Team of ABN AMRO • CERT-IDC - Computer Emergency Response Team of Energis IDC
Industry Organisations	<ul style="list-style-type: none"> • ICT-Office • CIO Platform • VNO-NCW (Confederation of Netherlands Industry and Employers) • NVB (The Netherlands Bankers Association)
Academic Organisations	<ul style="list-style-type: none"> • TNO and CPNI (Centre for the Protection of critical National Information Infrastructure) • SurfNet (A non-profit 'task organisation' forming part of SURF) • SAFE-NL (platform for Security, Applications, Formal Aspects and Environments) • Sentinels • NVSO (National Collaboration for Security Research) • Nlnet Foundation
Others	<ul style="list-style-type: none"> • PvIB (Platform for Information Security) • ECP-EPN (Electronic Commerce Platform - Platform for eNetherlands) • Nederlandse consumentenbond (Dutch Consumer Union) • NEN (Dutch Normalisation Institute) • ISSA NL • OWASP NL • ISACA NL

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁹ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory¹⁰.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID,

⁹ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

¹⁰ <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation via the responsible Ministries

The prevention, detection and prosecution of cyber security threats fall under three ministries: the Ministry of Safety and Justice (V&J), the Ministry of Economic Affairs, Agriculture and Innovation (EL&I) and the Ministry of the Interior and Kingdom relations (BZK).

V&J treats detection and prosecution of cybercrime as well as national security and crisis management, BZK is responsible for governmental cyber security, and EZ strives for a properly functioning telecommunications and ICT market with self-regulation and prevention. The ministries work closely together to tackle NIS issues with different stakeholders as further described below.

Co-operation via CPNI.nl

Along the lines of the former National Infrastructure Security Co-ordination Centre (NISCC) in the UK, the Dutch National Infrastructure against Cybercrime (NICC) was established as a temporary organization in the past. The objectives of the NICC were to bring together public and private bodies from each sector in confidential environment and to exchange best practices and experience in fighting cyber-crime. The NICC also established information exchange points for threats and actual attacks, based on information obtained from national intelligence or Computer Emergency Response Teams (CERTs). Since 2006, information exchange points have existed to address the financial sector, the electricity sector, rail transport, multinational enterprises, aviation, SCADA (Supervisory Control And Data Acquisition) systems and the provision of drinking water. From January 1st, 2011, the former Dutch Information Centre Cybercrime (NICC) got a permanent place within TNO under CPNI.nl.

Under this new form, CPNI.nl also continues the Cybercrime Information Centre (IKC) which helps to prevent potential cyber attacks on power stations and other vital infrastructure, and addressing the challenges of malicious software that can disrupt business or sensitive information capture. Initially the IKC was set up with a temporary mandate, but it is now permanently housed at TNO as part of CPNI.nl. Since January 2011, the new CPNI.nl initiative is charged with the responsibility of creating a National Infrastructure against cyber-crime – not only by developing new features, but by collaborating with others as much as possible and by integrating existing initiatives.

The programme supports, facilitates and finances initiatives by other public and private organizations that contribute to safer computer-supported work processes. It is the role of CPNI.nl to monitor the entire process, to gather and disseminate information and to encourage public and private organizations to share their knowledge.

The information exchange Centre Cybercrime is the key platform of the protection of the national information infrastructure in the Netherlands where the government and the private sector exchange sensitive information. It is based on the information exchange model of the British Centre for the protection of National Infrastructure (CPNI, previously NISCC) in which a select group of public services work closely with vital sectors regarding the risks of cybercrime and the identification of appropriate measures. The core of the organisation of this model consists of national security agency (AIVD), the police (KLPD), GOVCERT.NL and the NICC.

Around this core, several ISACs (Information Sharing and Analysis Centres) are organized for the different vital sectors. With the consent of the participants in this model, the public players can pass on essential information between the different ISACs, and to other relevant parties, in an anonymized fashion.

In the information exchange centre Cybercrime, new threats are signaled immediately. Some of its key successes include:

- The development of a hacking scenario in the energy sector from the programme National Security;
- The Notice-and-Take-Down (NTD) phishing experiment of GOVCERT.NL and the banks;
- The discussion on relevant threats from specific countries, including recommendations on the taking of specific measures;
- Collaboration on the newest modi operandi of cyber-criminals around Internet banking;
- The discussion on potential vulnerabilities of process control systems in the energy sector;
- The collaboration from the Netherlands regarding a European exchange platform, together with ENISA and CERT-Hungary;
- The development of several security benchmarks such as the SCADA security benchmark for the drinking water sector and the process control security benchmark in the energy sector.

CPNI has also taken over the CIIP activities of the former NAVI collaboration platform which connected government and business stakeholders in the protection of the critical physical and digital infrastructure. Officials involved in the critical information infrastructure in the Netherlands can contact CPNI.nl for information and independent advice about protection against malicious disruption.

CPNI.nl aims to ensure that parties working in the critical sectors in the Netherlands can share knowledge and information. For this purpose, it maintains contacts with government bodies and business enterprises operating in the critical sectors and with relevant contacts and organisations abroad. It makes knowledge and information available in various ways, such as organising meetings, communicating via its website, and providing access to its knowledge base. CPNI.nl also maintains and develops a wide network of contacts among security professionals, in order to facilitate in public-private cooperation for the security of the national critical information infrastructure.

Co-operation via the Data Protection Authority

The CBP, Data Protection Authority, is responsible for ensuring compliance with privacy and data protection legislation in the Netherlands. Specifically the body regulates fair and lawful use and security of personal data in the country in collaboration with possible public or private stakeholders. The CBP is convinced that self-regulation will contribute effectively to the achievement of the individual's fundamental right to the protection of his privacy. As such, the Authority is promoting the appointment of a data protection officer and is encouraging companies to formulate a code of conduct for their branch of industry or sector. The use of personal information should be reported to the CBP (unless there is a waiver for it). Furthermore the CBP performs several related activities such as regulation advice, awareness raising, mediation, treatment of complaints, etc.

Co-operation via the Regulator

OPTA, the independent regulator for post and electronic communications, is charged with ensuring compliance with regards to electronic communications legislation, including the enforcement of unsolicited electronic communication ("spam") and unsolicited installation of software, in close

collaboration with other national authorities, regulators and the private sector. They work closely with private sector players by providing them with information about laws and regulations, and consulting them for new regulatory developments. OPTA also offers an alerting service on their website to inform stakeholders about new posts, and they issue publications relevant to their scope of responsibility.

OPTA works with various industry organisations (e.g. Internet providers) on information security measures and compliance with legislation and regulations in the areas of post and electronic communications, including regarding electronic signatures, spam and privacy. Furthermore they collaborate with the Team High Tech Crime and Internet service providers to prevent and respond to Cybercrime.

It should be noted that due to internal reforms, the Dutch government is preparing to merge several regulating parties – including OPTA, the competition authority (NMA) and the consumer union – into a unified structure. The different regulators will continue to exist and remain under the responsibility of EL&I.

Co-operation via GOVCERT.NL

The GOVCERT.NL is the national government point of contact and centre for expertise for warning, alerting and response services on ICT attacks and intrusions in The Netherlands. They coordinate with other CERTs and relevant NIS stakeholders for the purpose of incident management and focus on three main areas: prevention, knowledge exchange and incident handling. GOVCERT.NL assists government officials in preventing security incidents and, if necessary, responding appropriately. They also offer assistance to its constituency in dealing with all sorts of incidents, ranging from spam mail to large scale network attacks on a 24/7 basis.

GOVCERT.NL is also an information centre. It provides participants access to the knowledge and experience of our staff and organizations partaking. Furthermore, they encourage the exchange of information amongst these organizations. Their data bank facilitates exchange by means of mailing lists, an archive of relevant documents and best practices. GOVCERT.NL also organizes regular meetings to give participants the opportunity to exchange knowledge and ideas on current affairs.

GOVCERT.NL keeps a close watch on incident reports by non-participating organizations. If relevant, they make sure that their participants are provided with such information immediately. Furthermore, the parties involved can communicate via them, or directly with each other.

GOVCERT.NL is also part of an extensive network of affiliated organizations, mainly other Computer Emergency Response Teams (CERTs). Since this network is a vital information hub, GOVCERT.NL makes its expertise available to other teams as it is to benefit from the knowledge of the international CERT community. The aim is to achieve maximum results with minimum means, and international collaboration is one way to realize this. That is why GOVCERT.NL encourages the development of shared standards and specialization in different areas.

A key example of the co-operation facilitated by GOVCERT.NL is via the o-IRT-o, which stands for the Dutch name 'operationeel Incident Response Team overleg' (operational Incident Response Team meeting). This forum is initiated by GOVCERT.NL in 2002. At the moment 31 organisations are participating in o-IRT-o. o-IRT-o is a group of incident handlers from the public and private sector in the Netherlands. Participants from the private sector are handlers at ISP's, banks, multi-national or industrial companies. From the public sector GOVCERT.NL is participating but also universities, employees from the national police force and the High-Tech Crime Centre. GOVCERT.NL facilitates this forum to stimulate the exchange of knowledge about various security- and incident-related topics like incidents, security-threat trends and best practices.

Also, the incident handlers in the Netherlands know each other and they can co-operate together during serious incidents. Participants of o-IRT-o have signed a non-disclosure agreement. This agreement is signed on behalf of the person, not on behalf of the organisation where the participant works for.

Co-operation via the National Continuity Forum Telecommunications (NCO-T)

The National Continuity Forum Telecommunications (NCO-T) has the objective to develop a way to implement the obligations put down on telecom operators in the Netherlands. It addresses the preparations to be made by an operator to be able to operate critical telecommunications services during a situation of Exceptional Circumstances. Participants of NCO-T are the designated operators and the Directorate-General Energy, Telecommunications and Markets of the Ministry of Economic Affairs.

The forum has a legal basis, and is organised in a plenary committee, which decides on agreements how to fulfil abovementioned preparations, and ad hoc working groups to develop the agreements. Examples of work items are: risk analysis, agreements in the field of crisis management, interdependencies with other critical infrastructures, etc. The NCO-T performs several activities focussed on the definition of a common understanding, reduction of the vulnerability of critical services, supporting facilities needed to fight a crisis, and identifying possibilities on a coordinated approach during a crisis.

Apart from the formal role of the NCO-T, the providers are given the opportunity to participate in discussions on the development and implementation of national policies in the field of critical services and/or infrastructures. Through this opportunity the government intends to prevent the development of non-optimal policies and/or regulation which could become an unnecessary burden to the market players. There is an incentive to share good practice in a forum such as the NCO-T group. However, there are no monetary incentives to do so. There are some efforts undertaken to build up a repository on good practices. Nevertheless, operators have numerous forums available to discuss these issues over coffee with each other and they do.

Co-operation via Academic Organisations

The 'platform for Security, Applications, Formal Aspects and Environments' in The Netherlands (SAFE-NL) is the main community for R&D cooperation in ICT security. SAFE-NL provides a forum for researchers and practitioners from research institutions, industry and government agencies to exchange ideas on the state of the art in security technology, current and novel application areas of this technology, and on the requirements for effective deployment of secure systems.

To this end, SAFE-NL organises informal one-day workshops on security in The Netherlands, provides a moderated public mailing list for the exchange of ideas over security, and maintains this community website to inform a larger public of its activities. The scope of SAFE-NL includes:

- Algorithms, protocols and tools for security;
- Secure system design;
- Hardware security (e.g. smart cards);
- Verification and validation methods for secure systems;
- Data models and policies for secure systems;
- Legal, social, organisational and economical aspects of security.

Furthermore there is Sentinels, a Dutch research program on security in ICT, networks and information systems. The Sentinels program aims to give a significant boost to security expertise in the Netherlands by providing and managing resources for scientific research in information security, by building a national IT-security community, and by disseminating the results into

industry and government in the Netherlands. Sentinels is financed by three Dutch organizations: the Ministry of Economic Affairs, the Netherlands Organization for Scientific Research Governing Board (NWO-AB), and the Technology Foundation STW.

Co-operation via NVSO National Collaboration for Security Research

Philips Research, TNO Information and Communication Technology, and the Centre of Telematics and Information Technology of Twente University have joined forces by initiating the NVSO (Nationaal samenwerkingsVerband Security Onderzoek - National Security Knowledge Centre) with the ambitious plan of bridging the gap between the security research and the industrial security needs in the Netherlands.

The aim of the NVSO is to develop a joint vision on security research in the Netherlands as well as to facilitate in the execution of this vision, in order to increase build-up and transfer of scientific knowledge in security on topics relevant for the Dutch Industry. Areas of relevant security that have been identified so far include: Secure Systems Engineering, Secure Information Management, Trust, Organizational Security, Security Applications and Applied Cryptology.

Co-operation via Industry Organisations

ICT-Office unites over 500 companies in the Dutch IT, Telecom, Office and Internet sectors. The most important issues on ICT-Office's agenda include innovation, the cooperation between industry and universities, the ICT labour market, global sourcing, tendering procedures, and fair market principles. Through active interest articulation and communication, the ICT-Office helps to ensure that the Dutch IT, Telecom and Office sectors retain and extend their competitive strength in a globalising world. The organisation has set up a working group on information security.

The Confederation of Dutch Industry and Employers (VNO-NCW) is the largest employers' organization in the Netherlands. It represents the common interests of Dutch business, both at home and abroad, and provides a variety of member services. The confederation runs several coordination commissions, including specific ones aimed at improving legislation, implementation and enforcement regarding Information policy, cybercrime, privacy and telecommunications. Through collaboration with the government (EZ, BZK) strategic priorities are determined for future work. Through collaboration with ECP-EPN, guidance is provided to different stakeholders.

ECP-EPN is a non-profit platform which dedicates itself to the development of the Netherlands as an Information Society by taking the opportunities the Information Society offers and to take away threats and thresholds. ECP-EPN provides a public-private collaboration platform for Internet Security ('platform Internetveiligheid') which occupies itself with topics such as combating botnets, the execution of Notice-and-takedown and awareness coordination.

The Netherlands Bankers Association (NVB) represents common interests of the banking sector and strives towards a strong, healthy and internationally competitive banking industry in the Netherlands. NVB runs and participates in several information security awareness campaigns, primarily from the perspective of safe Internet banking. They run the awareness websites 3xkloppen.nl and veiligbankieren.nl, and collaborate on Digibewust.

Co-operation via Other Organisations

Furthermore there are very active information security organisations, such as ISSA, OWASP, ISACA, etc. where stakeholders from the academic world, the public sector and the private sector come together to share knowledge and best practices regarding various NIS topics.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

In the Area of security incident management, there is a strongly developed national/governmental CERT or CSIRT in place in the Netherlands with GOVCERT.NL. They provide various services that illustrate their maturity level and breadth of services rendered to the Dutch constituency, including 24 hours help with security incidents, but also an ICT Risk alert service for various stakeholders.

24-hour help with ICT security incidents

Security incidents in ICT are becoming more frequent and the damage increases. Activities of organizations can (partially) stop, confidential or personal information might be publicly exposed unintentionally, etc.

GOVCERT.NL supports government agencies in handling incidents and limiting the damage. GOVCERT.NL coordinates the response to ICT incidents and is therefore 24 / 7 available.

Incident response depends on the situation and may include:

- Telephone intake of incidents by specialists;
- Advice on the handling of it incidents;
- Analysis of malicious software (malware) among participants, the nature and severity of infection determine;
- An assessment of the leaked information;
- Using the (inter) national network of GOVCERT.NL;
- Deployment of specialized software for logging and combating malware;
- Supporting of technical staff;
- Support of incident response management by experienced managers;
- Onsite assistance;
- Crisis communication and press information support.

ICT Risk Alert

GOVCERT.NL continuously monitors hundreds of sources on the Internet and therefore has a better understanding of current threats. Based on these activities, GOVCERT.NL issues early warnings on potential threats, such as software vulnerabilities, virus outbreaks and targeted attacks.

Participants in GOVCERT.NL get customized alerts: tailored to the ICT environment of the participant and the products that the organization uses. Participants can always be sure that they are informed about relevant threats. The warnings include - if possible - a concrete advice on how the risks can be reduced. As such, GOVCERT.nl performs continuous monitoring of vulnerabilities in IT products in use by government agencies and end users.

IT Risk Alert is also available for individual computer users. They receive warnings about vulnerabilities in common software and common viruses. Computer users can log on to this service Waarschuwingsdienst.nl.

Cyber exercises

In order to prepare the Netherlands against massive and ever better cyber attacks, it took part in international exercises against cyber terror, such as the Cyber Europe 2010 Exercise facilitated by ENISA.

Another key example was the U.S. Cyber Storm III exercise in which the following countries participated: the U.S, Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, New Zealand, Norway, Sweden, Switzerland, The Netherlands and Great Britain. These countries are all members of the International Watch and Warning Network (IWWN).

The purpose of the exercise was to evaluate the existing plans, procedures and possible measures to carry out for the safety and vital services to ensure an appropriate response to large-scale failure of ICT systems. The exercise enhanced the awareness and crisis management in organizations that play a key role in ICT disturbances. These are GOVCERT.NL, the National Police Agency High Tech Crime Team, the National Crisis Centre (NCC), National Counterterrorism Centre (NCTb) and various ministries. CERTs from other countries also participated in the exercise.

In addition, the functioning of the ICT Response Board practice (IRB) was tested. The ICT Response Board (IRB) is a public-private partnership. Participants at this moment are telecom companies, energy suppliers, banks and government bodies such as the National Police Agency, the National Coordinator for Counterterrorism and GOVCERT.NL. The IRB is still in formation.

Notice-and-Take-Down (NTD)

In the area of Notice-and-Take-Down (NTD) there is also increased collaboration in the case of security incidents are detected. Increasingly, Internet providers have subscribed to the NTD Code of Conduct. As from January 1st 2009 the NICC has passed on responsibility for the NTD project to ECP-EPN.

Private and public sector organizations work together in this platform to stimulate the information society. ECP-EPN will ensure the further development of the NTD. A workgroup of initiative leaders and other interested parties are working hard on the continued adoption of the Code of Conduct in the business world. They are intensifying their examination of the issues involved with the exchange of personal information.

The Ministry of Justice is looking closely into the legal implications of an NTD request. The NTD Code of Conduct is also receiving a great deal of interest from outside the Netherlands. The NICC gave a presentation to a delegation from the Czech Republic, Germany and the UK in June 2009 about the manner in which governmental organizations and ISPs in the Netherlands collaborated in the creation of the Code of Conduct. These countries are considering collaborating with ISPs in a similar way. They are using the Dutch Code of Conduct as good practice.

Emerging NIS risks

Critical Infrastructure

Regarding critical infrastructure, the first sectoral risk analysis in 2005 has shown that malicious disruption as a cause of failure of critical infrastructure needed more attention in the Netherlands. Measures focused on the security of the critical infrastructure had to be intensified. In this light a National Advisory Centre on Critical Infrastructure (NAVI) was created which recently was absorbed in the setup of CPNI.nl in the Netherlands (for CIIP).

NAVI's mission was to intensify and facilitate security measures in the Netherlands for critical sectors. The threats identified by the National Risk Assessment within the National Security strategy are the basic principles for increasing the insight on these threats for the critical infrastructure. Critical infrastructure and local crisis management services will focus on these threats when it concerns the interdependencies, joint exercises or the development of guidelines.

Preventing critical sectors to fail is considered important, but it is also important to be ready if one fails and to be ready if the chance to fail increases as a crisis occurs. In this order the national government finds it important that all relevant parties, from critical sectors to local crisis management services are quickly alerted for an upcoming danger. Therefore the current alerting system for counterterrorism will be extended with some of the threats identified by the National Risk Assessment.

Botnets

Another key emerging risk, botnets, was analyzed in particular for the Netherlands upon specific request of EL&I. Botnets are networks of (unnoticed) infected computers used for large-scale spamming, and increasingly for identity theft and attacks on corporate websites. The technical University of Delft (TUDelft) was commissioned to investigate the problem of botnet infections in the Netherlands and the role of ISPs in mitigating this problem. The results were published in January 2011.¹¹

Between January 2009 and summer 2010, there were probably between 450,000 and 900,000 and possibly more computers infected in the Netherlands and part of so-called botnets.

¹¹ Source: <http://www.rijksoverheid.nl/onderwerpen/cybercrime/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html>

Resilience aspects

Since January 2011, the new CPNI.nl initiative is charged with the responsibility of creating a National Infrastructure against cyber-crime – not only by developing new features, but by collaborating with others as much as possible and by integrating existing initiatives in order to create the National Infrastructure. The programme supports, facilitates and finances initiatives by other public and private organizations that contribute to safer computer-supported work processes. It is the role of CPNI.nl to monitor the entire process, to gather and disseminate information and to encourage public and private organizations to share their knowledge. CPNI is currently running 3 key projects to improve resilience:

- National Roadmap for secure process control systems (PCS);
- Capacity Advisory Electricity and Telecom / ICT (CAET);
- Vital Lessons Learned.

Currently different agencies still operate under the ministries involved in network resilience issues. The Directorate of Crisis Management, the National Co-ordination Centre (NCC), and the government computer emergency response team GOVCERT.NL, all report to the BZK. Hence, these activities support the ministry's efforts regarding public order and safety except GOVCERT.nl, their activities support network and information security.

The Directorate-General for Energy and Telecommunications must undertake the necessary regulatory steps to ensure the continuation of supply of critical energy and telecommunication services to citizens and companies. This directorate reports to EL&I, responsible for national CIP/CIIP policy for the private energy and telecommunication sectors which includes several approaches to raise awareness and cooperation with as well as the private industry, including SMEs.

The telecom regulator OPTA (Onafhankelijke Post en Telecommunicatie Autoriteit) is an autonomous administrative authority and non-departmental agency of the EZ. OPTA operates within the EU Telecommunications Regulatory Framework and has to take action when something happens regarding reliability and dependability of telecommunication as far as this falls within the scope of the Framework. Accordingly, The Netherlands have divided the full range of subjects within the scope of resilience and of network & information security between EL&I, OPTA and BZK.

Experience in The Netherlands has shown that business and government interests regarding reliability and dependability of public e-communication networks overlap. The biggest positive force for change by operators is to provide clients with dependable and reliable service in order to stay competitive. For policy and national supply reasons, the government shares this interest in achieving greater dependability and reliability of public e-communication networks.

Via the NCO-T, providers are given the opportunity to be involved in the specification of specific obligations. However, the Minister of Economic Affairs is and shall continue to have ultimate responsibility in this respect. For infrastructure operators, membership is mandatory. However, participation in meetings and activities is voluntary. Nevertheless, because its decisions are binding, it is in the best interest of operators to be active participants. NCO-T is conducting the benchmarking exercises to help operators to get a better idea about how to deal with crisis as well as continuity management. NCO-T will subsequently discuss findings and decide what actions operators must take in order to help improve dependability and reliability of public communication networks.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented in the Netherlands by two acts: (i) the Act on the Protection of Personal Data of 6 July 2000 (Wet bescherming persoonsgegevens) (the "DPA"); and (ii) the Exemption Decree DPA of 7 May 2001 (vrijstellingsbesluit Wbp, or the "Decree").

The competent national regulatory authority on this matter is the Dutch Data Protection Board (College bescherming persoonsgegevens, or the "Board").

Personal Data and Sensitive Personal Data

The DPA defines personal data to mean any information relating to an identified or identifiable natural person - therefore closely based on the standard definition of personal data.

Although the definition only applies to individuals as opposed to legal entities, data concerning legal entities can be classified as personal data. This is true if these data are of such a nature that they can (together with other data) be decisive for the manner in which a natural person may be judged or treated in society. Data about contact persons of legal entities also constitute personal data.

The Board follows the Opinion on Personal Data. In line therewith, an IP address (in principle) is considered as personal data.

Under the DPA, sensitive personal data includes both: (i) the standard types of sensitive personal data; and (ii) personal data concerning a person's criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct. Biometric information revealing racial or ethnic origin or concerning health is considered as sensitive personal data by the Board (e.g. a photo on an ID).

Sensitive personal data may not be processed unless one of the exemptions in the DPA applies. Sensitive personal data may be processed (i) if the processing is carried out with the data subject's explicit consent, (ii) if the data was explicitly made public by the data subject, (iii) if it is necessary for the determination, execution or defence of any rights in legal proceedings, (iv) if it is necessary to comply with a matter of international law, or (v) if it is necessary in view of an overriding public interest (provided certain additional conditions are met).

Information Security aspects in the local implementation of the Data Protection Directive

The data controller must comply with the general data security obligations. In meeting these obligations the data controller may also take into account the costs of implementing security obligations.

Enforcement

Prosecutions for criminal offences are brought before the Dutch criminal courts. The authority to impose administrative fines, to apply administrative enforcement, to issue an administrative order on pain of a penalty sum and to institute an investigatory audit is vested in the Board. Civil proceedings are brought before the Dutch civil courts and claims for injunctions may be brought before the court in interlocutory proceedings.

NIS awareness at the country level

As awareness centre under the EU Safer Internet Programme, Digivaardig & Digibewust raises awareness and informs Dutch citizens about using the Internet and new technologies in a safe and responsible way. The aim is to encourage as many Dutch citizens to take advantage of the opportunities offered by Internet and other ICT-applications and create awareness of the possible risks and dangers that are involved.

The Dutch Awareness Centre is part of the Digivaardig & Digibewust programme. This is a partnership of government, business and social sector organizations.

Therefore a strong network of national stakeholders supports the awareness centre by knowledge, experience and contacts. Microsoft, IBM, UPC, NVB, KPN, SIDN, NVPI and the Dutch ministry of Economic Affairs are supporting the programme financially. The centre initiates, coordinates and participates in a broad range of national activities and initiatives for different target groups, including children, parents and teachers. But also senior citizens, SME's, and the digitally unskilled are important target groups. Activities for children, parents and teachers are amongst others:

National campaigns

The Dutch Awareness Centre coordinates the Dutch celebration of Safer Internet Day every year in February and continuously cooperates with a large group of stakeholders on a variety of other campaigns – e.g. the campaign about safe use of Internet run by the Ministry of Justice¹² (www.veiliginternetten.nl), the campaign about safe use of personal data "Watch your space" (since 2008), etc.

Reaching the target groups

To reach the target groups the Dutch Awareness Centre cooperates with different organisations that are in close connections with the target groups. A broad network of experts in the domain of children and new media has formed around the Centre. These experts use information materials from the programme for their educational activities.

Youth Council: DigiRaad

The Dutch DigiRaad consists of enthusiastic young people aged 10-18 years old. This council advises the Dutch government and the Digivaardig & Digibewust programme on ways of making Internet safer for young people. The DigiRaad works in close contact with Frank Heemskerk, Secretary of State of the Ministry of Economic Affairs.

They advised him to make sure that information and training is given to pupils – and certainly to their teachers as well – on working with new media. The DigiRaad also has regular discussions with business and interest groups on important topics like anonymity and privacy. With this council youth are offered the right, the means, the space and the opportunity to participate and influence decisions about their online and real life.

Different projects and initiatives

The Dutch Awareness Centre is supporting different national projects to raise awareness about safe use of Internet and other digital media or to make youngsters aware of their digital skills - i.e. the cyber parents initiative: together with the Dutch Association Public Education (Vereniging

¹² See: www.veiliginternetten.nl

Openbaar Onderwijs) the Awareness Centre works on creating a national network of parents who will stimulate the safe use of Internet at schools.

New knowledge by research

Gathering information and initiating new knowledge is important for the Centre and its stakeholders. For example, in February 2009 the Dutch Awareness Centre launched a survey about teenagers and online privacy and in 2008 about gaming within the family. Upcoming surveys are i.e. the difference between what parents think that is safe or unsafe and what really is safe or unsafe.

Another clearly inspiring case in the Netherlands is 'Waarschuwingsdienst.nl', the Dutch National Alerting Service. Their goals are providing citizens and SMEs with warnings regarding IT security related incidents. Furthermore they also provide awareness raising materials such as cartoons, movies and papers. Warnings are provided via this public website (www.waarschuwingsdienst.nl), e-mail alert and SMS-alert services which are all free of charge. The National Alerting Service actually resides within GOVCERT.NL, the Computer Emergency Response Team for the Dutch government.

The coordinator of the Dutch Awareness Centre:

The coordinator of the Digivaardig & Digibewust programme is ECP-EPN, the platform for the Information Society. ECP-EPN acts as a coordinator of the Dutch Awareness Centre.

ECP-EPN is a non-profit platform which dedicates itself to the development of the Netherlands as an Information Society by taking the opportunities the Information Society offers and to take away threats and thresholds. It addresses the social meaning of ICT.

Consumer Union initiatives

The Dutch Consumer Union ('Consumentenbond') had performed a research that indicated that Dutch consumers had an unfounded feeling of security about doing things online. Consumers appeared not to understand sufficiently all relevant risks nor did they adequately protect their computers. Therefore the Consumer Union launched a campaign called 'Do let yourself get hacked', or in Dutch 'Laet je net hacked'¹³.

The Dutch consumer union produced a number tools to increase awareness with Dutch consumers, including a privacy quiz, online FAQs, checklists and tests, a newsletter, etc. Additionally they developed a handbook called 'Securely Online', or 'Veilig Online' in Dutch. The handbook is an interesting publication that helps consumers to educate themselves on using the Internet safely, protecting their privacy, and recognizing threats timely. The publication contains screen examples, step-by-step exercises, explanations on various threats, information about children and the Internet, Privacy-sensitivity of social networks and online banking, and the protection of wireless networks.

Joop Bautz Information Security Award

Another very interested practice regarding the creation of information security awareness in the Netherlands is the annual Joop Bautz Information Security Award for students which is organised by the PvIB. This award is given to the individual that the most promising and timely contribution has been published within the field of Information Security. The individual is a person studying at

¹³ <http://www.laatjeniethacken.nl/>

an accredited college or university or research institute in the Netherlands, a Dutch study at an accredited college or university international knowledge institute.

Winners are selected based on criteria in the following domains:

- Theory: contributions to the theory of information security. It can include fundamental developments (e.g. the development of a new class of encryption algorithms) but also application models (remember the model of the 2003 WPKI potential) or security. This focus area is interesting for thinkers / students / PhD / article writers.
- Practice: Among this research are specific practical achievements, e.g. implementation projects, or work on the front (risk management) or back (audit and supervision) of the information security process. This focus is interesting for doers: project managers, consultants, managers, administrators.
- Instrumentarium: This area relates to security products (hardware and software) and security services (in the broadest sense of the word). This area is interesting for industry and consumer of products or services, both for hardware and software suppliers as for the consultancy industry.
- Social relevance: Social relevance is in a sense, a criterion that can be applied in the previous three focus areas of theory, practice, and instrumentation. Because of its appealing character, a contribution for the entire security community, it is differentiated.

Country-specific activities for identifying and promoting economically efficient approaches to information security

The Netherlands are very supportive of research regarding the economics of cyber security. As illustration of this commitment, the Dutch government specifically supports studies in this area, particularly in collaboration with the OECD. In the past years there was specific support regarding the OECD publications on "The economics of malware"¹⁴, "the market consequences of Cybersecurity"¹⁵, etc. Additionally a study was conducted regarding "The Role of Internet Service Providers in Botnet Mitigation"¹⁶.

¹⁴ http://www.oecd-ilibrary.org/science-and-technology/economics-of-malware_241440230621

¹⁵ http://www.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software/the-market-consequences-of-cybersecurity_9789264056510-8-en

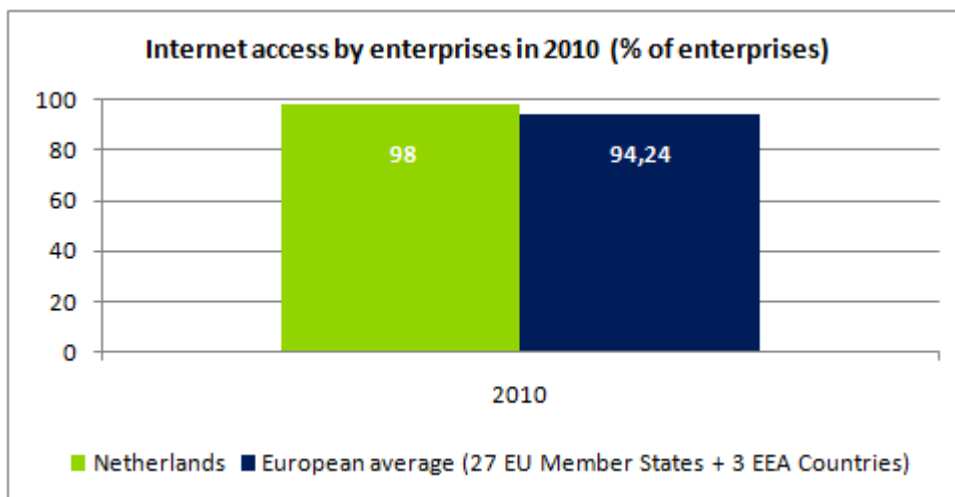
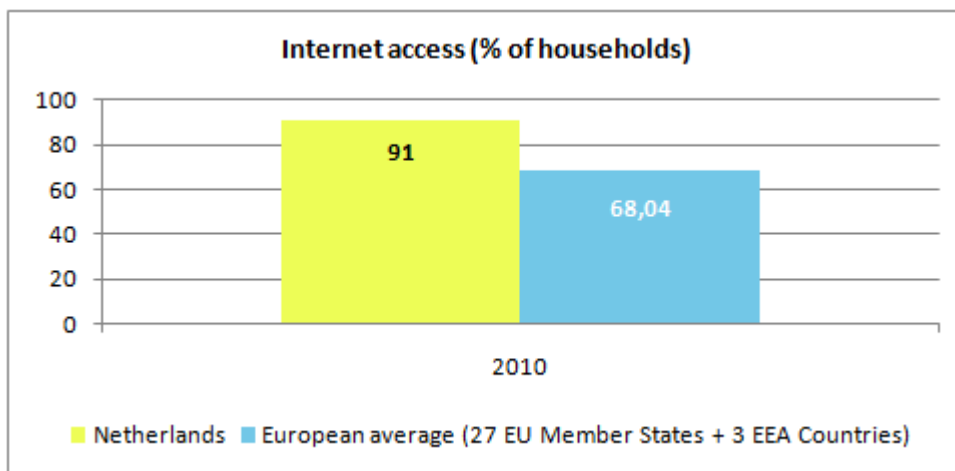
¹⁶ http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-service-providers-in-botnet-mitigation_5km4k7m9n3vj-en

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in the Netherlands, a series of relevant statistics are included in this section. These statistics mainly indicate that the Netherlands are above the European average in terms of NIS and ICT development.

Internet access of population and enterprises

The following graphs provide an overview of the situation¹⁷ of Internet access in the Netherlands for enterprises and respectively households, relative to the European average.

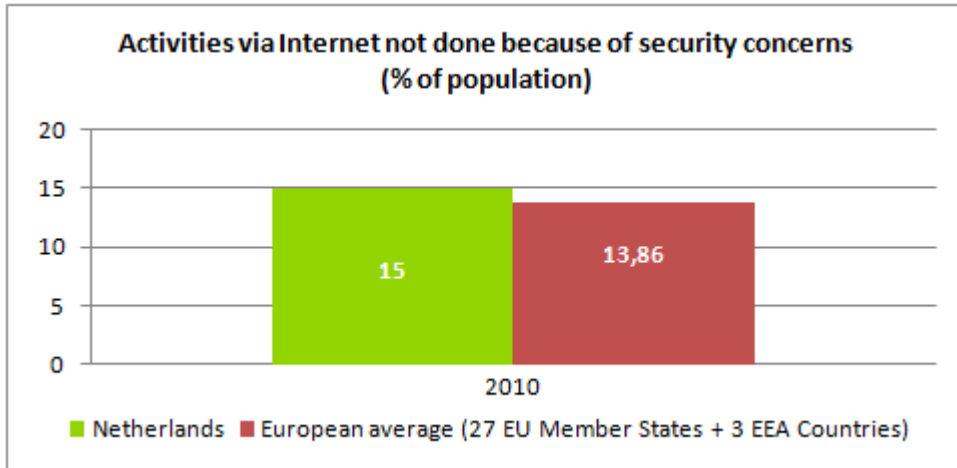


In 2010, the statistics indicate that the enterprises in the Netherlands are slightly above the European average, while households have a level of Internet access that is clearly ahead the European average.

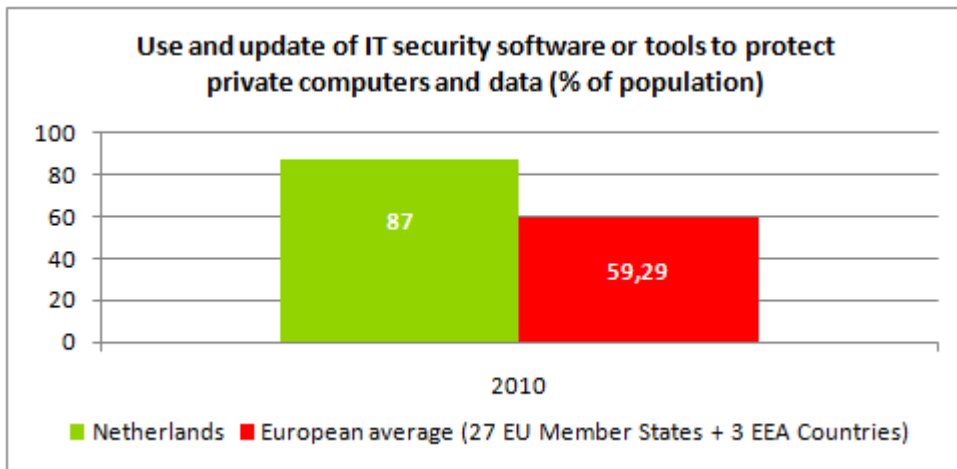
¹⁷ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in the Netherlands that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is slightly above the European average:



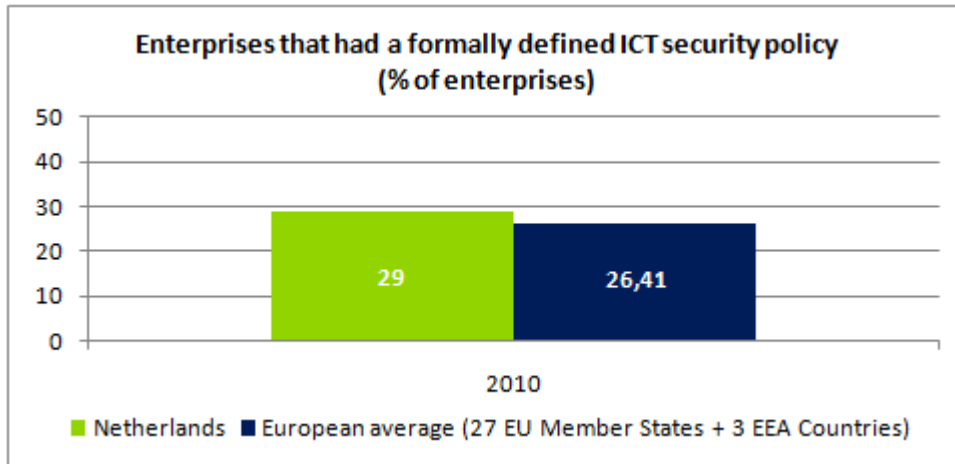
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



Also, it appears that the use of security tools to protect private computers and data is more widely spread than the European average.

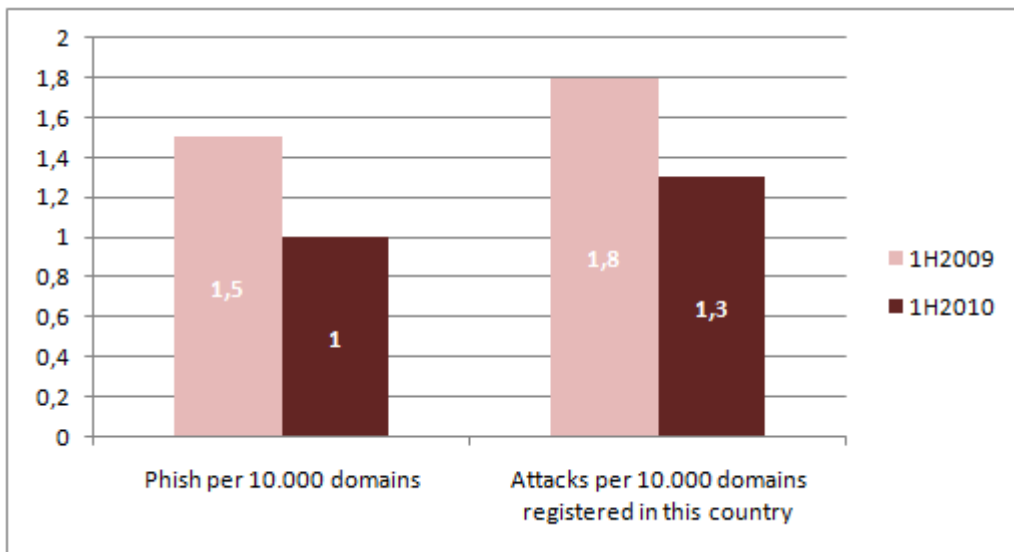
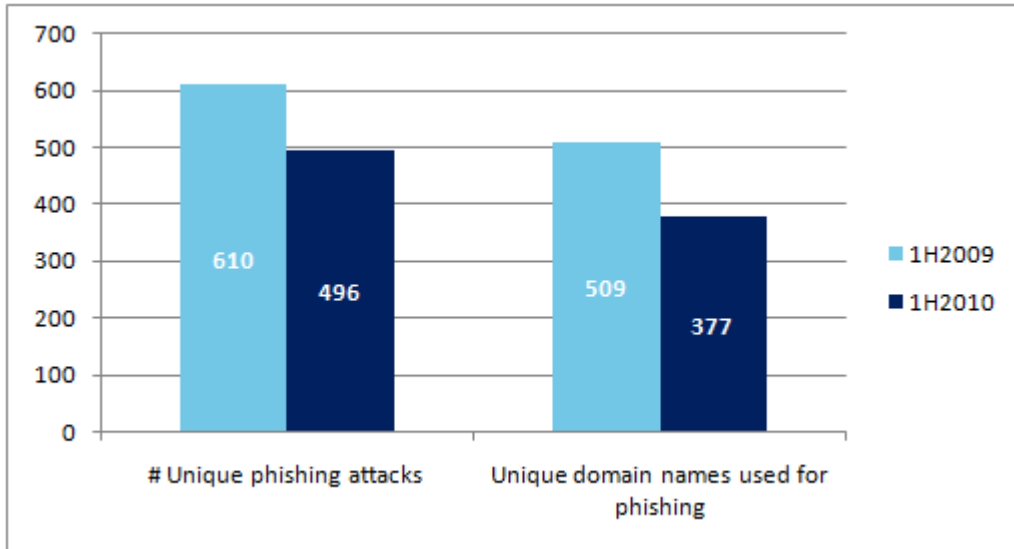
Statistics on use of Internet by enterprises and related security aspects

More enterprises in the Netherlands have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, The Netherlands was mentioned in the global report¹⁸ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁸ See: Global Phishing Survey: Trends and Domain Name Use 1H2010, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of Economic Affairs, Agriculture and Innovation (EL&I)	Ministry of Economic Affairs, Agriculture and Innovation is active regarding the development of the electronic communications market and IT, including network and information security	www.rijksoverheid.nl/ministeries/eleni
2. Ministry of the Interior and Kingdom Relations (BZK)	<p>The ministry of the Interior and Kingdom Relations (BZK) formulates policy, prepares legislation and regulations, and is also responsible for coordination, supervision and policy implementation. It has a principal role regarding steering and development of e-government within the Netherlands, including governmental information security. Furthermore the Ministry of the Interior is responsible for GovCert.nl</p> <p>The Comsec Agency (NBV) is part of the National Security Service (AIVD) of the Netherlands and advises the government, in particular on the security of sensitive information. The NBV evaluates and develops security products, and provides advice to potential users about their deployment. Furthermore the NBV applies its expertise to perform scientific research, provide policy advice, and participate in various fora regarding information security.</p>	<p>www.rijksoverheid.nl/ministeries/bzk</p> <p>www.aivd.nl/organisatie/eenheden/nationaal-bureau/nbv</p>
3. Ministry of Security and Justice (S&V)	The Ministry of Security and Justice has the principal role regarding NIS from the perspective of NIS related law enforcement and combating cybercrime. Furthermore it is responsible for general National security, including emergency crisis coordination through its national crisis centre (NCC) and terrorist threats through the counter terrorist body NCTB.	www.rijksoverheid.nl/ministeries/venj
4. Team High Tech Crime	The Dutch Team High Tech Crime is a specific unit of the Dutch police which was founded to police networks and communication systems in the Netherlands, and tackle crimes using or directed against information and communication technology	www.politie.nl/klpd
5. AT (Agency for Telecoms)	AT is a governmental organisation for technical support and advice on telecommunications policy and enforcement including the availability of the international emergency number 112. As a specialised agency of the Ministry of Economic Affairs, the three main tasks of Agency for Telecommunications are to obtain, allocate and protect frequency space.	www.agentschap-telecom.nl
6. CBP (Data Protection)	The CBP supervises the fair lawful use and security of personal data to ensure appropriate	www.cbpweb.nl

National authorities	Role and responsibilities	Website
Authority)	<p>privacy and data protection in the Netherlands. The use of personal information should be reported to the CBP (unless there is a waiver for it). Furthermore the CBP performs several related activities such as regulation advice, awareness raising, mediation, treatment of complaints, etc.</p>	
7. OPTA (Independent Regulator for Post and Electronic Communications)	<p>OPTA regulates the telecommunications and postal industries within the Netherlands, and enforces legislation. OPTA works with various industry organisations (e.g. Internet providers) on information security measures and compliance with legislation and regulations in the areas of post and electronic communications, including regarding electronic signatures, spam and privacy.</p> <p>OPTA works with the Team High Tech Crime and Internet service providers to prevent and respond to Cyber Crime.</p> <p>As part of its activities, OPTA operates the spamklacht.nl initiative to fight spam email.</p>	<p>www.opta.nl</p> <p>www.spamklacht.nl</p>
8. Logius	<p>Logius is a Dutch governmental shared service organization for ICT. It is responsible for the management and ongoing development of specific ICT services for Dutch government agencies regarding:</p> <ul style="list-style-type: none"> • Access (DigiD and PKIoverheid) • Information exchange • Information Security (GOVCERT.NL and Waarschuwingsdienst.nl) • Standardisation <p>GOVCERT.NL is the Computer Emergency Response Team of the Dutch government that supports governmental organisations regarding IT and information security regarding prevention, warning, advice, Knowledge sharing and monitoring. Furthermore they support the management of security incidents 24/7.</p> <p>Waarschuwingsdienst.nl is part of GOVCERT.nl and informs private users and small organisations about actual information security threats on the Internet via their website, email and SMS. Furthermore the website provides various materials such as trends, background information, awareness information, etc. regarding information security and cybercrime.</p>	<p>www.logius.nl</p> <p>www.govcert.nl</p> <p>www.waarschuwingsdienst.nl</p>

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST¹⁹ member • TI²⁰ listed 	
9. GOVCERT.NL	<p>GOVCERT.NL is the Computer Emergency Response Team of the national Government of the Netherlands.</p> <p>GOVCERT.NL is a central alert and information contact point on security incidents, alerts, hacks, errors, in applications and hardware.</p> <p>GOVCERT.NL informs and advises on security matters. GOVCERT.NL supports governments on prevention and handling of security incidents.</p> <p>GOVCERT.NL is</p> <ul style="list-style-type: none"> • FIRST Member • TI Listed 	www.govcert.nl
10. AMC-CERT	<p>AMC-CERT is the Academic Medical Centre CERT, University of Amsterdam.</p> <p>AMC-CERT is</p> <ul style="list-style-type: none"> • TI Listed 	www.amc.uva.nl/cert/
11. CERT-RU	<p>CERT-RU is the Radboud University Nijmegen CERT (formerly CERT-KUN).</p> <p>CERT-RU is TI Listed.</p>	http://www.ru.nl/cert
12. CERT-RUG	<p>CERT-RUG is the Computing Centre University of Groningen CERT.</p> <p>CERT-RUG is</p> <ul style="list-style-type: none"> • TI Listed 	www.rug.nl/rc/security
13. CERT-UU	<p>CERT-UU is the Computer Emergency Response Team - Universiteit Utrecht.</p> <p>CERT-UU is TI Listed.</p>	www.cs.ruu.nl/cert-uu/
14. SURFcert	<p>SURFnet CERT is the Computer Emergency Response Team of SURFnet. SURFnet is the Internet provider of the Dutch Higher Education institutes and many research organizations.</p> <p>SURFcert is</p> <ul style="list-style-type: none"> • FIRST Member • TI Listed 	http://cert.surfnet.nl
15. UvA-CERT	<p>UvA-CERT is the Computer Emergency Response Team - University of Amsterdam</p> <p>UvA-CERT- is</p> <ul style="list-style-type: none"> • TI Listed 	http://ic.uva.nl/cert
16. ING Global CIRT	<p>ING Global CIRT is the Computer Incident Response Team of ING global. ING is a global player active in the financial sector.</p> <p>ING Global CIRT is</p> <ul style="list-style-type: none"> • FIRST Member • TI Listed 	http://www.ing.com

¹⁹ <http://www.first.org/members/teams/>

²⁰ <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> FIRST¹⁹ member TI²⁰ listed 	
17. KPN-CERT	<p>KPN-CERT is the Computer Emergency Response Team of KPN. KPN is a ISP, Internet Service Provider, active in several countries around the world.</p> <p>KPN-CERT is</p> <ul style="list-style-type: none"> FIRST Member TI Listed 	www.kpn-cert.nl
18. RABOBANK SOC	<p>Rabobank Nederland SOC is the Support Operation Centre of Rabobank. Rabobank is a global player active in the financial sector.</p> <p>The Rabobank SOC is</p> <ul style="list-style-type: none"> FIRST member 	www.rabobank.nl
19. CERT IDC	<p>CERT IDC is the Computer Emergency Response Team of Energis IDC.</p> <p>CERT IDC is</p> <ul style="list-style-type: none"> TI Listed 	www.energis-idc.net
20. AAB GCIRT	<p>ABN AMRO Global CIRT is the Global Computer Incident Response Team of ABN AMRO. ABN Amro is a global player active in the financial sector.</p> <p>AAB GCIRT is</p> <ul style="list-style-type: none"> FIRST member 	www.abnamro.com/

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
21. ICT-Office	<p>ICT-Office unites over 500 companies in the Dutch IT, Telecom, Office and Internet sectors. The most important issues on ICT-Office's agenda include innovation, the cooperation between industry and universities, the ICT labour market, global sourcing, tendering procedures, and fair market principles.</p> <p>The organisation has set up a working group on information security. Through active interest articulation and communication, the ICT-Office helps to ensure that the Dutch IT, Telecom and Office sectors retain and extend their competitive strength in a globalising world.</p> <p>Recent key initiatives address cybercrime and organisational protection against cyber risks (please refer to the URLs listed on the right).</p>	<p>www.ictoffice.nl (cybercrime)</p> <p>www.ictoffice.nl/index.shtml?id=10379&ch=ICT</p> <p>www.beschermuwondernemingen.nl</p>
22. CIO Platform	<p>CIO platform is an independent organisation of CIO's and IT Directors from large public and private organisations in the Netherlands. A characteristic of its members is that they are the final responsible people for the deployment of ICT in key organisations that rely on ICT.</p> <p>CIO platform facilitates discussions among its members regarding NIS challenges, and has also</p>	<p>www.cio-platform.nl</p> <p>www.cio-platform.nl/bmtool</p>

Industry Organisations	Role and responsibilities	Website
	developed a Bmtool which allows organisations to assess the maturity of their information security measures.	
23. NVB (The Netherlands Bankers Association)	NVB represents common interests of the banking sector and strives towards a strong, healthy and internationally competitive banking industry in the Netherlands. NVB runs and participates in several information security awareness campaigns, primarily from the perspective of safe Internet banking. They run the awareness websites 3xkloppen.nl and veiligbankieren.nl, and collaborate on Digibewust.	www.nvb.nl www.3xkloppen.nl www.veiligbankieren.nl
24. VNO-NCW (Confederation of Netherlands Industry and Employers)	<p>The Confederation of Dutch Industry and Employers (VNO-NCW) is the largest employers' organization in the Netherlands. It represents the common interests of Dutch business, both at home and abroad, and provides a variety of member services.</p> <p>The confederation runs several coordination commissions, including specific ones aimed at improving legislation, implementation and enforcement regarding Information policy, cybercrime, privacy and telecommunications. Through collaboration with the government (EZ, BZK) strategic priorities are determined for future work. Through collaboration with ECP-EPN, guidance is provided to different stakeholders.</p>	www.vno-ncw.nl

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
25. TNO (Dutch Organisation for Applied scientific research) and CPNI (Centre for the Protection of National Information Infrastructure)	<p>TNO is the largest independent Dutch research organisation that works for a variety of customers: governments, the SME sector, large companies, service providers and non-governmental organisations. The conduct conduct research and foster collaboration through over 30 knowledge centres in a broad array of topics.</p> <p>CPNI was founded as part of TNO in the beginning of 2011. CPNI facilitates collaboration and provides advice which is targeted primarily at the critical national infrastructure (CNI) - those key elements of the National Information Infrastructure which are crucial to the continued delivery of essential services to The Netherlands. CNPI.nl has several projects ongoing in the area of critical information infrastructure protection, but also runs the continuation of the former ICTU program against cyber crime, NICC (National Infrastructure against Cyber Crime). The core of the NICC is the Information exchange platform (IKC) which now continues in CPNI.</p> <p>CPNI brings parties in the critical sectors together by organizing and supporting knowledge and information hubs. They manage a wide network</p>	www.tno.nl www.cpni.nl www.samentagencybercrime.nl

Academic Organisations	Role and responsibilities	Website
	<p>of contacts among security professionals, and it serves as a meeting point for critical infrastructure parties in government, research and business at home as well as abroad.</p>	
26. SURFnet	<p>SURFnet is a non-profit 'task organisation' forming part of SURF, the Dutch higher education and research partnership for ICT-driven innovation. SURFnet ensures that researchers, teachers, and students can work together simply and effectively with the aid of ICT. SURFnet therefore promotes, develops, and operates a hybrid network, a trusted identity, and a pioneering collaboration environment. SURFnet is thus the driving force behind ICT-based innovation in higher education and research in the Netherlands.</p> <p>As part of its activities, SURFnet also operates the SURFnet CERT. Additionally, Surfnet has set up an initiative called 'Cybersave yourself' where it provides various resources and knowledge on NIS to its constituency. The campaign provides an online toolkit and now focuses on phishing, social media, confidential information, backup, and mobile computing.</p>	<p>www.surfnet.nl</p>
27. SAFE-NL (platform for Security, Applications, Formal Aspects and Environments)	<p>The 'platform for Security, Applications, Formal Aspects and Environments' in The Netherlands (SAFE-NL) is the main community for R&D cooperation in ICT security. SAFE-NL provides a forum for researchers and practitioners from research institutions, industry and government agencies to exchange ideas on the state of the art in security technology, current and novel application areas of this technology, and on the requirements for effective deployment of secure systems.</p> <p>To this end, SAFE-NL organises informal one-day workshops on security in The Netherlands, provides a moderated public mailing list for the exchange of ideas over security, and maintains this community website to inform a larger public of its activities. The scope of SAFE NL includes:</p> <ul style="list-style-type: none"> • Algorithms, protocols and tools for security. • Secure system design. • Hardware security (e.g. smart cards). • Verification and validation methods for secure systems. • Data models and policies for secure systems. • Legal, social, organisational and economical aspects of security. 	<p>www.safe-nl.org</p>
28. Sentinels	<p>Sentinels is a Dutch research program on security in ICT, networks and information systems. The Sentinels program aims to give a very significant boost to security expertise in the Netherlands by providing and managing resources for scientific research in information security, by building a national IT-security community, and by disseminating the results into industry and</p>	<p>www.sentinel.nl</p>

Academic Organisations	Role and responsibilities	Website
	<p>government in the Netherlands.</p> <p>Sentinels is financed by three Dutch organizations: the Ministry of Economic Affairs, the Netherlands Organization for Scientific Research Governing Board (NWO-AB), and the Technology Foundation STW.</p>	
29. NVSO (National Collaboration for Security Research)	<p>Philips Research, TNO Information and Communication Technology, and the Centre of Telematics and Information Technology of Twente University have joined forces by initiating the NVSO (Nationaal samenwerkingsVerband Security Onderzoek - National Security Knowledge Centre) with the ambitious plan of bridging the gap between the security research and the industrial security needs in the Netherlands.</p> <p>The aim of the NVSO is to develop a joint vision on security research in the Netherlands as well as to facilitate in the execution of this vision, in order to increase build-up and transfer of scientific knowledge in security on topics relevant for the Dutch Industry. Areas of relevant security that have been identified so far include: Secure Systems Engineering, Secure Information Management, Trust, Organizational Security, Security Applications, and Applied Cryptology.</p>	www.nvso.nl
30. Nlnet Foundation	<p>The Nlnet foundation stimulates network research and development in the domain of Internet technology. It financially supports organization and people that contribute to an open information society. It funds software, events, educational activities and more, including in the areas of information security and privacy. NLnet Foundation tries to bridge the digital privacy divide by boosting confidentiality and standardisation of online communication.</p>	www.nlnet.nl

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
31. PvIB (Platform for Information Security)	<p>PvIB is a key knowledge centre in the field of information security in the Netherlands. PvIB It is the platform where information, knowledge and experience on information is collected, enhanced, enriched and then propagated.</p> <p>The PvIB unites diverse stakeholders and interested people in the field Information Security. PvIB organizes various events such as a 'Security Cafe', specific events, workshops, etc. Additionally PvIB offers various publications such as a newsletter, expert letters, a magazine, books, theses, etc. Furthermore, PvIB organises the Joop Bautz Information Security Award.</p>	www.pvib.nl
32. ECP-EPN (Electronic Commerce Platform - Platform for	<p>ECP-EPN is an Independent platform for the Information Society where the government, companies and organisations can collaborate and</p>	<p>www.ecp.nl</p> <p>www.ecp.nl/platform-</p>

Others	Role and responsibilities	Website
eNetherlands)	<p>exchange knowledge. A key NIS initiative is the public-private collaboration platform for Internet Security ('platform Internetveiligheid') which occupies itself with topics such as combating botnets, the execution of Notice-and-takedown and awareness coordination.</p> <p>ECP-EPN runs various programs, including Digivaardig & Digibewust. This program is an initiative from the government, the private sector and different organisations which aims for enabling the Dutch population to use digital solutions such as email, Internet, etc. Its objective is also creating awareness regarding security and the possible risks in the digital environment.</p> <p>ECP-EPN cooperates with Ejure, a Dutch centre of legal expertise on IT and the Information Society (www.ejure.nl).</p>	<p>internetveiligheid</p> <p>www.mijndigitalewereld.nl</p> <p>www.digivaardigdigibewust.nl</p>
33. Nederlands econsumentenbond (Dutch Consumer Union)	<p>The Dutch Consumer Union is the organisation that comes up for the interests of all Dutch consumers. They have a wide range and scope of activities, and regarding NIS they launched a number of interesting consumer initiatives. In particular, the campaign and website 'Don't get hacked', and also the Handbook 'Safely Online' are great examples of their efforts towards enhancing the security in the information society.</p>	<p>www.consumentenbond.nl</p> <p>www.laatjeniethacken.nl</p> <p>www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht-2011/handboek-veilig-online-helpt-gevaaren-te-herkennen</p>
34. NEN (Dutch Normalisation Institute)	<p>The NEN is the Dutch normalisation and standardisation institute which also represents the Netherlands in European (CEN, CENELEC and ETSI) and worldwide (ISO, IEC and ITU) standardisation efforts.</p> <p>The NEN has a specific working group on IT security that actively cooperates on international information security standards and has made a Dutch translation/version of the ISO/IEC 27001 standard for national use.</p>	<p>www.nen.nl</p>
35. ISSA NL	<p>The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. The mission of the ISSA is to enhance the knowledge and skills of its, encourage exchange of information security techniques, approaches, and problem solving, be the global voice of the information security professional, and promote best practices in information security.</p> <p>The Netherlands ISSA Chapter (ISSA NL) is an independent chapter of the Information Systems Security Association (ISSA). It facilitates, among other things, knowledge sharing events on various information security topics throughout the year in the Netherlands.</p>	<p>www.issa-nl.org</p>
36. OWASP NL	<p>The Open Web Application Security Project (OWASP) is an open-source application security</p>	<p>www.owasp.nl</p>

Others	Role and responsibilities	Website
	<p>project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions.</p> <p>The chapter in the Netherlands organizes local events such as the OWASP NL Cafe, Mini-meetings, chapter meetings and specific events.</p>	
37. ISACA NL	<p>ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems.</p> <p>The chapter in the Netherlands organizes local events such as education and training, workshops, roundtables and other specific events.</p>	www.isaca.nl

References

- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- European Commission, Europe's Digital Competitiveness Report, Volume 2: i2010 — ICT Country Profiles available at http://ec.europa.eu/information_society/eeurope/i2010/key_documents/index_en.htm#EDCR
- Netherlands - ENISA CERT Directory: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/netherlands>

