Ministry of Security and Justice

The National Cyber Security Strategy (NCSS)

Strength through cooperation

1 Introduction

The Netherlands supports safe and reliable ICT[1] and the protection of an open, free internet. Society's growing dependence on ICT makes it increasingly vulnerable to the misuse and disruption of ICT systems. For this reason, the Government has launched a National Cyber Security Strategy, with input from a wide range of public and private parties, knowledge institutions, and civil society organisations. The Strategy constitutes the Government's response to Parliamentary motions tabled by Raymond Knops and Marcial Hernandez.[2] It also embodies the integrated approach to cybercrime announced in the 2010 coalition agreement.

Structure of the Strategy

This Strategy is divided into two parts. The first part (Chapters 2 to 4) presents an analysis of the problem, describes policy principles for cyber security, and sets out objectives. The second part (Chapter 5) sets out a number of lines of action, each containing priority activities for improving cyber security – activities that will be implemented by the Government, and in collaboration with other parties.

2 Developments that call for action

ICT is essential for our society and economy.

Safe and reliable ICT is essential for our prosperity and well-being, and serves as a catalyst for further sustainable economic growth. In Europe, 50% of productivity growth is due to the use of ICT.[3] The Netherlands aims to lead the world in the use of ICT while guaranteeing the safety of 'digital society'. The Netherlands wants to become the Digital Gateway to Europe.

Society is vulnerable

ICT offers opportunities, but also increases vulnerabilities in a society where critical goods and services are increasingly interrelated. A deliberate or accidental breakdown caused by technical/human error or natural causes could lead to social disruption. The complexity of ICT systems and our growing dependence on them are leading to new vulnerabilities that could facilitate misuse and disruption. Examples include the rapid developments in mobile data transmission and cloud computing, which give way to new vulnerabilities and opportunities for misuse. The growing use of internet services involving the entry of personal details and the rise in the popularity of social media are also creating new forms of misuse, such as identity theft.

[1] 'ICT' is an umbrella term referring to digital information, information infrastructures, computers, systems, applications, plus the interaction between information technology and the physical world that is the subject of communications and information exchange.

[2] Motion tabled by Raymond Knops, House of Representatives, 2009-2010, 32 123 X, no. 66; motion tabled by Marcial Hernandez, House of Representatives, 2010-2011, 32 500 X, no. 76.

[3] European Commissioner Neelie Kroes at the opening of the 2010 World Congress on Information Technology in Amsterdam.

Recent examples

Three recent incidents illustrate these vulnerabilities and forms of misuse:
In the second half of 2010, cyber security experts identified Stuxnet, an advanced malware program that disrupts the automation of industrial processes. Analysis showed that Stuxnet must have been expensive to develop. It is suspected that the Stuxnet attack was financed by a state and aimed at the critical infrastructure of another state, leading to global side-effects on other critical organisations.
In an internationally coordinated operation in late 2010, the National Police Services Agency (KLPD) worked with partners in the Netherlands and abroad to dismantle a large botnet: a collection of computers misused remotely, often for criminal purposes and usually without the knowledge of their owners. The botnet, known as BredoLab, was masterminded from Armenia, its operations were concentrated in the Netherlands, and it was present in several other countries. Worldwide, millions of computers were taken over by BredoLab, which distributed spam and denial-of-service attacks.
The measures taken by a number of companies against Wikileaks prompted its supporters to carry out worldwide denial-of-service attacks against Paypal, Mastercard, public prosecutors, and the police. The hackers temporarily disabled these organisations' websites, demonstrating the plainness of 'hacktivism'.

Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.

Existing parties in digital society need to cooperate nationally and internationally

When cyber attacks occur, it is often difficult to identify the perpetrator, who may be a loner, an organisation, a state, or a combination of all three. The nature of the cyber threat[4] is also often unclear. But many cyber attacks involve the same techniques and methods[5] – illustrating the importance of further cooperation among parties concerned with cyber security, including public bodies working on particular types of threat, businesses that maintain the network and information infrastructure, and knowledge institutions concerned with cyber security and the public.

Digital society is global. Cyber attacks and disruptions instantaneously transcend national borders, cultures, and legal systems. It is often unclear which jurisdiction applies to data transmission, and it is often uncertain whether the law can always be effectively applied. The Government wants to make it easier to combat the misuse of ICT, wherever it occurs.

[4] cybercrime, cyber terrorism, cyber activism, cyber espionage, and cyber conflict

[5] such as malware, botnets, spam, phishing, and targeted attacks

3 Basic principles

Investing in cyber security means investing in our future, our economic growth, and our innovativeness – not only because safe ICT and the safe use of ICT are possible in the Netherlands, but also because the Netherlands is a major centre of knowledge and development in cyber security. We need to prioritise cooperation throughout the entire security system between civilian and military parties, public and private parties, and national and international parties. Only then can we ensure the resilience of our ICT infrastructure in critical sectors, a rapid and effective response to cyber attacks, and appropriate legal protection in digital domains. The following principles underlie our Strategy:

Interlinking and strengthening initiatives

A great deal is happening in the area of cyber security. But consistency is lacking in several areas. This observation is borne out by the findings of the 2010 National Report on Trends in Cybercrime and Digital Security and the National Security Think Tank's report on ICT Vulnerability and National Security. As a result, duplications will be removed and initiatives pooled. Wherever possible, the Government will build on existing initiatives and, wherever necessary, develop new ones.

Public-private partnerships

ICT infrastructure, goods, and services are largely provided by the private sector. Continuity and security of supply are essential for the sector's survival and for society as a whole, because the disruption of supply can also lead to social disruption. Mutual trust between the public and private sectors is essential if we are to work together and share information as equal partners. Every party concerned must gain value from participation in joint initiatives – an outcome that will be facilitated by an effective cooperation model with clearly defined tasks, responsibilities, powers, and guarantees.

Individual responsibility

All users (individuals, businesses, institutions, and public bodies) should take appropriate measures to secure their own ICT systems and networks and to avoid security risks to others. They should take care when storing and sharing sensitive information and respect the information and systems of other users.

Division of responsibilities between ministries

The Minister of Security and Justice is, in accordance with the National Security Strategy, responsible for coherence and cooperation on cyber security. At the same time, each party in the cyber security system has its own tasks and responsibilities.

Active international cooperation

The cross-border nature of threats makes it essential to promote international cooperation. We must aim for an international level playing field. Many measures can be effective only if they are taken or coordinated internationally. The Netherlands supports and actively contributes to efforts such as the EU's Digital Agenda for Europe and Internal Security Strategy, NATO's development of cyber defence policy as part of its new strategic vision, the Internet Governance Forum, and other partnerships. The Netherlands advocates the widespread ratification and implementation of the Council of Europe's Convention on Cybercrime.

Measures must be proportionate

There is no such thing as 100% security. When undertaking cyber security activities, the Netherlands makes choices based on risk assessment. In doing so, it aims to protect our society's core values, such as privacy, respect for others, and fundamental rights such as freedom of expression and information gathering. We still need a balance between our desire for public and national security and for protection of our fundamental rights. Measures must be proportionate. To this end, we will apply, and where necessary strengthen, safeguards and testing mechanisms, including the existing supervisory instruments.

Self-regulation if possible, legislation if necessary

The public and private sectors will achieve the ICT security they seek primarily through self-regulation. If self-regulation does not work, the Government will examine the scope for legislation. But legislation would have to meet three conditions: it should not unduly distort competition and, as far as possible, should ensure a level playing field; the administrative burden should not be disproportionately increased; and the costs should be in reasonable proportion to the benefits.

We live in a fast-moving world, and legislation can soon become obsolete. The Government will consider whether legislation needs to be tailored to developments in ICT.

4 The Strategy's goal

Security and trust in an open and free digital society

The Strategy's goal is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT. To this end, the responsible public bodies will work more effectively with other parties to ensure the safety and reliability of an open and free digital society.

This will stimulate the economy and increase prosperity and well-being. It will ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong.

5 The working plan: work in progress

To achieve the objectives of the National Cyber Security Strategy, the following lines of action have been drawn up. The Netherlands will:

- ensure an integrated approach by public and private parties;
- ensure appropriate and up-to-date threat and risk assessments;
- strengthen resilience against ICT disruptions and cyber attacks;
- strengthen our capacity to respond to ICT disruptions and cyber attacks;
- intensify the investigation of cybercrime and prosecution of its perpetrators;
- promote research and education in cyber security.

To implement each line of action, priority activities have been devised.

Work in progress

The Netherlands is doing a great deal to ensure cyber security. Below, we describe a number of priority activities, some new and some yet to be developed in full. They vary in the detail to which they have been worked out. Some are still at the blueprint stage, so that it is not yet possible to describe them in full. They are clearly still work in progress. They will be described in detail after the Strategy's publication.

5.1 Setting up the Cyber Security Council and the National Cyber Security Centre

Responsibility for digital security in the Netherlands lies with many parties. There is still insufficient cohesion between policy initiatives, public information, and operational cooperation. The Government therefore considers it essential to foster a collaborative approach between the public sector, the private sector, and knowledge institutions. The goal is to strengthen the network and ensure coordination from strategic to operational level.

- The Government considers a new network-centred form of collaboration essential to achieve an integrated and coherent approach to cyber security. It aims to set up a Cyber Security Council, where strategic-level representatives from all relevant parties will sit and iron out the content and implementation of this Strategy. In the next few months, in consultation with all the relevant parties, the Government will decide how the Council is to be formed. The Council will be facilitated by the responsible public bodies.

- The Government wants public and private parties, acting within their statutory scope, to collect information, knowledge and expertise in a National Cyber Security Centre, which will help improve understanding of developments, threats, and trends and help parties deal with incidents and make decisions in crises. The Government is inviting public and private parties to join the Centre. To this end, it is devising a partnership model.

- The Government will also expand GOVCERT.NL,[6] strengthen it, and incorporate it into the Centre.

The Government wants the Council to start work on 1 July 2011 and the Centre to come into operation on 1 January 2012.

5.2 Setting up threat and risk analyses

Strengthening security begins with understanding vulnerabilities and threats. By gathering and analysing knowledge and information from national and international public and private parties,[7] we will gain a better understanding of current and potential new threats and vulnerabilities. The National Cyber Security Centre will adopt the working methods set out in this Strategy, cataloguing risks and identifying capacities that need to be strengthened in order to prevent threats and respond to disruptions. The knowledge thus gained will make it possible to take targeted measures throughout the cyber security system, from prevention to response and from investigation to prosecution.

One of the tasks of the National Cyber Security Centre is to create a single comprehensive picture of the current ICT threats, including a report on trends in cybercrime and digital security (the first edition of which was published in 2010).

[6] GOVCERT.NL aims to strengthen information security within the Dutch public sector by monitoring sources on the internet, by issuing threat warnings and advisory opinions on ICT vulnerabilities, and by helping public authorities deal with ICT-related incidents.

[7] Including GOVCERT.NL, the AIVD (General Intelligence and Security Service) and the MIVD (Military Intelligence and Security Service), the police, special investigative services (such as the FIOD and SIOD), regulators (such as OPTA and the Netherlands Consumer Authority), government inspectorates (such as the Health Care Inspectorate), private parties (such as ISPs and security vendors), and national and international knowledge and research institutions.

The AIVD and MIVD[8] will contribute to this picture. Where necessary, they will strengthen their cyber capacity.

The Government is informed of threats to national security by the annual National Risk Assessment.[9] Cyber security will receive extra attention in this Assessment.

5.3 Increasing the resilience of critical infrastructure

We must prevent social disruption due to ICT breakdowns or cyber attacks. Various parties, from individuals to suppliers, have a responsibility in this regard. The user must be confident that an ICT good or service can be used safely. Suppliers must therefore offer safe ICT goods and services. Users must also take necessary security measures.

- In 2011, the Telecommunications Act is being amended. This will provide a legislative basis for a number of existing agreements with the largest telecommunications companies about the continuity of their critical telecommunications infrastructure. Areas covered include the reporting of disruption or breakdown of services, minimum requirements for the continuity of services, and compliance with international standards. Wherever possible, the Netherlands will work for a joint European approach in these areas.

- The Cybercrime Information Hub will continue its operations as part of the Centre for the Protection of National Infrastructure (CPNI).[10] This year, the Government will examine how the CPNI and the National Cyber Security Centre can work together.

- The responsible public bodies will work with these organisations to encourage compliance with the current minimum ICT security standards based on good practices. The Government will work with critical sectors to learn more about potential measures to prevent the disruption of their critical ICT facilities. On this basis, the responsible public bodies will urge critical sectors to take the same measures. One example is the Emergency Communications Facility (NCV), which from 1 May 2011 will replace the current emergency network. Critical organisations will be able to join the NCV.

- The Government has developed a package of measures specifically geared to preventing digital espionage. It has published a manual entitled 'Analysis of Vulnerability to Espionage' to help businesses increase their resilience to espionage.

[8] The AIVD and MIVD occupy a unique position with regard to information on cyber threats (such as digital espionage, cyber terrorism and cyber extremism) by conducting research in the interests of national security.

[9] The National Risk Assessment analyses various types of threat to national security using a uniform method for constructing middle-term scenarios with scores for probability and potential impact. It then makes proposals for strengthening capacity in order to lessen the impact of threats.

[10] The CPNI is a platform where critical sectors and public bodies can share information in a trusted environment on incidents, threats, vulnerabilities, and good practices in the areas of cybercrime and cyber security. The goal is to increase these parties' resilience to disruptions.

- Public bodies must improve their own resilience. For this reason, the Government aims to ensure that, by the end of 2011, 80% of the critical organisations in the critical sectors public administration and public order and safety have continuity plans in place. These will include scenarios of widespread disruption to ICT and the electricity supply.

- In mid-2011, the Government will draw up an information security framework for the civil service and a new regulation governing the protecting of classified information.[11] It will also institute a public-sector-wide audit cycle for information security.

- During the course of 2011, the Government will decide whether an electronic identity card that would be acceptable to the public will be incorporated into travel documents. Individuals will then be able to identify themselves reliably on the internet, entering an electronic signature that guarantees their privacy.

- Public authorities will fulfil the European obligation to report the leaking of data in the telecommunications sector. And pursuant to the coalition agreement, the Government is developing a proposal to make it compulsory for all ICT parties to report the loss, theft, or misuse of personal details.

- In 2011, the Government will make choices about security in relation to the processing of personal details. It will be guided by European developments in privacy legislation. The Government will shortly inform Parliament of its position on privacy, including the obligation to report.

- The Government wants to consult with ICT vendors to seek ways of improving the security of hardware and software. It is also committed to establishing international agreements in this area. In addition, the Netherlands will participate actively in the Internet Governance Forum, facilitated by the United Nations. The Government intends to play an active part in the global open and transparent dialogue by broaching issues that can contribute to this Strategy, such as improving the rules for internet use and combating misuse.

The Government wants to consult with suppliers to improve user information on the security of ICT goods and services.[12] The responsible public bodies will work with suppliers of ICT goods and services to develop national campaigns on current developments and vulnerabilities targeted at individuals, businesses, and public bodies themselves.[13]

[11] The AIVD's National Communications Security Agency (NBV) promotes the protection of special information by providing approved security products and ones developed in-house, by assisting in their implementation, by contributing to policy and regulations in this area, and by giving advice on information security.

[12] Four good examples: the 'Three Times Right' campaign, aimed at banks and individuals; the 'Protect Your Business' initiative, launched by the ICT trade association ICT Office to encourage SMEs to conduct a risk analysis and protect their data appropriately; the 'Cyber Safe Yourself' campaign, for colleges and universities; and the Bits of Freedom 'Webwijs' campaign.

[13] Examples include the 'Safe Internet', and 'Digi-Skilled and Digi-Aware' campaigns (by ECP-EPN). The 'Waarschuwingsdienst.nl' (GOVCERT.NL) serves the same purpose.

5.4 Capacity for responding to ICT disruptions and cyber attacks

An ICT disruption or attack needs to be met with various responses before stability can return. ICT incidents that lead to a breach in the availability, integrity, or exclusivity of the network or information infrastructure must be addressed primarily by the organisation affected. Wherever incidents could result in social disruption or damage to critical facilities, processes or persons, the responsible public bodies will respond appropriately.

- In summer 2011, the Government will launch its National ICT Crisis Plan, which includes a plan to coordinate national and international exercises.

- The ICT Response Board (IRB), a public-private partnership that gives advice on measures to counteract major ICT disruptions to decision-making organisations, will come into operation in 2011 under the auspices of the National Cyber Security Centre.

- Internationally, the Government will focus on strengthening cooperation in operational responses between the CERT organisations in Europe. It will also aim to strengthen the International Watch and Warning Network (IWWN), which now operates as an informal forum on global ICT incidents.

- A major terrorist attack on or via the internet could have a significant impact on society. The Government is therefore expanding the Counterterrorism Alert System (ATB) to include cyber threats, which will then be part of the exercise programme.

- The Ministry of Defence is developing knowledge and capacities to be able to operate effectively in the digital domain. It is doing its utmost to maximise its opportunities for sharing knowledge and expertise with civilian and international partners. At the same time, the Ministry is examining how it can make knowledge and capacities available for its third primary task under the Civil-Military Cooperation Intensification Project (ICMS).

- A cyber security education and training centre is being established.

- To make its own networks and systems more resilient, the Ministry will, in the next few years, further expand the responsibilities of the Defence Computer Emergency Response Team (DefCERT). In addition, the Ministry will invest in increasing security awareness among staff and work to achieve accreditation of systems and processes.

- A doctrine for cyber operations is being developed to protect the Ministry's own resources and units.

5.5 Intensifying the investigation of cybercrime and the prosecution of its perpetrators

The rapid growth in cybercrime calls for effective enforcement to maintain confidence in digital society. The implementing organisations in the criminal justice system (primarily the police and other investigative services plus the Public Prosecution Service and the judiciary), which share responsibility for combating cybercrime, will need to have sufficient specialists on board. Such experts can deal with complex cases involving high-tech crime as well as high-volume cases that threaten to diminish confidence in ICT among the public, small businesses, and the private sector as a whole. The goal is to increase willingness to report incidents and apprehend perpetrators. International cooperation also improves our ability to solve cross-border crime.

- The Government aims to create a pool of registered experts from the public and private sectors and knowledge institutions, so that scarce expertise can be shared and specialists can be offered challenging career prospects.

- As to enforcement, the Government aims to encourage more cross-border investigation with enforcement agencies from other European countries and international partners. The Government is also examining the scope for further international legislation on cybercrime.

- At national level, the Government will set up a steering committee on priority crime, with a view to providing the entire criminal justice system with sufficient specialists to deal with cybercrime. The chair of this committee will also be a member of the Cyber Security Council. The Public Order and Safety Inspectorate will examine the performance of the police in investigating cybercrime.

- During the next few years, within the framework of its current budget, the police will gain more investigative capacity, especially for the investigation of cybercrime and apprehension of its perpetrators. The regional police forces will have cybercrime investigators and specialists, and the National Police Services Agency will have a high-tech crime team. The high-tech crime team should be dealing with around 20 cases by 2014. The investigation and prosecution services will take part in the activities of the National Cyber Security Centre.

- In the next few years, the existing programme-based approach to cybercrime (PAC) will play a central part in creating a police knowledge centre, strengthening the police's organisational system, and shifting emphases within existing capacities. The Public Prosecution Service and the judiciary will have sufficient prosecutors, support staff, judges and examining magistrates with specialist knowledge of cybercrime.

5.6 Encouraging research and education

The quest for cyber security is driven by scientific research and the development of innovative security solutions. Proper training at all levels is essential to maintain the reliability of ICT systems and future resistance to threats. The Netherlands needs a substantial occupational group of ICT professionals if our digital economy is to grow.

- Via the National Cyber Security Council, the Government will improve coordination between research programmes in the public sector and, wherever possible, between these programmes and those in the private sector and knowledge institutions. The responsible public bodies will assist parties more actively in raising money for research from Euroregion and European funds.

- Strengthening education and training at all levels is essential if we are to resist threats and continue using ICT reliably. It is also a prerequisite for expanding the Dutch digital economy. The Government is developing a plan with educators and the professional groups concerned to increase the cyber security component in educational programmes. It will also continue to study the scope for certifying qualified ICT security professionals – which includes ensuring clarity on the content of courses. A good example has been set by the initiative of an existing group of ICT security professionals, who have set out the features of such courses.

6. Financial consequences

The above activities will be absorbed within existing budgets.

Publication
Ministry of Security and Justice
P.O.Box 20301 | 2500 EH | The Hague
The Netherlands
June 2011 | J-9228