The National Cyber Security Strategy (NCSS)

Success through cooperation

1. Introduction

The Netherlands stands for safe and reliable ICT[1] and the protection of the openness and freedom of the Internet. The increasing dependence on ICT makes society increasingly vulnerable to abuse and (large-scale) disruption. This is why the cabinet presents the National Cyber Security Strategy which has been prepared with contributions from a broad range of public and private parties, knowledge institutes and social organisations. With this Strategy the cabinet meets the Knops and Hernandez[2] motions and shapes the integral approach to cyber crime announced in the coalition agreement.

Structure of the paper
This strategy comprises two parts. The first part, Chapters 2 through 4, sets out an analysis of the problem, the basic principles of the policy area of cyber security and the goal to be achieved. The second part, Chapter 5, sets out a number of action lines and per line priority activities which this cabinet wishes to carry out itself and with other parties to improve cyber security.

2. Developments which require action

ICT is of fundamental importance for our society and economy
Safe and reliable ICT is of fundamental importance for our prosperity and well-being and forms a catalyst for (further) sustainable economic growth. In Europe 50% of the growth in productivity is due to the application of ICT[3]. The Netherlands aspires to be among the world leaders in the use and application of ICT in society and at the same time guarantee the safety of the digital society. The ambition is to grow into the *Digital Gateway to Europe*.

Society is vulnerable
ICT offers opportunities, but also increases the vulnerability of a society in which ever more vital products and services are intertwined. A deliberate or unintentional disruption as a result of technical or human failure or due to natural causes can lead to social disruption. The complexity of ICT facilities and our increasing dependence on them lead to new vulnerabilities and can facilitate disruption. Examples of this are the rapid developments of mobile data traffic and cloud-computing which entail new vulnerabilities and new possibilities of abuse. The increase in the use of Internet services whereby personal data must be used and the increase in the popularity of social media also result in new vulnerabilities and abuse, for example, in the form of identity theft.

Recent examples
Recent incidents illustrate this notion of vulnerability and abuse. For example, in the second half of 2010 advanced malware - Stuxnet – was discovered which is specifically geared to industrial process automation. Analysis showed that the development of this malware must have cost a great deal. There is suspicion that this attack was financed by a state, directed at the vital infrastructure in another state, with worldwide side effects in other (vital) organisations.
In an internationally coordinated action, at the end of 2010 the Netherlands National Police Force was involved in a joint venture with partners at home and abroad to tackle a large botnet, a collection of computers of often unsuspecting owners which can be abused remotely for, e.g., criminal activities. The botnet, called Bredolab, was controlled from Armenia, with a focal point in the Netherlands and had branches in various other countries. Worldwide, millions of computers were part of this botnet, which was used, inter alia, to send spam and carry out DDoS attacks.
The measures that a number of companies took against WikiLeaks was a reason for WikiLeaks supporters to carry out worldwide DDoS attacks against, inter alia, Paypal, Mastercard, the Public

[1] ICT is the entirety of digital information, information infrastructures, computers, systems, applications and the interaction between information technology and the physical world regarding which there is communication and information exchange.

[2] Knops motion; Second Chamber of Parliament, parliamentary year 2009-2010, 32 123 X, no. 66; Hernandez Motion ; Second Chamber of Parliament, parliamentary year 2010-2011, 32 500 X, no. 76.

[3] Euro commissioner Kroes during the opening of the WCIT conference 2010 in Amsterdam.

Prosecution Office and the police. This resulted in the websites of these organisations being temporarily unavailable and the simplicity of hacktivism became clear.

***Cyber security** is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information.*

Cooperation between existing parties in the digital society is necessary, including at an international level
In the actual event of a cyber attack it is often difficult to determine what the cause or source is. It can be an individual, an organisation, a state or a combination of these players. Often it is not immediately clear what type of cyber threat[4] is involved. In a cyber attack use is often made of the same techniques and methods[5]. All of this makes extensive cooperation between parties involved with cyber security of great importance, from government organisations which focus on separate types of threats, companies which maintain the network and information infrastructure, to knowledge institutes in the area of cyber security and citizens.

Digital society is global. Cyber attacks and disruptions cross over national borders, cultural and legal systems in the blink of an eye. It is often unclear which jurisdiction applies and it is uncertain whether applicable laws can be effectively enforced. The cabinet wants to improve the effectiveness of action against abuse in the digital world, wherever it comes from.

3. Basic principles

Investing in cyber security means to invest in our future, our economic growth and our innovation. Not only because it makes safe ICT and safe use of ICT possible in the Netherlands, but also because the Netherlands is an important player in the knowledge and development of the domain of cyber security. This requires a high priority for cyber security (civil-military, public-private, national-international, throughout the entire safety chain) which has to result in a resilient ICT infrastructure, in resilient vital sectors, fast and effective response and an adequate legal protection in the digital domain. The following basic principles apply.

Linking and reinforcing initiatives
There are many on going initiatives in the area of cyber security. However, there is a lack of coherence with regard to a number of issues. The findings in the national Trend Report on Cyber Crime and Digital Safety 2010 and the Report on ICT Vulnerability and National Security of the National Security Thinktank supports this view. That is why double activities are removed and initiatives are combined. Where possible existing initiatives form the basis for further expansion and if necessary the cabinet will develop new initiatives.

Public-Private Partnership
ICT infrastructure, products and services are for the greater part supplied by private sectors. Continuity and certainty of supply are not only important for the business world in connection with their continuity. Society itself has an interest in this, e.g. to prevent social unrest due to disruptions. Mutual trust is essential for cooperation and sharing information with each other. Government and business communities must work together as equal partners. The relevant parties must derive added value from participation in joint initiatives. A good cooperation model with clear tasks, responsibilities, powers and safeguards supports this.

Individual responsibility
All users (citizens, companies, institutions and public authorities) take suitable measures to secure their own ICT systems and networks and to prevent security risks for others. They are careful when

[4] Cyber crime, cyber terrorism, cyber activism, cyber espionage or cyber conflict

[5] Like malware, botnets, spam, phishing and targeted attacks

storing and sharing sensitive information and respect the information and the systems of other users.

Division of responsibility between departments
In line with the basic principles of the National Security Strategy, the Minister of Security and Justice is in charge of the coherence and cooperation within the field of cyber security and is accountable in this respect. Besides this, each party retains its own tasks and responsibilities.

Active international cooperation
The cross-border nature of threats makes it essential to focus on strong international cooperation. The basic principle is an international 'level playing field'. Many measures will only be effective if they are aligned or implemented at an international level. The Netherlands supports and actively contributes to the efforts of, e.g., the EU (Digital Agenda for Europe and the Internal Security Strategy), NATO (development of cyber defence policy in the framework of the new strategic concept), the Internet Governance Forum and other joint ventures. The Netherlands is a proponent of a broad ratification and implementation of the Cyber Crime Convention of the Council of Europe.

The measures to be taken must be proportionate
There is no such thing as one hundred percent security. The Netherlands makes choices in tackling cyber security activities on the basis of the weighing up of risks. A number of core values in our society play an important part. Privacy, respect for others and fundamental rights such as the freedom of expression and information gathering must be maintained. An appropriate balance must remain between, on the one hand, our desire for public and national security and, on the other, the safeguarding of our fundamental rights. Measures must be proportional. Toward this end safeguards and review mechanisms, including the existing supervision functions, are utilised and where necessary reinforced.

Self-regulation if possible, legislation and regulations if necessary
Government and businesses achieve the desired digital security first through self-regulation. If self-regulation does not work, the options of legislation and regulation are reviewed. The basic principles are that regulations may not result in an unnecessary distortion of competition and must ensure a level playing field as much as possible, that the administrative burdens are not disproportionately increased and the costs are reasonably proportional to the benefits. Developments are rapid. This can result in legislation quickly becoming obsolete. The cabinet will determine whether legislation should be adjusted to the developments in the digital domain.

4. Goal of the strategy

Security and confidence in an open and free digital society
The goal of this strategy is to reinforce the security of the digital society, in order to increase confidence in the use of ICT by citizens, the business community and government. Toward this end, the Dutch government wants to work together more effectively with other parties on the security and the reliability of an open and free digital society.

This will stimulate the economy and increase prosperity and well-being. Good legal protection in the digital domain is guaranteed and social disruption is prevented or adequate action will be taken if things were to go wrong.

5. Work plan "Work in progress"

The following action lines have been chosen to achieve the goal of this National Cyber Security Strategy:

- The Netherlands will see to an integral approach by public and private parties.
- The Netherlands will see to adequate and topical threat and risk analyses.
- The Netherlands will reinforce the resilience against ICT disruptions and cyber attacks.

- The Netherlands will reinforce the response capacity to deflect ICT disruptions and cyber attacks.
- The Netherlands will intensify investigation and prosecution of cyber crime.
- The Netherlands will stimulate research and education.

Concrete actions for the action lines are set out below.

Work in progress
A lot of activity is already going on with regard to the subject of cyber security as a whole. A number of priority new activities or activities to be enhanced are elaborated below. The degree in which these activities are elaborated differs. For a number of activities the process is still at an early stage, so that at present no broadly supported picture can be presented of the activity to be realised. We are therefore clearly dealing with work in progress. After publication of this action plan, the elaboration of these points will be continued with the relevant parties.

5.1. Setting up the Cyber Security Board and National Cyber Security Centre

The concern for digital security lies with many different parties in the Netherlands. At present there is still insufficient coherence between the entirety of good policy initiatives, information provision and operational cooperation. The cabinet therefore finds it important that there is a joint approach with the business community and knowledge and research institutions. The goal is the reinforcing of the network and taking care of the coordination from strategic to operational level.

- The cabinet believes a new network-oriented joint venture form is necessary to achieve the integral and coherent approach to cyber security. The input of the cabinet is the establishing of a Cyber Security Board on which representatives of all relevant parties have a seat at strategic level and in which agreements are made on the implementation and elaboration of this strategy. In the coming months, in consultation with all relevant parties, it will be decided how to set up the Board. The government will facilitate the Board.

- It is a wish of the cabinet 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 invites public and private parties to join this Centre. A joint venture model will be developed to enable this.

- The cabinet will expand and reinforce the current GOVCERT.NL[6] and place it within this Centre.

The cabinet's goal is for the Board to be operational on 1 July of this year and the Centre on 1 January 2012.

5.2. Preparing threat and risk analyses

The reinforcing of security starts with insight into vulnerabilities and threats. By bringing knowledge and information of (inter)national public and private organisations[7] together and analysing them, better insight is gained into topical and possible new vulnerabilities and threats. Alignment is sought with the working method of the national security strategy: i.e. charting risks and identifying capacities which have to be reinforced in order to prevent threats and to be able to respond to disruptions. With this knowledge, all target groups can take measures in the entire chain, from prevention to response and investigation and prosecution.

[6] GOVCERT.NL focuses on reinforcing information security within the Dutch government and does so by monitoring sources via internet, giving advice on ICT vulnerabilities and issuing alerts in the event of threats and by offering support to government organisations when handling ICT-related incidents.

[7] Inter alia GOVCERT.NL, AIVD and MIVD[7], police, Extraordinary Investigation Services (e.g. FIOD, SIOD), supervisory agencies (e.g. OPTA and Consumer Authority), National Inspectorates (e.g. the Public Health Inspectorate), private parties (e.g. ISPs and security vendors), national and international knowledge and research institutions.

- 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, inter alia in the form of the Trend Report Cyber Crime and Digital Security which was first published in 2010.

- AIVD and MIVD[8] (Netherlands information and security services) 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[9] of the threats to national security. Cyber security will be paid extra attention.

5.3. Increasing the resilience of vital infrastructure

Social unrest due to ICT disruptions or cyber attacks must be prevented. Various parties have a responsibility in this respect, from citizen to supplier. The user must be able to rely on an ICT product or service being safe to use. The supplier must therefore offer a sufficiently safe ICT product or service. The user must also take the necessary security measures him-/herself.

- The 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. This concerns the reporting of disruptions of fall-out of services, minimum requirements in the area of continuity of services, and the alignment with international standards. Where possible there will be alignment with a European joint approach to these topics.

- In the coming years the Cyber Crime Information Exchange will be continued under the flag of CPNI.nl[10]. This year it will be reviewed how the cooperation between CPNI.nl and the National Cyber Security Centre will be given shape.

- Together with the vital organisations, 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 believes the increasing of individual resilience to be of great significance. That is why the cabinet is working to bring about that 80% of the vital organisations in the vital sectors of Public Administration and Public Order and Security will have a continuity plan by the end of 2011, which plan will set out 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 Categorised

[8] The AIVD and MIVD have a unique information position with regard to cyber threats (such as digital espionage, cyber terrorism and cyber extremism) due to the research which is conducted in the interests of national security.

[9] The National Risk Assessment elaborates various types of threats to national security with a uniform method in scenarios for the mid-long term and gives them scores as to probability and impact. Proposals are then made for reinforcing capacities to reduce the (consequences of the) threats.

[10] The Cyber Crime Information Exchange provides a platform where vital sectors and government parties exchange information in a trusted environment on incidents, threats, vulnerabilities and good practices in the area of cyber crime and cyber security. The goal is to increase the resilience of these parties to disruptions.

Information Regulation[11]. 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. Citizens can then reliably identify themselves via the Internet and place a qualified electronic signature whereby privacy is guaranteed.

- 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 details. The European developments in the area of privacy will provide direction in this respect. The cabinet will inform the Second Chamber of Parliament in the near future regarding the position on privacy. The disclosure obligation will be included therein.

- 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 goal of this is to play an active role, in the global context of an open and transparent dialogue, of touching upon topics which can contribute to this strategy, such as improving the game rules on the Internet and combating abuse.

- The cabinet wants to consult with suppliers to make information on the security of ICT products and services better available for the user[12]. 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[13].

5.4. Response capacity for withstanding ICT disruptions and cyber attacks

In order to be able to adequately respond to various threats and to be able to return to a stable situation in the event of a disruption of attack, various response activities are necessary. The relevant organisation will in the first instance itself deal with ICT incidents which lead to a breach of the availability, integrity or exclusivity of the network and information infrastructure. 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. This plan will include a exercise plan, which aligns both national and international exercises.

- The ICT Response Board (IRB), a public-private joint venture which gives the crisis decision making organisations advice on measures to combat or counteract large-scale ICT disruptions, will come into operation in 2011 and will be placed as a function in the National Cyber Security Centre.

[11] The National Bureau for Connection Security (NBV) of the AIVD promotes the security of special information by making approved and self-developed security products available, by offering assistance during the implementation thereof, by making a contribution to policy and regulations in this area and by giving advice on information security.

[12] Good examples are the "knock 3 times" campaign of the banks, which was directed to citizens, the initiative "Protect your business" of the industry association ICT~Office to encourage SMEs to carry out a risk analysis and good information security, the campaign "Cybersafe yourself" for colleges and universities and "Webwijs" of Bits of Freedom.

[13] Examples of this are the campaigns "Safe on the Internet", "Digi-abled and Digi-aware" (by ECP-EPN). The "Waarschuwingsdienst.nl" for current threats by GOVCERT.NL also serves this goal.

- Internationally focus will be on reinforcing the cooperation in the operational response between the CERT organisations in Europe and besides that the goal is to reinforce the International Watch and Warning Network (IWWN) which currently functions as informal globally operating consultation in the event of ICT incidents.

- The social impact of a large-scale terrorist attack on or via the Internet can be substantial. The Terrorism Combating Alerting System (ATb) will therefore be expanded with a cyber component and drills will be carried out.

- The Ministry of Defence is developing knowledge and capacities to be able to operate effectively in the digital domain. The maximum 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.

- A cyber education and training centre (OTC) will be founded.

- 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.

- A doctrine for cyber operations is being developed for the response to an attack to protect individual resources and units.

5.5. Intensifying investigation and prosecution of cyber crime

The rapid development of cyber crime requires effective combating in order to maintain confidence in the digital society. Toward this end the enforcement bodies in the criminal law chain (primarily the police and other investigation services, but also the Public Prosecution Office and the judiciary) which are charged with combating cyber crime must have a sufficient number of specialists. This concerns the very specialist handling of complex cases ("high tech crime") and the handling of less complex (high volume) cases which affect the confidence that citizens, the SME sector and the rest of the business community have in ICT. The goal is for the willingness to report an offence and the chance of catching the perpetrators to increase and that perpetrators are dealt with more severely. International cooperation also enables cross-border crime to be tackled better.

- The cabinet intends to realise the establishing of an expert pool and to set up a register of experts for government, universities and the business community, so that scarcely available expertise can be shared and specialists are offered a challenging career perspective.

- With regard to law enforcement the cabinet is focusing 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. For cyber crime the goal is that in the entire criminal law chain there are sufficient specialists to adequately tackle cyber crime cases. The chairman of this steering group 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.

- Within the current budgetary framework of the police, the coming years there will be a shift to greater investigation capacity and within that context also in the direction of investigation and prosecution of cyber crime. These are Internet monitors and specialists within the regions and with the High Tech Crime Team of the National Police Force. The intention is for the High Tech Crime Team to be dealing with some 20 cases in 2014. The investigation and prosecution services will participate in the National Cyber Security Centre.

- The cyber crime programme approach will play a central role in the coming years in, inter alia: the setting up of a knowledge centre within the police, the reinforcement of the police organisation and the effective shift within the existing capacities. The Public Prosecution Office and the judiciary will have a sufficient number of specialised public prosecutors, secretaries of the public prosecution office, judges and cyber law magistrates.

5.6. Stimulating research and education

Scientific and applied research and the stimulation of the development of innovative security solutions are a driving force for cyber security. A good education at all levels is necessary to continue producing reliable ICT and to be able to continue withstanding threats. A professional vocational group is a prerequisite for the growth of the digital economy in the Netherlands.

- The cabinet will better align research programmes of the government and where possible of scientific research centres and the business community in the National Cyber Security Board. In addition the government will supervise the aforementioned parties even more actively than now when tapping into multiplying research funds of, e.g., European and Euregion funds.

- Reinforcement of education at all levels is necessary to be able to continue withstanding threats and to continue producing reliable ICT and is a prerequisite for the growth of the digital economy in the Netherlands. Together with the vocational groups and the education sector 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. This requires that the content of the courses be clear. A good example of this is the initiative of the vocational group of information security officers to make the characteristics of the various courses clear.

6. Financial consequences

The above activities will be dealt with within the existing budgets.