National Cyber Security Strategy 2

From awareness to capability

Foreword

The digital domain has been a part of Dutch society for more than two decades. During this period, information and communications technology has proven to be an important factor in productivity growth and innovative power. The Netherlands is the European leader in responding to technological trends and the effective use of ICT tools and skills. The Netherlands is also an international internet hub, has the world's most competitive internet market and has one of the highest number of internet users.

Safeguarding digital security and freedom and maintaining an open and innovative digital domain are preconditions for the proper functioning of our society. Therefore, we published the first National Cyber Security Strategy (NCSS1) in 2011. The purpose of the NCSS1 was to realise a secure, reliable and resilient digital domain through an integral cyber security approach based on public-private partnerships, as well as to seize the ensuing opportunities for society.

Developments in the digital domain, both national and international, are taking place at a rapid rate. In recent years, the potential and actual impact of cyber security threats have become clearer due to a number of highly publicised incidents. These threats may not only disrupt our digital infrastructure, but may also compromise the integrity, availability and confidentiality of the information we document, analyse and exchange in the digital domain.

In order to be able to continue to respond to these threats, the Netherlands plans to further strengthen and extend their alliances with public and private parties, both national and international. This involves not viewing cyber security as an isolated element, but rather in correlation with human rights, internet freedom, privacy, social-economic benefits and innovation. The National Cyber Security Strategy 2 (NCSS2) explains this broader government vision on cyber security and states responsibilities and concrete steps.

About 130 parties, including public and private parties, knowledge institutions and social organisations, were involved in the drafting of this new cyber security strategy.

Furthermore, extensive consultations were held with the wider ICT community. At the request of the government, the Cyber Security Board, consisting of representatives from public and private parties as well as the world of academia, gave recommendations about the course of the new strategy.

With this strategy, the Netherlands wants to continue to be the world leader in the area of cyber security. Fortunately, we do not have to start from scratch. The Netherlands already has a solid digital infrastructure and has many internet pioneers and innovative ICT entrepreneurs who are active the world over. Furthermore, the Netherlands has a proven talent in building coalitions: not only within its borders, but also in the area of international peace and security. Together, we can create a secure, free and profitable digital domain. Everyone will have to take responsibility for his or her own digital resilience and for society's digital resilience. The government is taking the lead with this new strategy and will publish annual reports about the progress made.

The Minister of Security and Justice
I.W. Opstelten

Table of contents

'We are moving from structures to coalitions in which all parties — national and international — are represented in order to achieve supported standards.'

Executive summary

For more than two decades, the digital domain[1] has been a part of Dutch society and it has made an important contribution to productivity growth and innovative power. The Netherlands has made substantial investments in the way in which it responds to technological trends and the effective use of ICT tools and skills. Partly for that reason, the Netherlands has become an international internet hub, with the world's most competitive internet market and one of the highest number of internet users. As a result of this, the digital domain has become more intertwined with our daily lives. Having a secure digital domain is a precondition to making optimal use of the opportunities offered by digitisation to society.

> ***Cyber security*** *refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred.*
>
> *Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.*

In recent years, we have gained more insight into the threats and vulnerabilities in the digital domain. According to the Cyber Security Assessment Netherlands (CSBN), the biggest threats come from other states and professional criminals. The threats from other states mostly concern the theft of confidential or competition-sensitive information (cyber espionage), while professional criminals mainly focus on digital fraud and theft of information. Due to the increased complexity of, dependence on and vulnerability of ICT-based products and services, our digital resilience to these and other cyber threats is currently still insufficient.

In addition to these threats, we are also facing other challenges in the digital domain. For instance, major international private parties have increased their influence in determining the rules in the digital domain, and the civil and military domains have become more intertwined. Furthermore, the international policy context of cyber security has become wider. Cyber security cannot be realised in isolation and therefore will have to be viewed in correlation with internet freedom, including freedom of speech and privacy, and social-economic benefits, in terms of the economic and social opportunities digitisation offers.

All these developments require us to now take the next step in the approach to cyber security, based on the following vision:

> *Working with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities for our society offered by digitisation are used to the full, threats are countered effectively and fundamental rights and values are protected.*

The table on the next page provides a rough idea of the step we will take with the NCSS2.

The correlation between security, freedom and social-economic benefits proposed in the NCSS2 is a dynamic balance that is intended to be realised in a constantly open and pragmatic dialogue between all stakeholders, both national and international. For this, we need a clear governance model. The underlying fundamental principle is that the responsibilities that apply in the physical domain should also be taken in the digital domain. In order to bring the dialogue about cyber security between the various stakeholders to a new level

1 The digital domain is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as well as information, such as data and programme codes, located in this domain where geographical limitations do not apply.

NCSS1	NCSS2
Public-private partnership	Private-public participation
Focus on structures	Focus on networks / strategic coalitions
Formulation of multi-stakeholder model	Clarifying the relationships between the various stakeholders
Capacity-building in the Netherlands	Capacity-building both in the Netherlands and abroad
General approach: deploy wide capacity for resilience-increasing measures	Risk-based approach: balance between protection of interests, threat to interests and acceptable risks in society
Formulation of fundamental principles	Presentation of (policy) vision
From ignorance to awareness	From awareness to capability[2]

of maturity, the following three management areas are of the utmost importance: (self) regulation, transparency and knowledge development. These themes have been included in this strategy in various forms.

The government will play a more active role in the digital domain. On the one hand, by increasing investments in the security of its own networks and services and, on the other hand, by bringing parties together and by taking action if the security of companies and private individuals or the latter's privacy come under threat. Where necessary, the government will establish frameworks and standards, for instance when it comes to the security requirements of vital services and processes.

Private individuals are expected to apply some form of 'cyber hygiene' (basic security measures) and to take a certain amount of personal responsibility. For their part, the government and the business community will facilitate this by improving their digital skils and by emphasising their duty of care with respect to their clients. This also includes offering secure ICT products and services. Companies and government bodies have to be accountable for their responsibility in this respect and practise transparency about which cyber security measures they take and about how they handle user data. It is the government's goal to enable citizens and businesses to digitally and safely handle their affairs with the government by 2017.

The Netherlands also plans to promote the outlined integral approach on an international, involving all parties, which is aimed the correlation between security, freedom and social-economic benefits.

The Netherlands wants to play a prominent role in the search for new coalitions for defence, diplomacy and development in which all parties involved are represented, in order to reach internationally accepted standards related to actions in the digital domain. Therefore, the Netherlands works actively towards international cooperation and will take up a clear position as cyber security mediator and hub.

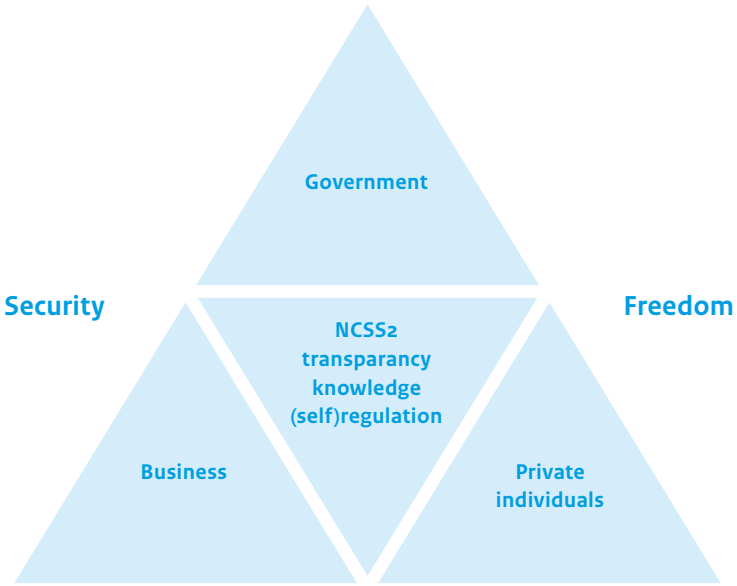
Based on the vision, the government aims to realise the following ambitions:

***The Netherlands** is a leader in cyber security:*

- *Dutch society knows how to make safe, optimal use of the advantages of digitisation.*
- *Dutch businesses and the research community are pioneers in 'security by design' and 'privacy by design'.*
- *Together with its international partners, the Netherlands is part of a progressive coalition that seeks to protect fundamental rights and values in the digital domain.*

The realisation of these ambitions will be detailed on the basis of the following strategic objectives which serve as a guideline to the 2014-206 action programme.

2 Not all parties in the Netherlands are sufficiently aware of cyber security. We will have to continue to give it our attention.



Annual progress reports will be drawn up and the action programme will be updated when necessary.

1. The Netherlands is resilient to cyber attacks and protects its vital interests in the digital domain.
2. The Netherlands tackles cyber crime.
3. The Netherlands invests in secure ICT products and services that protect privacy.
4. The Netherlands builds coalitions for freedom, security and peace in the digital domain.
5. The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.

The following themes are central elements of the objectives:

1 Risk analyses, security requirements and information sharing within critical infrastructure sectors

Within the framework of the protection of critical infrastructure, the government, working with vital parties, identifies critical ICT-dependent systems, services and processes. These efforts are linked to a programme that will establish basic security requirements on the basis of risk analyses.

2 More active approach to cyber espionage

The Dutch government is committed to raising awareness among citizens, businesses, organisation and government bodies about information security and privacy. The government also ensures that the issue is prioritised within the intelligence and security services, which will be given the tools to better document cyber threats and investigate and combat advanced attacks. To this end, the intelligence and security services have combined their cyber capabilities in the Joint Sigint Cyber Unit (JSCU).

3 Feasibility study on separate vital network

An exploratory study is conducted to determine whether it is possible and useful, from both a technical and organisational perspective, to create a separate ICT network for public and private vital processes. A separate network widens the range of options for safeguarding the continuity of vital processes. It also makes it possible to set up private, cloud-based data storage, thus strengthening the privacy and integrity of the data in storage or in the cloud concerned.

4 Enhancing civil-military cooperation

Civil and military domains within the digital domain have become more intertwined. Therefore, options for deploying the digital capabilities of the Netherlands Defence organisation on a national level in preventing and countering attacks on the civil infrastructure will be detailed. The central question is how to optimally share knowledge and expertise between civil parties and the Defence organisation.

5 Strengthening the National Cyber Security Centre

The position of the National Cyber Security Centre (NCSC) is bolstered by means of a stronger structure for confidential information-sharing and analysis. Furthermore, the NCSC assumes the role of expert authority, providing advice to private and public parties involved, both when asked and at its own initiative. Finally, based on its own detection capability and its triage role in crises, the NCSC develops into Security Operations Centre (SOC)[3] in addition to its role as a Computer Emergency Response Team (CERT).

6 International approach to cyber crime: updating and strengthening legislation (including the Criminal Code).

There is a need for effective, swift and efficient investigation of cyber crime in accordance with clear rules. Scarce capabilities have to be targetedly deployed among vulnerable sectors and groups. The Netherlands assumes a vanguard role in harmonising legislation governing international investigations, for instance in the Council of Europe. The Netherlands will also work to strengthen and expand international partnerships like EC3, at Europol.

7 Supported standards, 'security by design' and 'privacy by design'

Together with private sector partners, the government works to develop standards that can be used to protect and improve the security of ICT products and services.

8 Cyber diplomacy: hub for expertise for conflict prevention

The Netherlands aims to develop a hub for expertise on international law and cyber security. The goal of the hub for expertise is to promote the peaceful use of the digital domain. To this end, the Netherlands combines knowledge from existing centres. The centre brings together international experts and policymakers, diplomats, military personnel and NGOs.

9 Taskforce on cyber security education

To enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government join forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education).

A PPP taskforce on cyber security education is set up which will focus on giving advice about cyber security education.

10 Encouraging innovation in cyber security

There is a need for more coordination of supply and demand, which can be achieved by linking innovation initiatives to leading sector policy. In addition, the government, the business community and the world of academia will launch a cyber security innovation platform where start-ups, established companies, students and researchers can connect, inspire one another and attune research supply and demand. The PPP implementation of the second edition of the National Cyber Security Research Agenda (NCSRA) will also contribute to this development.

3 In addition to response, SOC comprises other aspects from the cyber security chain, such as awareness, resilience, detection, alerting, reporting and crisis management.

We are taking the step from being aware to being capable. Expertise development, transparency and (self-) regulation are essential means to realise this.

More products and services are being connected with each other and with the internet. How safe is this and what does it mean for our privacy?

1 The importance of cyber security

1.1 INTRODUCTION

The digital domain[4] has become more intertwined with our daily lives. Citizens, government bodies and businesses are using digital applications for online interactions, transactions, more efficient collaboration, communication and entertainment. More equipment with integrated ICT services is connected to the internet: computers and telephones, but also cars, thermostats and medical equipment. This increasing digitisation is not only for ease, efficiency and pleasure, but is also an important drive behind innovation and economic growth.

Key indicators of internet use in the Netherlands[5]

- In 2012, the Netherlands had 1.2 million internet users.
- The Netherlands has the most competitive internet market and the second highest percentage of computers per household in the world (94% of all households).
- The Dutch are pioneers in using innovative, digital services: 95% of Dutch youth use social media; the Netherlands is the front runner in online banking in Europe, and in 2012, circa 10 million Dutch people shopped online.
- The turnover of the Dutch ICT sector amounted to 29.8 billion euros in 2011, which is 5% of the GDP.
- The ICT sector in the Netherlands is the most innovative in the world. More than two-thirds of Dutch ICT businesses conducted research or other innovative activities in the period between 2008 and 2010.
- In fact, the Netherlands functions as the digital gateway to Europe. Together with Germany and the United Kingdom, the Netherlands is responsible for 18% of worldwide internet traffic, owing to the three major internet hubs in Amsterdam, Berlin and London.

The risks associated with ICT use have become increasingly clear in recent years due to a number of highly publicised incidents[6]. The advent of cloud services, mobile services and innovative, ICT-based applications nearly always usher in new vulnerabilities.

> ***Cyber security*** *refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred.*
>
> *Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.*

Increasing the Netherlands' digital resilience cannot be achieved by the government alone, as the ICT infrastructure itself and knowledge about this infrastructure is largely in the hands of national and international private parties. Therefore, cyber security is the sum of joint efforts of government bodies, the business community, organisations and citizens, both on a national and international level. Just like in the physical world, 100% security in the digital domain can never be achieved.

4 The digital domain is the conglomerate of ICT tools and services and comprises all entities that can be or are digitally linked. The domain comprises both permanent, temporary or local connections, as well as information, such as data and programme codes, located in this domain where geographical limitations do not apply.

5 ICT Knowledge and Economy 2012, Statistics Netherlands.

6 For instance: the DigiNotar incident, a hacked municipal waste water system and the Pobelka botnet.

Relation of the NCSS2 to strategic policy documents:
The NCSS2 follows on from the insights and recommendations arising from the following strategic policy documents:

- The National Security Strategy (NV Strategy) is aimed at preventing the compromise of vital national interests that may lead to social disruption.[7] Both in 2010 (cyber conflict) and in 2012 (cyber espionage), cyber security scenarios were included in the NV Strategy.

- The International Security Strategy[8]is aimed at actions taken by the Netherlands abroad and in cooperation with other countries to secure its interests. Cyber security is an important theme in this strategy, which is best acted on in collaboration with our European and international partners.

- The Defence Cyber Strategy[9] is aimed at the role of the Netherlands armed forces in the digital domain. An important element in this strategy is that it acknowledges that military and civil, public and private, national and international actors have become more intertwined.

- In its Digital Agenda[10], the Dutch government focuses on ICT being able to contribute to the country's economic growth. In the Digital Agenda, the government formulates its ambitions for using ICT to further growth and prosperity, including the required preconditions, for having an open, reliable and swift infrastructure and for having sufficient ICT knowledge and making sufficient use of such expertise.

- The information security awareness strategy[11] for government administrators and managers. With the Taskforce on Management, Information Security and Services, the government pursues an active awareness policy to get the government's information security at the desired level. This is not only an important precondition for the implementation of the government's plans concerning the concept of the digital government 2017, but also in view of the Government-Wide Implementation Agenda for eGovernment Services until 2015 (i-NUP), in which a basic infrastructure will be realised.

- The ePrivacy Letter[12] describes preconditions for a sound protection of personal details privacy, in particular in the relationships between citizens and businesses.

- The EU Cyber Security Strategy[13], which was launched in 2013 is an important step towards a secure digital environment in Europe. The Dutch NCSS2 is in line with the fundamental principles of the EU Cyber Security Strategy, based on which the Netherlands is taking new steps.

- In the autumn of 2013, a medium-term vision on the telecommunications market was presented to the House of Representatives. The starting point of the vision is that the telecommunications market cannot be viewed as being separate from developments on the internet and that public values such as reliability and openness have to be reviewed by the telecommunications market in light of the broader context of internet economics.

7 The five vital interests are: territorial security, physical security, economic security, ecological security, and social and political stability.

8 International Security Strategy, 21 June 2013

9 Defense Cyber Strategy, House of Representatives 2011 – 2013, 33 321, no. 1

10 Letter to Parliament 'Digital Agenda.nl', House of Representatives 2010 – 2011, 29 515, no. 331

11 Vision letter on the digital government, House of Representatives 2012 – 2013, 26 643, no. 280

12 Government view on e-privacy: on the road to justified trust. 24 May 2013

13 The EU Cyber Security Strategy 'Protection of an open and free internet and opportunities in the digital world' (February 2013) and associated draft directives: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (February 2013).

1.2 THREATS

In July 2013, the third Cyber Security Assessment Netherlands (CSBN) was published. The findings from this edition of the CSBN[14] are an important source for a risk-approach[15] to cyber security. The CSBN shows that the biggest threats come from other states and professional criminals.

States form a threat particularly in the form of theft of confidential or competition-sensitive information (digital espionage) of businesses, government bodies and citizens. Several states have made substantial investments in cyber capabilities and therefore have highly advanced equipment at their disposal. These states' digital espionage activities are likely to be widespread, and many of these activities are currently undetected.

Professional criminals also continue to pose a substantial threat. Digital fraud and theft of information are the two most common crimes among professional criminals. Citizens, businesses and governments alike regularly fall victim to botnets and ransomware. Furthermore, a criminal cyber services sector, through which 'cyber-crime-as-a-service' is made commercially available, has expressly become visible. Access to such remedies has become cheaper and more low threshold for criminals.

Despite the fact that good initiatives and measures have been taken to increase resilience to and awareness of such crimes, also based on the NCSS, society's vulnerability is still on the increase. At many organisations, digital resilience is still below par. Relatively simple yet important technical basic measures, like the timely updating of systems or password policies, are often not implemented. Furthermore, many organisations are struggling with legacy systems. Replacing these outdated systems, on which often a vital part of an organisation's information provision facilities depend, is a complex and expensive problem.

1.3 CHALLENGES

Future developments in cyber security are hard to predict. However, a clear picture can be painted of the challenges which currently and in the long-term influence the security and openness of the digital domain:

- *The Internet of Things (everything is connected to the internet) and hyperconnectivity (everything is connected to each other)* promotes innovation and results in usability. At the same time, it raises the question of whether or not digitally linked products and services are actually safe and what the implications may be for privacy.
- *The amount of data available in digital form is only increasing;* as will the interest in acquiring such data. Governments and businesses, increasingly working with large data files, which are also increasingly stored in the cloud, are faced with increased risks.
- *The playing field in the digital domain is not only determined by states, but also by major private market parties.* Governance in the digital domain is therefore complex and cannot always be solved in traditional forums, as it requires a multi-stakeholder approach. This applies to security standards as well as to the protection of fundamental rights and values.
- *In the cyber domain, we see an increasingly interwovenness of civil and military domains due to substantial mutual dependence on similar ICT systems and application and the complex attribution issue.* When it comes to the Dutch contingent deployed abroad, we have to take into consideration that civil targets in the Netherlands may be subject to cyber attacks. Furthermore, in case of large-scale attacks, the Defence organisation's cyber capabilities may be called upon to protect the vital national civil infrastructure. In view of the above, clear parameters for strengthened cooperation in the digital domain are needed.
- *The increased complexity and dependence on ICT-based products and services require a higher level of expertise.* This both concerns the level of expertise of average internet users and sufficiently-qualified experts. The Netherlands is expected to have a shortage of 6,800 IT workers in 2017.[16]

14 The NCSC publishes the CSBN each year and is produced in close cooperation with public and private parties.

15 The risks desribed are determined based on three correlated factors: interests, threats and resilience.

16 Based on estimations of Nederland ICT.

Cyber security cannot be achieved in isolation and will have to be approached in correlation with subjects like fundamental rights, values and social-economic benefits.

2 Vision

***Working** with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities for our society offered by digitisation are used to the full, threats are countered effectively and fundamental rights and values are protected.*

2.1 INTRODUCTION: TO A NEW APPROACH AND WORKING METHOD

In 2011, we published the first National Cyber Security Strategy (NCSS1). A lot has happened since then. The partners within the National Cyber Security Centre have succeeded in gaining a better insight into threats. The third Cyber Security Assessment Netherlands has made a more focused approach possible. Furthermore, the international implementation has gained importance. Agreements about cooperation, standards of conduct and standards will have to be made in a European, and wider international, context. The international policy context has also become wider. Cyber security cannot be achieved in isolation and will have to be approached in correlation with subjects like fundamental rights, values and social-economic benefits. All these developments require us to now take the next step in the approach to cyber security,

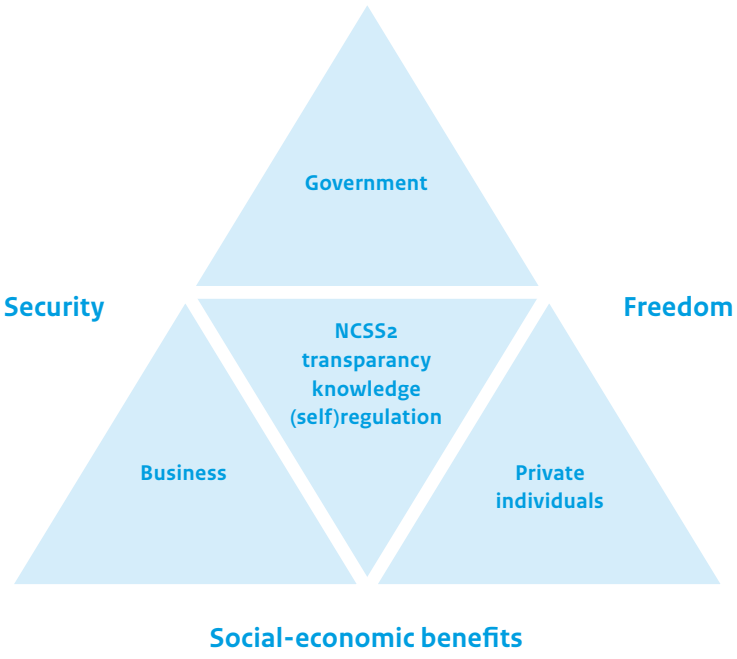
The table below provides a rough idea of the step we will take with the NCSS2.

2.2 SECURITY, FREEDOM AND SOCIAL-ECONOMIC BENEFITS

Cyber security measures require a tailor-made approach. This is shaped in three ways. Firstly, by tailoring measures to the problem they are intended to solve (risk-based), secondly, by always viewing cyber security in correlation with social-economic benefits, more specifically the economic and social opportunities digitisation offers and thirdly, by guaranteeing fundamental rights and values. This correlation between security, freedom and social-economic benefits is a dynamic balance that is intended to be realised in a constantly open and pragmatic dialogue between all stakeholders, both national and international.

NCSS1	NCSS2
Public-private partnership	Private-public participation
Focus on structures	Focus on networks / strategic coalitions
Formulation of multi-stakeholder model	Clarifying the relationships between the various stakeholders
Capacity-building in the Netherlands	Capacity-building both in the Netherlands and abroad
General approach: deploy wide capacity for resilience-increasing measures	Risk-based approach: balance between protection of interests, threat to interests and acceptable risks in society
Formulation of fundamental principles	Presentation of (policy) vision
From ignorance to awareness	From awareness to capability[17]

17 Not all parties in the Netherlands are sufficiently aware of cyber security. We will have to continue to give it our attention.



2.2.1. SECURITY

Cyber security concerns ICT security and the security of information stored in ICT systems. Disruptions to ICT-based services and processes may have major social consequences, and a disruption to vital services and processes may even lead to social unrest. Protecting personal information, state secrets and other sensitive information is vital for ensuring the trust parties have in the digital domain.

Processing personal information and the protection of privacy is subject to strict standards and supervision, partly based on European legislation. Recent revelations about secret activities of states aimed at acquiring information underline the importance of raising awareness about information security among all stakeholders, as well as the necessity to increase our critical infastructures resilience to such activities.

A wide approach by the entire ICT security chain is required to reach the desired level of security[18]. It starts with having insight into the threats and a sound preventative approach, but it also requires parties to adopt an effective response strategy. This also means that criminals in the digital domain will have to be successfully stopped. There is a need for clarification regarding the role of the police service as well as for updated options and powers to realise an effective investigation and prosecution.

2.2.2 FREEDOM

Protecting fundamental rights and values requires many parties to make an effort and preferably takes place in a national and international context. The proposed approach entails the development of international standards. In addition to governments, an important role can be played by private sector parties and social organisations. The Netherlands is promoting this approach internationally, at the United Nations, during international cyberspace conferences, like the ones held in London, Budapest and Seoul, in other multi-stakeholder settings like the Internet Governance Forum, by promoting the principles of cyber security as published by the World Economic Forum, and in developing trust-inspiring measures between states, like the Organisation for Security and Cooperation in Europe (OSCE).

A good example of the multi-stakeholder approach is the Freedom Online Coalition which was initiated by the Netherlands and of which 21 countries have become a member and who jointly form a powerful lobby. The Netherlands aims to promote the growth of this coalition. We now have to take it a step further and have the starting points we developed become an integral part of meetings about cyber security standards, and incorporate them into the design of new and innovative products and services.

18 The security chain comprises: pro-action, prevention, preparing, repression and after-care (repair).

2.2.3 SOCIAL-ECONOMIC BENEFITS

The innovative power of farther-reaching digitisation is an important stimulus for social-economic benefits. Social-economic benefits both concerns economic growth and the options digitisation offers society, for instance in the form of education applications, options for maintaining social contacts, but also improved government facilities. The government's goal of enabling citizens and businesses to digitally handle their affairs with the government by 2017 will make an extra impact in the realisation of iGovernment.[19] This will only enhance the social importance of iGovernment. Security and cyber security measures are therefore vital and require making some necessary investments.

Organisations have increasingly realised that by investing in cyber security, they can prevent major costs and a damaged reputation. This strategy is aimed at encouraging Dutch companies viewing cyber security as a competitive advantage.

Critical consumers have started to attach more and more importance to security and privacy, which is an opportunity for Dutch companies to invest in innovative products and services that take these things into account in the design stages. The government intends to play a stimulating role in this development by means of including cyber security requirements in its purchase conditions.

2.3 CLEAR ROLES, ACTIVE PARTICIPANTS

The digital domain comprises an abundance of parties and actors who have become increasingly connected to each other and dependent on each other. In order to be able to act safely in the digital domain, which is characterised by a great (chain) dependence between the parties, it is important for citizens, organisations and government bodies to actively participate ('do democracy'[20]), based on a clear allocation of roles and a great degree of transparency. The underlying fundamental principle is that the responsibilities that apply in the physical domain should also be taken in the digital domain. How these roles relate to one another will become clear in the future. The direction in which the actors are moving is explained here.

2.3.1 THE INTERVENING GOVERNMENT: FACILITATE, PROTECT AND CONTROL

Security is one of the government's core tasks, and this also applies to the digital domain. Countering cyber crime and cyber espionage and the prevention of social disruption caused by cyber incidents therefore are important priorities for the government. The starting points are a risk-based approach, strengthened cooperation and setting the right example by investing in the security of its own networks and services.

In addition, the government is responsible for the online security and privacy and citizens. The protection of valuable and personal information of citizens and businesses and tackling cyber crime therefore remain the focal points. In May 2013, the government's vision on e-privacy was published. The aim is to enable citizens to better control their personal information through the inclusion of the requirement of consent. Organisations are obliged to carefully, transparently and legally handle any information issued by citizens, and citizens should be able to call organisation to account.

Finally, the government has a duty to promote and facilitate initiatives aimed at increasing cyber security.

If required, the government also acts in a controlling manner, which may include determining regulations and standards, for instance for the vital sectors. In consultation with the vital sectors, the government is establishing cyber security requirements where this has not been already done. Existing sectoral regulatory authorities will have to widen their scope, if they have not already done so, to also include cyber security, in which overlap should be prevented.

As an expert authority, the NCSC gives advice, both when asked and at its own initiative, when major vulnerabilities are detected or in the event of (imminent) crisis situations. It is then up to the organisations themselves to implement the recommendations, or to be transparent about their reasons for not doing so. This is particularly important when it concerns government bodies, also with respect to the regulatory authorities and/or line ministries.

19 Vision letter on the digital government 2017, 23 May 2013, reference number 2013-0000306907

20 Government standpoint on the promotion of a vital society, the 'do democracy', Parliamentary Papers II, 2012-2013, 33400-VII no. 79

2.3.2 THE COMPETENT CITIZEN: CYBER HYGIENE AND PERSONAL RESPONSIBILITY

Citizens are expected to apply some form of basic 'cyber hygiene' and skills in using ICT, like surfing the web. This includes carefully using personal information, installing updates, using good passwords and balancing functionality and cyber security. The government works to increase the digital resilience of government, citizens and the business world. It aims to achieve this by means of awareness campaigns, strengthening digital skills, research and innovation and supporting social organisations and initiatives in the context of the 'do democracy'. A policy that supports responsible disclosure and removes obstacles also fits in with this context. This also enables conscious and involved citizens to safely inform government bodies, businesses and institutions about detected vulnerabilities in their ICT security.

2.3.3 RESPONSIBLE BUSINESSES: DUTY OF CARE AND ACCOUNTABILITY

Citizens can no longer be expected to completely understand and assess the security and privacy aspects of ever more complex ICT services and -products, as offered by major international players. This clearly leaves room for ICT suppliers and producers. Security by design and privacy by design should more than currently be standard design principles.

Providers of ICT networks and services or other ICT-based services have a specific responsibility (duty of care) with respect to their clients. The substantiation of this responsibility must preferably be achieved by means of self-regulation. An example is the fight against botnets, in which Internet Service Providers (ISPs) play a vital role.

The dependencies in the digital domain are also expressed in the chain of producers, providers and clients. These mutual dependencies will have to be discussed by the chain partners in order to conclude joint agreements about minimum requirements, interoperability and reliable information-sharing. This also makes it possible to strengthen the security of the entire chain. Insurance companies can play a major role in insuring residual risks.

2.3.4 (SELF) REGULATION, TRANSPARENCY AND KNOWLEDGE DEVELOPMENT AS CONTROL MECHANISMS

The Netherlands is working to realise an active participation of citizens, businesses and government in the digital domain in the context of an ever increasing mutual dependence between these actors and a complex environment in which a balance between security, freedom and social-economic benefits is constantly pursued.

This means that steps have to be taken from unaware via aware to capable. In order to make this movement towards a new level of cyber security maturity possible, the following three management areas are of the utmost importance: (self) regulation, transparency and knowledge development. These themes have been included in this strategy in various forms. (Self) regulation concerns the development of standards but also concepts like the duty of care. Transparency is a precondition for strenghtening trust between the actors. Examples of transparency are clear reports about measures taken by the government and the business world to improve cyber security and privacy measures. Knowledge development in the broadest sense of the word (awareness, education, innovation) is necessary to ensure that all actors can take their responsibility and optimally benefit from the opportunities offered by digitisation.

2.4 INTERNATIONAL VISION AND USE: AN INTEGRATED APPROACH

As an open economy, the Netherlands benefits from a stable and freely accessible digital domain. In view of the fact that cyber security and international cooperation are inextricably linked, the Netherlands will promote its integral public-private cyber security approach outside its own borders. The approach developed in which defence, diplomacy and development come together in international missions to increase stability in the area concerned (crisis management and nation building) is the inspiration for the integral Dutch use of the digital domain[21].

The Netherlands wants to play a prominent role in the search for new coalitions in which all parties involved are represented in order to reach internationally accepted standards related to actions in the digital domain. To this end, the Netherlands works actively towards international cooperation and takes up a clear position as cyber security mediator and hub.

2.4.1 DEFENCE

Defence in the digital domain not only concerns military capabilities, but also the wide civil range of capabilities

21 This is also called the 3D approach.

of intelligence and security services, the police service, national cyber security centres and businesses with their own response capabilities. This is a complex whole in which good agreements and coordination are preconditions, both national and international. Strengthened civil-military cooperation is therefore necessary.

In order to safeguard the deployability of the Netherlands armed forces and to increase the effectiveness of the armed forces, the Defence organisation is increasing its digital resilience and is developing its own capabilities to conduct cyber operations within the applicable statutory parameters. This concerns both the capability to protect its networks and systems from attacks and the capability to take offensive measures. The Defence organisation's digital capabilities can be deployed nation-wide at the request of civil authorities. These capabilities will also be deployed in international operations, both as part of our own capabilities and for the benefit of strengthening or building the capabilities of local authorities. In doing so, the capabilities of the armed forces contribute to the integrated approach proposed by the Netherlands.

NATO may play an important role as a facilitator, including promoting national capability build-up, improved information exchange and interoperability and public-private cooperation. The Netherlands also strives to participate in exercises and to strengthen EU-NATO cooperation, in which the overlap of capabilities should be avoided.

Cooperation in the area of defence in an EU context will be mostly aimed at crisis management, pan-European exercises and the effective investigation and prosecution of cyber crime. In an international context, the Netherlands continues to promote the importance of a broader ratification of the Convention on Cybercrime of the Council of Europe (Budapest Convention). A good cooperation between national Computer Emergency Response Teams (CERTs) is of vital importance for swift actions and an early detection of threats, vulnerabilities and incidents. In the Netherlands, the NCSC fulfils this role. A further expansion and strengthening of existing alliances like the EGC and FIRST is a priority for the Netherlands. Flexibility and mutual trust are of paramount importance in these alliances.

2.4.2 DIPLOMACY

The Netherlands attaches great importance to mechanisms that ensure stability in the digital domain. We do this by investing in formal and informal alliances, within and outside of Europe, globally and in multi-stakeholder settings. Therefore, with its position in the area of international law, the Netherlands wants to contribute to the discussions about the application of legal rules in the digital domain. In addition, cyber diplomacy instruments will have to be defined. This may be in the form of so-called trust-inspiring measures, 'rules of the road', or standards of conduct.[22] With The Hague as the city of international peace and security, the Netherlands aims to develop into an 'international centre of cyber diplomacy' where diplomats, policymakers and cyber experts come together.

2.4.3 DEVELOPMENT

Threats in the digital domain transcend boundaries. Therefore, the Netherlands can benefit from countries being able to counter such threats. The NCSC focuses on strengthening CERT capabilities in countries that request its support in this matter.

The Netherlands also supports capability building in the EU by means of, among other things, the implementation of the EU Cyber Security Strategy. The associated objective is to create a basic level of security and a level playing field. Promoting the cyber security approach in a European framework will be an important issue during the Netherlands' EU presidency in 2016. Particular themes promoted by the Netherands in a European context, in addition to the forementioned strenghtened CERT cooperation, are:

- Maintaining open standards, content and interoperability of the internet
- Promoting innovation of secure ICT products (security by design)
- Security requirements for new and existing (embedded) ICT.

22 The starting point for the Netherlands in this context are the UN's Manifesto and the Geneva and The Hague Conventions.

Proficient users and a sufficient number of cyber security professionals are necessary for making optimal use of the opportunities offered by digitisation and for being resilient to the ever more advanced threats.

3 Approach

The Dutch vision on cyber security is translated into a concrete approach, and is described in this chapter. Section 3.1 states the Dutch ambitions in the area of cyber security and the strategic objectives that support cyber security. Sections 3.2 up to and including 3.6 clarify the NCSS2 objectives, and the most important focal points are clarified per objective. The action programme is included in Annexe 1. The action programme states the action items that are implemented in the NCSS2 context.

3.1 AMBITION AND STRATEGIC GOALS

Based on the vision, the government aims to realise the following ambitions:

The Netherlands is a leader in cyber security:

- *Dutch society knows how to make safe, optimal use of the advantages of digitisation.*
- *Dutch businesses and the research community are pioneers in 'security by design' and 'privacy by design'.*
- *Together with its international partners, the Netherlands is part of a progressive coalition that seeks to protect fundamental rights and values in the digital domain.*

The realisation of these ambitions is given shape based on the strategic objectives below. These objectives are the central themes of the 2014-2016 action programme. Annual progress reports will be drawn up and the action programme is updated when necessary.

1. The Netherlands is resilient to cyber attacks and protects its vital interests in the digital domain.
2. The Netherlands tackles cyber crime.
3. The Netherlands invests in secure ICT products and services that protect privacy.
4. The Netherlands builds coalitions for freedom, security and peace in the digital domain.
5. The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.

3.2 THE NETHERLANDS IS RESILIENT TO CYBER ATTACKS AND PROTECTS ITS VITAL INTERESTS IN THE DIGITAL DOMAIN

Our critical infrastructure increasingly depends on ICT systems. Disruptions to these systems or a violation of the confidentiality of information stored in such systems by states and criminals have a major impact. It may even lead to social disruption. There is an increased interwovenness of military and civil dimensions, public and private dimensions, and national and international dimensions in the digital domain. For instance, national security may be threatened by a large-scale cyber attack on one or more private organisations[23]. The speed with which such attacks can occur and develop requires a swift, coordinated and flexible response and an early involvement of the most important parties involved.

Therefore, it is of major importance that we gain more insight into the critical processes and services, and in the risks they may run. It is similarly important to critically view the underlying ICT chain structure and 'legacy' systems. Based on this risk-based approach, we will increase the resilience of vital services and processes and work to an effective joint public-private and civil-military response, and with the help of our international partners.

1 Risk analyses, security requirements and information sharing within critical infrastructure sectors

Within the framework of the protection of critical infrastructure, the government, working with vital parties, will identify critical ICT-dependent systems, services and processes. These efforts are linked to a programme that will establish basic security requirements on the basis of risk analyses.

In addition, a training programme for response to large-scale ICT incidents is set up. In cooperation with its partners, the National Cyber Security Centre sets up a national detection and response network for the central government and other vital sectors. Provided with safeguards related to confidentiality and privacy, these

23 Highly-publicised digital attacks that have caused major damage or that could have been substantially disruptive, such as DigiNotar in the Netherlands, Stuxnet in Iran and the cyber attack on Aramco in Saudi Arabia, were not aimed at military targets, but at strategic civil targets.

networks will work to a real-time analysis and sharing of threat information.

2 More active approach to cyber espionage

The Dutch government is committed to raising awareness among citizens, businesses, organisation and government bodies about information security and privacy. This means that awareness campaigns will partly focus on increasing knowledge and insight into the risks of cyber espionage. On the other hand, the government also ensures that the issue is prioritised within the intelligence and security services, which are given the tools to better document cyber threats and investigate and combat advanced attacks. To this end, the intelligence and security services have combined their cyber capabilities in the Joint Sigint Cyber Unit (JSCU). Furthermore, the government will prioritise a better protection of data citizens share with the government and being more transparent about data management.

3 Feasibility study on separate vital network

An exploratory study is conducted to determine whether it is possible and useful, from both a technical and organisational perspective, to create a separate ICT network for public and private vital processes. A separate network widens the range of options for safeguarding the continuity of vital processes. It also makes it possible to set up private, cloud-based data storage, thus strengthening the privacy and integrity of the data in storage or in the cloud concerned.

4 Enhancing civil-military cooperation

Digital means increasingly form an integral part of military actions. In order to safeguard the deployability of the Netherlands armed forces and to increase the effectiveness of the armed forces, the Defence organisation is increasing its digital resilience and is developing its own capabilities to conduct cyber operations . Civil and military domains within the digital domain have become more intertwined. Therefore, options for deploying the digital capabilities of the Netherlands Defence organisation on a national level in preventing and countering attacks on the civil infrastructure will be detailed. The central question is how to optimally share knowledge and expertise between civil parties and the Defence organisation.

5 Strengthening the National Cyber Security Centre

In a short period of time, the NCSC has developed into the key entity in the public-private cyber security network. At the same time and in part due to the large number of incidents, expectations regarding the role of the NCSC have grown. In order to give shape to this, the position of the National Cyber Security Centre (NCSC) is bolstered by means of a stronger structure for confidential information-sharing and analysis. Furthermore, in its capacity as the expert authority, the NCSC provides advice to private and public parties involved, both when asked and at its own initiative. Finally, based on its own detection capability and its triage role in crises, the NCSC is developing into a Security Operations Centre (SOC), in addition to its role as a Computer Emergency Response Team (CERT)[24].

3.3 THE NETHERLANDS TACKLES CYBER CRIME

Cyber crime is a frequently occurring and increasing threat for all citizens and organisations in the digital domain. In order to offer adequate protection from cyber crime, the Netherlands will prioritise the fight against cyber crime by means of strengthening the current capabilities in the area of investigation and prosecution. Updated legislation, a close cooperation and information-exchange between the various players involved is of the utmost importance. The Netherlands will actively pursue national and international alliances, for instance in an EU framework, and deepen such alliances to achieve an all-encompassing and bold approach to cyber crime.

6 International approach to cyber crime: updating and strengthening legislation (including the Criminal Code).

There is a need for effective, swift and efficient investigation of cyber crime in accordance with clear rules. Scarce capabilities have to be targetedly deployed among vulnerable sectors and groups. The Netherlands will assume a vanguard role in harmonising legislation governing international investigations, for instance in the Council of Europe. The Netherlands will also work to strengthen and expand international partnerships like the European Cyber Crime Centre EC3, at Europol. This international cooperation will also eventually include, in the long term, a detailed form of arbitration between countries when they are not satisfied with the assistance offered by the investigation process. The Netherlands actively participates in international meetings and related activities, such as the Committee of Contracting States of the Council of Europe, the Convention on Cybercrime, the 'EU policy cycle on organised crime', and the discussions

24 In addition to response, SOC comprises other aspects from the cyber security chain, such as awareness, resilience, detection, alerting, reporting and crisis management.

within UNODC about a UN treaty in the area of cyber crime. In the Netherlands itself, a bill is being passed that will bestow more powers on the police service and the Public Prosecution Service in investigating cyber crime in the digital domain.

3.4 THE NETHERLANDS INVESTS IN SECURE ICT PRODUCTS AND SERVICES THAT PROTECT PRIVACY

An increasing amount of ICT-based products and services are linked to public networks, such as the internet, which for its part is linked to other products and services. This development offers many advantages, but also introduces new security risks. In the physical domain, it is customary to set security and quality requirements to products and services before they are marketed. However, in the digital domain, this is not common practice yet. For instance, the impact and side-effects of ICT products or services such as online investments or online shopping are hardly included in deliberations of whether or not to use them. Security and privacy requirements help organisations and citizens with protecting themselves against security risks. The government's digital service provision should set an example.

Innovation, security and privacy in the design phase of products and services can not only be successfully combined, but they can also support these products and services in distinguishing them from the competition. The efforts of the government and the business world should therefore be focused on making this rewarding. Cooperation with international partners is an essential element in this process.

7 Supported standards, 'security by design' and 'privacy by design'

Together with private sector partners, the government is working to develop standards that can be used to protect and improve the security of ICT products and services. To this end, the government in an international context will also enter into a dialogue with relevant private parties and will act in a framework-developing and standards-developing fashion to protect the privacy and security of users. Wherever possible, this also takes place in a European or wider international context, and a link is being sought with existing international standards and good practices[25]. By including standards in tendering requirements stimulates the government to implement it as a 'launching customer'.

3.5 THE NETHERLANDS BUILDS COALITIONS FOR FREEDOM, SECURITY AND PEACE IN THE DIGITAL DOMAIN

The Netherlands benefits from a stable, free and accessible digital domain and therefore wants to continue to play a leading role in the protection of this domain. With The Hague as the city of peace and security, the Netherlands aims to develop standards in a multi-stakeholder context and to protect fundamental rights and values in cyberspace. Furthermore, the Netherlands in cooperation with its international partners will work to preventing and fighting conflicts in the digital domain. Effectively responding to these conflicts is not only limited to the digital domain, but also requires an integrated approach, as is the case with other security threats. Use of traditional elements such as diplomacy, imposing sanctions, capability building and Defence capabilities have to be adjusted to the specific character of the digital domain. In light of this objective, cyber capabilities that fit in with the 3D approach (Development, Diplomacy, Defence) are being developed.

8 Cyber diplomacy: hub for expertise for conflict prevention

The Netherlands aims to develop a hub for expertise on international law and cyber security in order to promote the peaceful use of the digital domain. To this end, the Netherlands combines knowledge from existing centres. The centre brings together international experts and policymakers, diplomats, military personnel and NGOs. This creates a network that brings together multidisciplinary knowledge about subjects such as international standards for conflict prevention, civil-military cooperation and non-proliferation of cyber weapons in the digital domain. The network also contributes to discussions about this subject. This forms the basis for a series of multi-stakeholder, high-level meetings.

3.6 THE NETHERLANDS HAS SUFFICIENT CYBER SECURITY KNOWLEDGE AND SKILLS AND INVESTS IN ICT INNOVATION TO ATTAIN CYBER SECURITY OBJECTIVES

Until now, cyber security has been underexposed in education. Proficient users and sufficient cyber security professionals are necessary for making optimal use of the opportunities offered by digitisation and for being resilient to the ever more advanced threats. Cyber

25 In Dutch society, the Forum and Standardisation Authority promote interoperability and the application of open standards through a list of recommended and compulsory standards for the (semi) public sector.

security professionals are also needed to design and build the cyber security solutions of the future. The Netherlands has plenty of talented IT workers. However, their skills need to be honed as early as secondary school and then continued in top degree programmes in senior secondary vocational education, at a university of applied sciences or in university education. For this reason, the Netherlands has opted for a wide approach, ranging from primary education to higher education, and from work-based training to university, and from the board room to the coal face. In addition to education and training, awareness campaigns remain important. In order to be able to take the step from being aware to becoming capable, these campaigns will be used in a more targeted manner and more attention will be paid to the perspectives for action of the target group.

An excellent cyber security knowledge infrastructure not only works in support of our society's resilience, it also offers opportunities for developing expertise and for finding niches. This requires an attractive research and education climate to be created in which cyber security plays a prominent role. A multidisciplinary approach in which the non-technical sub-areas are also included is needed to promote cyber security innovation. The innovative products and services that are developed in this manner will help the Netherlands with anticipating swift technological and other developments in the digital domain. Dutch design (in security) can also become a quality mark for security and privacy in ICT products and services, thereby contributing to economic growth.

9 Taskforce on cyber security education

To enlarge the pool of cyber security experts and enhance users' proficiency with cyber security, the business community and the government have joined forces to improve the quality and breadth of ICT education at all academic levels (primary, secondary and professional education). A PPP taskforce on cyber security education will be set up which will focus on giving advice about the cyber security curriculum, in relation to the certification of information security experts and the further development of learning modules, among other things. For the time being, connections are being sought with current initiatives regarding information sciences education and the Technology Pact 2020.

10 Encouraging innovation in cyber security

Technological developments in the digital domain are taking place at an alarming rate. This means that being able to anticipate them is a vital element. Innovation arises where creative people and experts meet. This alone, however, is not enough. There is a need for more coordination of supply and demand, which can be achieved by linking[26] innovation initiatives to leading sector policy. In addition, the government, the business community and the world of academia will launch a cyber security innovation platform where start-ups, established companies, students and researchers can connect and inspire one another. In organising a follow-up to the SBIT research programme in 2012-2013, the government contributes to this. The farther-reaching PPP implementation of the second edition of the National Cyber Security Research Agenda (NCSRA) will also contribute to this development.

3.7 A JOINT EFFORT

The government and the Netherlands have big ambitions in the area of cyber security and comprise a broader long-term vision. This vision reflects the importance of and opportunities offered by ICT to our society and our economy, as well as the current threats and risks. A joint effort made by all parties involved is required, in which each of the parties is expected to take own responsibility. Therefore, the government has invited many organisations from government bodies and the business world to help with developing the strategy. Unfortunately, financial means are limited due to the current economic climate.

In the present strategy, the long-term ambition has been given shape in the 2014-2016 action programme (see also Annexe 1), which is detailed within the scope of the regular departmental budgets and the partners' budgets. Entirely in line with the move initiated by the action programme, the government will implement the broader strategy through participation, reprioritisation, smart coalitions and an integrated approach, which in its entirety will respond to increased problems that threaten our prosperity and wellbeing. The long-term ambition also shows that realising a secure digital domain – also in the long term – is by no means an ambition that is free of obligations. This ambition is given more shape in the future action programmes and will have to fall within the scope of the financial parameters that will be in place at that time. Therefore, the details regarding the implementation of the actions stated in the annexes take place in consultation and/or cooperation with private parties and the government bodies involved.

26 Such as the National Cyber Security Research Agenda (NCSRA) and The Hague Security Delta (HSD).

Annexe 1: 2014-2016 action programme

Objective 1:

The Netherlands is resilient to cyber attacks and protects its vital interests in the digital domain

Action	Who[27]	When
1. Cyber security is included in the vital infrastructure approach. An element of this approach will be periodically listing which ICT-dependent systems, services and processes are vital. This is linked to a resilience-enhancing programme and public-private crisis exercises.	In consultation with line ministries, vital sectors (including regional authorities)	2014 and beyond
2. Developing a system of supported open (technological) standards and minimum requirements for increasing the digital security of vital processes. Where possible, an alliance with existing national and international standards and *best practices* is pursued.	Line ministries, NCSC, vital sectors	2014
3. Encouraging that privacy and security by design are included in the tendering processes of products and services for the government.	All ministries	2014-2016
4. Conducting an exploratory study into a separate ICT network for (public-private) vital processes.	Security and Justice, line ministries	2014
5. Building and expanding a national detection and response network.	Security and Justice, Defence, public and private partners	2013 and beyond
6. Strengthening the digital resilience of the Dutch defence systems as well as increasing the capability to conduct cyber operations.	Defence	2014-2015
7. Committing local governments to a strengthened approach to information security.	Interior and Kingdom Relations (Taskforce BID)	2014
8. Formulating responsibilites and documenting procedures (including upscaling) in case of organisation-transcending incidents that are not crises.	Interior and Kingdom Relations, Security and Justice, intelligence and security services, local authorities	2015
9. Strengthening research and analysis capabilities to gain more insight into threats and risks in the digital domain.	Intelligence and security services, NCSC, police service	2014
10. Strengthening of NCSC, among other things, through the development of a Cyber Security Operations Center, in addition to its role as a CERT.	NCSC, intelligence and security services, vital sectors	2014

27 In compliance with existing responsibilities.

11. Mapping out risks of legacy systems in vital processes and services.	Security and Justice, Interior and Kingdom Relations	2014
12. Strengthening of existing sectoral regulatory authorities by including cyber security requirements (and avoiding overlap).	Sectoral regulatory authorities and line ministries	2015
13. Exploring accreditation options of companies that can be called upon as 'digital fire brigades'.	Security & Justice/NCSC and vital sectors	2015
14. Setting up a cyber reservists database.	Defence	2013
15. Setting up a Defence Cyber Command for overall coordination and readiness of cyber capabilities.	Defence	2014

Objective 2:

The Netherlands tackles cyber crime

Action	Who	When
16. Updating and strengthening (international) criminal legislation (including the Computer Crime Act III).	Security and Justice	2014-2016 (Computer Crime Act completed in 2014)
17. Improving cooperation with Europol's EC3 by exchanging knowledge and personnel.	Security and Justice	2014-2016
18. Include the strengthening of investigation and prosecution of cyber crime as a subject in the discussion about new National Priorities (the current subjects lapse on 1 January 2015).	Security and Justice, Public Prosecution Service, police service	2014
19. Strengthening the fight against cyber crime in the financial sector through cooperation.	Security and Justice, DNB, Public Prosecution Service, police service, Fiscal Intelligence and Investigation Service, NVB, bank sector as a whole	2014
20. The number of international investigations will be expanded to 20 in 2014.	Security and Justice, Public Prosecution Service and police service	2014
21. Supervising the link to the investigation and prosecution services in the digitisation of crime.	Security and Justice Inspectorate	2014
22. Strengthening the intake and registration process of cyber crimes reported to the police.	Police service	2014-2016

Objective 3:

The Netherlands invests in secure ICT products and services that protect privacy

Action	Who	When
23. Improving and/or developing standards, in an international context where possible, that are used to promote the security and privacy of ICT products and services.	Line ministries and partners	2014 and beyond
24. Launching awareness campaigns, such as Alert Online, in which privacy also plays a part.	Security and Justice, Dutch DPA, Electronic Commerce Platform Netherlands	2014-2016

Objective 4:

The Netherlands builds coalitions for freedom, security and peace in the digital domain

Action	Who	When
25. Giving shape to cyber diplomacy and in cooperation with international partners developing standards and trust-inspiring measures to counter conflict escalation in the digital domain.	Foreign Affairs, Security and Justice	2014-2016
26. Setting up a hub for expertise in the area of international law and cyber security with the purpose of promoting conflict prevention in the digital domain. A series of high-level meetings will be organised as part of this.	Foreign Affairs, Security and Justice	2014-2015
27. Continue to be the international leader in the area of internet freedom, for instance through the Freedom Online Coalition (FOC), and working to establish a powerful European approach to privacy protection and fundamental rights and values with respect to third countries.	Foreign Affairs, Interior and Kingdom Relations, Security and Justice	2014 and beyond
28. The Dutch government will increase its participation in multi-stakeholder events such as the Cyberspace Conferences and the IGF.	Economic Affairs, Foreign Affairs, Security and Justice	2014
29. The Netherlands works to develop cyber security capability in third countries through bilateral or regional initiatives.	Foreign Affairs, Defence, Security and Justice	2014-2016
30. Detailing options for national deployment of digital capabilities of Defence at the request of civil authorities.	Defence	2014

Objective 5:

The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives

Action	Who	When
31. A PPP taskforce on cyber security education will be set up which will focus on giving advice about the cyber security curriculum. This includes certification and the further development of learning modules.	Security and Justice Economic Affairs, Research, Education and Science	2014
32. For the time being, connections are being sought with current initiatives regarding information sciences education and the Technology Pact 2020.	Research, Education and Science	2015
33. Realising more work placement opportunities and technical traineeships in cyber security in the public sector.	Security and Justice and Interior and Kingdom Relations	2015
34. NL Agency and the Netherlands Organization for Scientific Research (NWO), as a follow-up to the 2012-2013 tender, will issue new tenders to the value of about € 6 million, to be roughly evenly distributed over an SBIR programme and long-term research.	Economic Affairs, NWO (co-financed by line ministries)	2014-2015
35. Developing Cyber Defence training and education programmes with private parties and Regional Training Centres.	Defence	2014
36. Drawing up a plan in order to better meet research needs in the business world through 'scientists on the job'.	NWO/ Netherlands Organisation for Applied Scientific Research in cooperation with the business community	2013, 2014
37. Launching a cyber security platform for start-ups and established companies, students and researchers.	Economic Affairs, Security and Justice and the business community	2015

This is a publication of the National Coordinator for Security and Counterterrorism

Visiting address
Turfmarkt 147
2511 DP Den Haag

Postal address
Postbus 20301
2500 EH Den Haag

T (070) 751 50 50
E info@nctv.minvenj.nl
I www.nctv.nl

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu