CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Kadri Kaska

National Cyber Security Organisation: the Netherlands

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of December 2014.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

THE NETHERLANDS

By Kadri Kaska
Researcher, NATO CCD COE

Table of Contents

1. INTRODUCTION: INFORMATION SOCIETY IN THE NETHERLANDS 5

1.1. Infrastructure availability and take-up 5
1.2. E-government and private sector e-services 5
1.2.1. Citizen and enterprise portals 6
1.2.2. E-Commerce & private sector e-services 7
1.2.3. E-service infrastructure 7

2. STRATEGIC NATIONAL CYBER SECURITY OBJECTIVES 7

2.1. National cyber security foundation 7
2.2. Cyber security strategy objectives 8
2.3. Defence Cyber Strategy 9

3. NATIONAL ORGANISATIONAL STRUCTURE FOR CYBER SECURITY AND CYBER DEFENCE 10

3.1. Political and strategic level cyber security management and coordination 10
3.1.1. Cyber Security Council 10
3.2. Operational cyber security capabilities and cyber incident management 11
3.2.1. National Cyber Security Centre 11
3.3. Military Cyber Defence Capabilities 15
3.3.1. Resilience 15
3.3.2. Cyber operational capabilities 16
3.4. Cyber intelligence 17
3.5. Cyber aspects of crisis management 17
3.5.1. Cyber crisis prevention 17
3.5.2. Crisis management 19

REFERENCES 21

1. Introduction: information society in the Netherlands

1.1. Infrastructure availability and take-up

The Netherlands is one of the most connected countries in Europe, with 95% of households having an internet connection and 92% of the population being considered regular internet users[1].[2] Under both metrics, the Netherlands ranks at the very top of the 28 countries of the European Union.

Both fixed and mobile broadband internet coverage have been universally available to the whole population since 2005 and 2008, respectively. The fixed broadband penetration rate[3] exceeded 40% in 2012, with 84% of households and 96% of enterprises having a subscription. Mobile broadband take-up is quickly catching up, with penetration rates doubling between 2010 and 2012; it stood at over 60% of the population in 2012. 33% of the population use mobile phones to access the internet.

A fixed broadband speed of at least 2 Mbps is practically universal (99% as of 2013); speeds of 10 Mbps and 30 Mbps are enjoyed by 69% and 42% of all subscribers respectively, while 9% of subscribers have ultra-high speed internet access (100 Mbps). The dominant access technologies are DSL and cable TV networks, but optical cable also holds a notable share.[4]

Infrastructure-wise, the Netherlands holds a remarkably strong position even considering the global context. A large portion of undersea optical cables to Europe run through the Netherlands.[5] The Amsterdam Internet Exchange, which interconnects more than 600 communications networks and handles data traffic volumes of up to 3 Tbit/s, is the world's largest.[6] The Netherlands is fourth in Europe and eighth globally among hosts for co-location data centres.[7] In 2014, Google announced an investment of €600 million in the Netherlands for the construction of a new data centre, planned to be operational by 2017.[8] Nearly 1% of the Netherlands' GDP is invested to ICT infrastructure.[9]

1.2. E-government and private sector e-services

The Netherlands was among the first countries in Europe to launch e-government programmes, introducing the first national ICT programme in 1994 and an action programme for electronic government (*Actieprogramma Elektronische Overheid*) in 1998.[10] A significant share of basic public services in the Netherlands were available

[1] Defined as 'individuals using the internet at least once a week in the last 3 months'.
[2] Unless otherwise indicated, statistical data in this section is drawn from the EU Digital Agenda Scoreboard for the Netherlands in 2013: EU Digital Agenda, 'Country Ranking Table, On A Thematic Group Of Indicators — Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"ref-area":"NL","time-period":"2013"}>.
[3] Broadband take up rate per 100 persons.
[4] 'Special Eurobarometer 396 - E-Communications Household Survey', 2013, 36 <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2629>.
[5] TeleGeography, 'Submarine Cable Map', 2014 <http://www.submarinecablemap.com>.
[6] Amsterdam Internet Exchange, 'About AMS-IX', 2014 <https://ams-ix.net/about/about-ams-ix>; Deloitte, 'Digital Infrastructure In The Netherlands – The Third Mainport', 2013 <http://ecp.nl/item/3937>. Internet exchange (peering) enables direct interconnection between networks at the exchange point, which reduces bandwidth requirement and cost to operators.
[7] Data Center Map, 'Colocation The Netherlands', 2014 <http://www.datacentermap.com/the-netherlands/>.
[8] Google Europe Blog, 'Expanding Our Data Centres In Europe', 2014 <http://googlepolicyeurope.blogspot.be/2014/09/expanding-our-data-centres-in-europe.html>.
[9] Interxion, 'Netherlands', 2014 <http://www.interxion.com/locations/netherlands/>.
[10] Jan van Dijk *et al*, 'E-Services for Citizens: The Dutch Usage Case', *Electronic Government*, 2007, Vol. 4656, 155-166. In Maria A. Wimmer *et al*, 'Electronic Goverment: 6th International Conference, EGOV 2007, Regensburg, Germany, September 3-7, 2007, Proceedings', Springer Science & Business Media, 2007 <http://dx.doi.org/10.1007/978-3-540-74444-3_14>. The initial programs have been followed up by Dutch National ICT Agenda 2008–2011 and the corresponding National Implementation Programme (NUP), and the National ICT Strategy 2012-2015 with the National Implementation

online by 2004, the majority of these hosting the entire transactional cycle online,[11] although initially, save for a few successful exceptions, take-up was rather low.[12] By 2010, the availability of basic public e-services to individuals had reached 100%, while supply to enterprises had reached 88%. The share of individuals having used the internet for interaction with public authorities had risen to nearly two-thirds of the population and 95% of enterprises.[13] In 2013, e-government take-up of the 20 basic public services measured had risen to 79% for individuals, although enterprise use had declined by 5 percentage points. With regard to individuals' take-up of e-government, the Netherlands ranked 2nd among the 28 EU Member States. Indicators of e-governance services rendered to enterprises remained above the EU averageas well. Currently, high quality e-services are also provided by the local municipalities in terms of both service availability and sophistication (that is, the entire transactional cycle being available online).[14] The nation's ambition is to enable fully digital interaction with government authorities by 2017.[15]

The 2012 United Nations E-government Survey ranked the Netherlands second on their World E-Government Development Leaders index, holding the first position in Europe.[16]

1.2.1. Citizen and enterprise portals

The Netherlands employs a governmental information and service web portal, www.mijnoverheid.nl ('My Government'), where users can access their records kept by government agencies, communicate with administrative authorities, and keep track of their transaction with administrative bodies.[17] The portal provides single sign-on access to e-services provided by national, regional and local authorities.[18]

A new single-point business portal, www.ondernemersplein.nl ('The Business Place'), was launched in 2014. The portal offers a wide range of government information for entrepreneurs in collaboration with both public and private sector partners.[19] Among other features, the portal supports business registration and communication with administrations, application for permits and licences, and the delivery of notifications and administrative decisions. All are integrated into the portal solution via a personal, secure message box.[20]

Programme (i-NUP). eGovernment Factsheets. 'eGovernment in The Netherlands', Edition 16.0, 2014 <https://joinup.ec.europa.eu/sites/default/files/55/a8/5e/eGov%20in%20NL%20-%20April%202014%20-%20v.16.pdf>.

[11] The study looked at 20 basic public services provided by the government to citizens and businesses in the areas of tax reporting, registrations and licences, and administrative services. Capgemini, 'Online Availability Of Public Services: How Is Europe Progressing? ', European Commission, Directorate General for Information Society and Media, 2005, 64-65.

[12] While online tax filing amounted to 82% of all income tax filings in 2005, a substantial share of the e-services offered were 'hardly used and only a few services are responsible for the bulk of the e–service usage in the Netherlands'. Dijk *et al* (n 10) 156. Such findings might have been emphasised due to the fact that the Netherlands was among the few European nations who also took effort to measure service take-up. Capgemini, Sogeti, IDC, RAND Europe and the Danish Technological Institute, 'Digitizing Public Services In Europe: Putting Ambition Into Action. 9th Benchmark Measurement', European Commission, Directorate General for Information Society and Media, 2010, 73.

[13] Capgemini (n 12) 73.

[14] ibid 11, 63-66, 78. This is significant against the EU prevalent background of lower service quality in rural areas as compared to governmental ones, especially those provided by smaller municipalities.

[15] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Visiebrief digitale overheid 2017', 2013 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017/visiebrief-digitale-overheid-2017.pdf>. Digital government 2017 vision paper presented to the House of Representatives in May 2013.

[16] United Nations Department of Economic and Social Affairs, 'United Nations E-Government Survey 2012: E-Government For The People', New York, 2012, 10 <http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/unpan048065.pdf>.

[17] Mijnoverheid, 'Uw persoonlijke website voor overheidszaken' <https://mijn.overheid.nl/?r=1>.

[18] Capgemini (n 12) 128-129.

[19] Ondernemers Plein, 'Over Ondernemersplein.NI' <http://www.ondernemersplein.nl/over-ondernemersplein/>. The new portal integrates the similar earlier resource, www.antwoortvoorbedrijven.nl, while adding new features.

[20] Capgemini (n 12) 93, 98.

The 2010 European e-government report highlighted the Netherlands as among the best in Europe for e-service portal usability, user-centric design, and service bundling.[21]

1.2.2. E-Commerce & private sector e-services

As for commercial e-services, the share of internet users using online banking services has remained steady at 86-87% over the past four years, and in 2013 the Netherlands ranked 3rd in the EU with this indicator. Other common uses of online services include looking for information about goods and services (89% of internet users), participating in social networks (59%), and engaging in educational (31%) and labour market services (22%).

The Dutch are avid users of internet commerce, with 78% of internet users ordering and 51% selling goods or services online. One-fifth of large enterprises and 8% of SMEs' turnover in 2013 relied on e-commerce and a significant share of enterprises employed some form of electronic solutions for business management.

1.2.3. E-service infrastructure

For the purposes of electronic identification and authentication enabling citizens to use public e-services, a username-password combination or Digital ID (DigiD) is used with secondary SMS verification. DigiD is not mandatory, but it is widely used for hundreds of governmental, administrative, social and healthcare services.[22] Paper IDs have been replaced with smart cards.[23]

Online service provision is supported by a number of legal acts, including the Government Information (Public Access) Act, Personal Data Protection Act (2000), eCommerce Act (2004), Telecommunications Act (2004), and Electronic Signature Act (2003).

A government cloud strategy was initiated in 2011 and supported by the national ICT strategy 2012-2015 (*'i-strategy'*) which was launched later the same year). It proposed the gradual implementation of government-wide cloud computing in a closed cloud.[24]

2. Strategic national cyber security objectives

2.1. National cyber security foundation

The first Dutch national cyber security strategy was adopted in February 2011.[25] The 2011 strategy focused on bringing coherence and consistency into the various national activities related to cyber security, clarifying the division of responsibilities among actors, taking steps to strengthen public-private cooperation, and advocating that any proposed measures taken toward ICT security be necessary and proportionate.[26]

---

[21] ibid 9.

[22] DigiD, 'About DigiD' <https://www.digid.nl/en/about-digid/>; DigiD, 'Wie Doen Mee?' <https://www.digid.nl/nl/over-digid/wie-doen-mee/>.

[23] Capgemini (n 12) 121.

[24] Verheid.nl, 'Brief van de minister van binnenlandse zaken en koninkrijksrelaties', 2011, Nr. 179 <https://zoek.officielebekendmakingen.nl/kst-26643-179.html>; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Betreft i-strategie rijk', 2011, 4 <http://www.nationaalarchief.nl/sites/default/files/docs/nieuws/kamerbrief-informatiseringstrategie-rijk.pdf>. An outcome of this endeavour has been the consolidation of 66 existing data centres into four major new centres. Binnenlands Bestuur, 'Potentie Overheidscloud Zit Vooral In Shared Services', 2013 <http://www.binnenlandsbestuur.nl/digitaal/partners/cgi/potentie-overheidscloud-zit-vooral-in-shared.9161777.lynkx>.

[25] Dutch National Cyber Security Centre, 'The National Cyber Security Strategy (NCSS): Strength Through Cooperation', The Hague: Ministry of Security and Justice, 2011 <https://www.ncsc.nl/english/current-topics/news/national-cyber-security-strategy-launched.html>.

[26] 'The National Cyber Security Strategy' (n 25) 5-6.

Implementation of the 2011 strategy, and in particular the institutional steps taken to establish the Cyber Security Council and the launch of periodic national threat and risk analyses known as Cyber Security Assessments,[27] accelerated a strategic understanding about 'threats and vulnerabilities in the digital domain' as well as a need for adjusting current approaches with regard to the participation of various actors, especially in the international arena.[28] Out of that consideration, in October 2013, the Dutch Minister of Security and Justice presented the Netherlands' current national cyber security strategy, entitled *'National Cyber Security Strategy 2: From Awareness to Capability'* (NCSS 2).[29] The drafting process of NCSS 2 involved a number of stakeholders from the public and private sectors, academia, and wider society, with the ICT community being specifically consulted.[30]

The vision statement of NCSS 2 highlights three aspects: the security, freedom and socioeconomic benefits of cyber security; clear cyber security responsibilities of individuals, businesses and government; and cooperation with international partners, specifically in the areas of defence, diplomacy, and development of CERT cooperation and secure ICT products.[31]

2.2. Cyber security strategy objectives

NCSS 2 sets five strategic cyber security goals:[32]

- strengthening ICT systems' resilience to cyber attacks and protecting the nation's vital interests, by the integrated actions of private and public (both civil and military) sector;
- tackling cyber crime;
- investing in secure ICT products and services that protect privacy;
- international cooperation to promote building coalitions for freedom, security and peace in the digital domain; and
- advancing awareness, skills and ICT and cyber security innovation.

These objectives rely upon ten common themes:

1. Identifying critical ICT-dependent systems, services and processes and establishing basic security requirements based on risk analyses.
2. Raising society's awareness about privacy and information security, and resourcing the intelligence and security services to better address cyber espionage.
3. Determining the feasibility of a separate ICT network for public and private vital processes.
4. Enhancing civil-military cooperation, with a specific focus on optimally sharing knowledge and expertise between the two.
5. Strengthening the National Cyber Security Centre by improving its capability for confidential information sharing and analysis. Further organisational upgrades envisaged by NCSS 2 with regard to the NCSC assuming the role of expert authority and security operations centre are already underway (see section 3.2).

[27] GOVCERT.NL. Dutch National Cyber Security Centre. 'Cyber Security Assessment Netherlands (CSAN)', The Hague: Ministry of Security and Justice, 2011, 3 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/cyber-security-report-2011.html>. Four such analyses have been published since the 2011 Strategy.
[28] 'National Cyber Security Strategy (NCSS) 2: From Awareness To Capability', The Hague: Ministry of Security and Justice, 2013, 7, 17 <https://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf>.
[29] National Cyber Security Centre, 'New Cyber Security Strategy Strengthens Cooperation Between Government and Businesses', 2013 <https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html>.
[30] Verheid.nl, 'Brief van de minister van veiligheid en justitie', Nr. 291, 2013 <https://zoek.officielebekendmakingen.nl/dossier/26643/kst-26643-291?resultIndex=7&sorttype=1&sortorder=4>.
[31] CSAN (n 27) 18-21.
[32] ibid 22-26.

6. Updating legislation and promoting international harmonisation efforts to strengthen cross-border cyber crime investigation.
7. Working with the industry to develop security standards, including 'security by design' and 'privacy by design'.
8. Working with partners to become a hub for expertise on international law and cyber security in order to promote the peaceful use of the digital domain.
9. Improving, in collaboration with various partners, ICT education at all academic levels in order to enlarge the pool of cyber security experts and enhance users' proficiency with cyber security.
10. Encouraging cyber security innovation by linking innovation initiatives, launching a cyber security innovation platform and continuing the National Cyber Security Research Agenda.

An annex to NCSS 2 sets out a concise action programme for 2014 to 2016 for achieving the five strategic goals, as well as itemising specific measures to be taken, mandating responsible entities (primarily government ministries, but some items also fall to the private sector), and establishing timelines.[33]

2.3. Defence Cyber Strategy

A sectoral Defence Cyber Strategy was announced by the Minister of Defence in June 2012. Based on the recognition of cyberspace as the fifth domain for military operations, the Defence Cyber Strategy considers the Dutch defence organisation's three core tasks – protecting territorial integrity, promoting stability and rule of law, and supporting civil authorities responsible for law enforcement, disaster relief and humanitarian assistance – as specific trajectories of strategic direction for strengthening the *resilience* and *capability* of the armed forces in the 'digital domain'.[34] The strategy is a further elaboration on defence-related aspects addressed in the national cyber security strategy.[35]

The strategy, envisioning cyberspace as an arena of military operations, treats 'digital assets as operational capabilities, i.e. as weapons or as intelligence assets, which must be incorporated in the operational capabilities of the armed forces as a whole', relevant to the protection of networks, systems and information, the deployment of offensive capabilities, and intelligence gathering using digital technology. For these purposes, the strategy communicates the intent to bring 'all activities connected with military operations in cyberspace' under central control and coordination. Furthermore, the strategy recognises the role of the defence organisation in cooperating with other actors - civilian, public and private, national and international - to defend against cyber threats affecting society as a whole.[36]

Based on these overall objectives, the Defence Cyber Strategy utilises a comprehensive approach designed on the basis of six focal points, incorporating the elements of defence, offense, intelligence, innovation, and cooperation:

- adopting a comprehensive approach;
- strengthening the cyber defence of the Defence organisation (defensive element);
- developing the military capability to conduct cyber operations (offensive element);
- strengthening the intelligence position in cyberspace (intelligence element);
- strengthening the knowledge position and the innovative strength of the Defence organisation in cyberspace, including the recruitment and retention of qualified personnel (adaptive and innovative elements); and

[33] CSAN (n 27) 28-33.
[34] 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace', Ministry of Defence, 2012, 4 <https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf>.
[35] 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 3.
[36] ibid 5.

– intensifying cooperation, both nationally and internationally (cooperation element).[37]

3. National organisational structure for cyber security and cyber defence

National cyber security roles and responsibilities in the Netherlands are divided among numerous actors, including Dutch Government ministries and private sector players. NCSS 2 identifies more than twenty bodies with individual and collective responsibilities for reaching the cyber security objectives posed by the strategy.[38] On the government level, these bodies include the Ministries of Security and Justice; Interior and Kingdom Relations; Economic Affairs; Defence; Foreign Affairs; and Research, Education and Science.[39] Among governmental agencies, tasks and responsibilities are defined for law enforcement and internal security entities (the Police Service, Public Prosecution Service, Fiscal Intelligence and Investigation Service, Security and Justice Inspectorate, and Intelligence and Security Services) as well as the Data Protection Agency, sectoral regulatory authorities (such as telecommunications), and the Central Bank. Regional and local authorities are also involved.

In the private sector, the bulk of the responsibilities defined in NCSS 2 falls on the financial sector (commercial banks, the Dutch Banking Association (NVB) and the Electronic Commerce Platform Netherlands in particular) and providers of vital services. Certain responsibilities require the involvement of the business community in general. Academia is also involved via the Netherlands Organisation for Scientific Research (NWO) and through government financing of independent research bodies such as the Netherlands Organisation for Applied Scientific Research (TNO).

The task of coordinating the various activities and ensuring a coherent implementation of NCSS 2 has been assigned to the national Cyber Security Council, set up in 2011 as a direct result of the 2011 NCSS.[40]

3.1. Political and strategic level cyber security management and coordination

3.1.1. Cyber Security Council

One of the 2011 NCSS's particular action items envisaged setting up a **Cyber Security Council** (*'Cyber Security Raad'*) as a body that would link the various parties responsible for the digital security of the country – the public and private sector as well as knowledge institutions – in a collaborative model, thereby improving cohesion in national policy initiatives, public information and operational cooperation.[41] The Council became operational on 30 June 2011.[42]

The Council's mandate, as defined by NCSS 2011, is the coordination and supervision of the implementation of the strategy, and involves four main threads: advising the government and private parties on developments in cyber security; setting national priorities in addressing threats to ICT; assessing national R&D needs; and knowledge sharing with public and private parties.[43]

---

[37] ibid 6.
[38] CSAN (n 27) 27-33.
[39] In addition to generic references made to 'all ministries' and 'line ministries' being responsible for certain activities.
[40] National Coordinator for Security and Counterterrorism (NCTb), 'Cyber Security Council Invested', 2011 <http://english.nctb.nl/currenttopics/press_releases/2011/press-release-110630.aspx>.
[41] CSAN (n 27) 9.
[42] NCTb (n 40).
[43] CSAN (n 27) 9; NCTb (n 40); National Cyber Security Centre, 'Cyber Security Assessment Netherlands (CSBN-2)', The Hague: Ministry Of Security and Justice, 2012, 53 <https://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-480116.pdf>.

In keeping with these expectations, the Council has issued several advice statements since its installation, *inter alia* providing recommendations in the course of drafting NCSS 2.[44] The Council functions as a mechanism for improving coordination of national research programmes, primarily in the public sector but also as far as possible between governmental programmes and those driven by the private sector or academia.[45] The Council also cooperates with both private and public organisations in developing dialogue, enhancing cyber awareness, and strengthening cyber defence.[46]

The Cyber Security Council was established by the Minister of Security and Justice and is co-chaired by representatives from the Government (the National Coordinator for Security and Counterterrorism under the Ministry of Security and Justice) and industry (currently KPN, a Dutch landline and mobile telecommunications company).[47] The Council involves 15 strategic-level representatives from the government representing the National Coordinator for Counterterrorism, the Ministry of Economic Affairs, the Ministry of Defence, the General Intelligence and Security Service, the National Police Services Agency, and the Board of Prosecutors General as the cybercrime portfolio holder.[48] The industry sector is represented by KPN, major ICT suppliers, major IT users, SMEs and critical infrastructure operators, and academia by the Universities of Tilburg and Delft, and by Radboud University Nijmegen.[49] With these different perspectives and portfolios, the composition of the Council also balances the various national interests and topics relevant to cyber security, in addition to the obvious public-private sector blend.[50] The Council is supported by its own secretariat;[51] in addition, responsible public bodies are tasked to assist it.[52]

The Council may offer advice with regard to cyber security developments both on request and on its own initiative.[53] In its advice, the Council is supported by the regular comprehensive public-private risk assessments, drafted and presented by the National Cyber Security Centre.[54] Based on the operating practice of the Cyber Security Council so far, the model is perceived to be a success. The Council has assumed the role of a connector rather well, and has been able to achieve consensus among the diverse and often competing interests of different stakeholders.[55]

3.2. Operational cyber security capabilities and cyber incident management

3.2.1. National Cyber Security Centre

Organisation

Together with setting up the National Cyber Security Council, NCSS 2011 proposed the creation of a **National Cyber Security Centre** (NCSC) which would bear the task to help improve 'understanding of developments, threats, and trends' as well as carry responsibilities in cyber incident handling and cyber incident-related crisis

[44] Elly van den Heuvel and Gerben Klein Baltink, 'Coordination And Cooperation In Cyber Network Defense: The Dutch Efforts To Prevent and Respond'. In M. E. Hathaway (ed), 'Best Practices in Computer Network Defense: Incident Detection and Response', IOS Press, 2014, 122-123.
[45] CSAN (n 27) 15.
[46] Van den Heuvel and Klein Baltink (n 44) 122; CSBN-2 (n 42) 53.
[47] Rijksoverheid, 'Cyber Security Raad Geïnstalleerd', 2011 <http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/06/30/cyber-security-raad-geinstalleerd.html>.
[48] The Council thereby also engages the governmental steering committee on priority crime (the scope of which includes cybercrime). CSAN (n 27) 13.
[49] CSAN (n 27) 9; NCTB (n 40).
[50] NCTb (n 40).
[51] Van den Heuvel and Klein Baltink (n 44) 122.
[52] CSAN (n 27) 9.
[53] Rijksoverheid (n 4747); Van den Heuvel and Klein Baltink (n 44) 122.
[54] Rijksoverheid (n 47).
[55] Van den Heuvel and Klein Baltink (n 44) 122; CSBN-2 (n 42) 7.

management.[56] The previously existing GOVCERT.NL was integrated into the new organisation with a strengthened and expanded mandate.[57]

The NCSC became operational from 1 January 2012 and soon assumed a key role in the public-private cyber security network, but due to growing expectations – triggered, on the one hand, by growing awareness, and on the other, by the volume and prominence of cyber incidents – NCSS 2 projected a strengthened role for the NCSC, upgrading it to an expert authority with the task of advising both public and private entities, both on request and on its own initiative.[58] The NCSC is now viewed as a 'Security Operations Centre', providing awareness, resilience, detection, alerting, reporting and crisis management, as well as advising both private and public parties.[59] The NCSC serves the central government as well as public and private organisations responsible for critical infrastructure, and seeks to strengthen public-private partnerships.[60]

Organisationally, the NCSC is subordinated to the **National Coordinator for Counterterrorism and Security** (*Nationaal Coördinator Terrorismebestrijding en Veiligheid*, NCTV) of the Ministry of Security and Justice,[61] thereby bringing cyber security under the umbrella of national security in the Netherlands.[62] It consists of a director and three teams for incident response, knowledge services, and development[63] and is situated within the Directorate of Cyber Security of the Ministry of Security and Justice.[64] The Directorate also contains a Policy Division responsible for the development of cyber security policies and strategies.[65]

In order to ensure that the NCSC follows the priorities of both the public and private sectors, a governance board consisting of representatives of both sectors was to be set up in 2014.[66] The board will act as a consulting body without official powers, while responsibility for the annual programme of the NCSC remains with the Minister of Security and Justice.

In 2010 an **ICT Response Board** (IRB) was set up, now a permanent organisational entity within the NCSC. The IRB is a public-private partnership engaging telecommunications companies, energy suppliers, banks and government bodies. It is activated in the event of major ICT disruptions and has the task to advise national crisis management bodies on mitigation measures.[67]

The NCSC relies on collaboration with the public and private sectors, including academia.[68] It draws from their collective knowledge and expertise and targets its analysis and products to both these audiences.[69] The

[56] CSAN (n 27) 9.
[57] GOVCERT.NL was established in 2002. GOVCERT.NL, 'Operational Framework NCSC-NL.' Version 28, 2011 <https://www.ncsc.nl/binaries/content/documents/ncsc-en/organisation/about-the-ncsc/operational-framework/1/Operational%2BFramework%2BNCSC%2BCSIRT%2B%2B28%2B11%2B2011%2B.pdf>; UNIDIR, 'The Cyber Index: International Security Trends and Realities', New York and Geneva, 2013, 37 <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>; CSAN (n 27) 9.
[58] National Cyber Security Centre, 'About The NCSC', 2014 <https://www.ncsc.nl/english/organisation/about-the-ncsc.html>; CSAN (n 27) 10, 24.
[59] CSAN (n 27) 10, 24.
[60] National Cyber Security Centre, 'Operational Framework NCSC-NL', The Hague: Ministry Of Security and Justice, Version 30, 2013 <https://www.ncsc.nl/organisatie/wat-is-het-ncsc/operational-framework.html>.
[61] National Cyber Security Centre, 'Organisation', 2014 <https://www.ncsc.nl/english/organisation/about-the-ncsc/organisation.html>.
[62] Van den Heuvel and Klein Baltink (n 44) 120.
[63] Operational Framework (n 60); Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Nieuw hoofd Nationaal Cyber Security Centrum (NCSC)', 2014 <http://www.nctv.nl/actueel/nieuws/nieuw-hoofd-nationaal-cyber-security-centrum-(ncsc).aspx?cp=126&cs=60005>.
[64] 'Nieuw hoofd Nationaal Cyber Security Centrum (NCSC)' (n 63); CSBN-2 (n 42) 2.
[65] Van den Heuvel and Klein Baltink (n 44) 120.
[66] ibid 121.
[67] CSAN (n 27) 12; National Cyber Security Centre, 'ICT Response Board', 2014 <https://www.ncsc.nl/english/services/crisis-management-reinforcement/ict-response-board.html>.
[68] Dutch National Cyber Security Centre, 'Cyber Security Assessment Netherlands (CSAN-3)', The Hague: Ministry Of Security and Justice, 2013, 2 <https://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands/>; 'Organisation' (n 61).
[69] CSAN (n 27) 9.

organisation's attention is focused on public interest, which leads it to mainly concentrate its activities on vital sectors such as energy, telecommunications, and the financial sector.[70] Accordingly, these sectors appear to be the most actively involved in the activities of the NCSC, while participants from the government include the ministries of Security and Justice, Economic Affairs, Agriculture and Innovation, the Interior and Kingdom Relations, Foreign Affairs and Defence, and also the Public Prosecution Service, the General Intelligence and Security Service (AIVD) and the National Police Services Agency (*Korps Landelijke Politiediensten*).[71]

The working model and mechanisms of public-private cooperation within the NCSC are not yet fully established, and assessment with regard to the most efficient forms of collaboration is ongoing with the involvement of stakeholders.[72]

Products and services

The NCSC product and service portfolio comprises threat and incident response, providing awareness and advice, crisis response, and a cooperation platform.[73]

With regard to threat and incident response, the NCSC serves as the central national notification and information body for ICT threats and security incidents, as well as the response coordination centre.[74] Round-the-clock incident response assistance is available to government bodies, encompassing both technical (such as malware analysis) and organisational support (incident response management, media and crisis communication). When needed, such assistance is also provided on-site.[75]

The NCSC issues threat alerts and advice on software vulnerabilities, computer virus outbreaks, and specific attacks.[76] Constant monitoring of both information sources and network traffic is employed by government organisations to maintain up-to-date threat awareness on new computer viruses and software vulnerabilities.[77] For information sources, specifically designed applications are used to monitor large numbers of information sources such as websites, social media, and notifications by trusted partners. A network of sensors and honeypots are used for network traffic monitoring, which allow NCSC to safely analyse internet-based threats and their attack vectors across government systems.[78]

Awareness and advice are supplied primarily to the central government and vital service organisations, but it is also provided to citizens, local governments and the business sector, to promote awareness and support prevention.[79] This occurs by the following means:

- *Knowledge sharing* on cyber threats, threat prevention, and response techniques, mainly with partners (both national and international). Such knowledge is shared by means including published reports, white papers, fact sheets, recommendations, guidelines and best practices, and by

[70] National Cyber Security Centre, 'Public-Private Cooperation', 2014 <https://www.ncsc.nl/english/organisation/partners/public-private.html>; National Cyber Security Centre, 'Partners', 2014 <https://www.ncsc.nl/english/organisation/partners.html>; National Cyber Security Centre, 'Knowledge and Expertise', 2014 <https://www.ncsc.nl/english/organisation/partners/knowledge-and-expertise.html>.
[71] 'Public-Private Cooperation' (n 70).
[72] ibid.
[73] 'Beschrijving producten en diensten NCSC', Nationaal Cyber Security Centrum, The Hague: Ministry Of Security and Justice, Version 1.0, 2013, 7 <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/dienstverlening/producten--en-dienstencatalogus-pdc-2013/1/NCSC%2BProducten%2Ben%2BDiensten.pdf>.
[74] CSBN-2 (n 42) 2; CSAN-3 (n 68) 2; NCSC (n 73).
[75] National Cyber Security Centre, '24/7 Assistance', 2014 <https://www.ncsc.nl/english/services/incident-response/24-7-assistance.html>.
[76] National Cyber Security Centre, 'Incident Response' <https://www.ncsc.nl/english/services/incident-response.html>.
[77] The NCSC avails the technology, but does not engage in the monitoring directly – the latter is formally done by participating government organisations in their relevant networks, from whom the NCSC then receives the relevant information.
[78] National Cyber Security Centre, 'Monitoring', 2014 <https://www.ncsc.nl/english/services/incident-response/monitoring.html>.
[79] CSBN-2 (n 42) 2; CSAN-3 (n 68) 2.

contributions at conferences.[80] Examples of such publications include the annual *Cyber Security Assessment Netherlands* (*Cyber Security Beeld Nederland*), and the *Trendrapport Cybercrime en Digitale Veiligheid*.[81] These publications are prepared for senior management in vital organisations, but the NCSC also publishes documents specifically intended for middle management, administrators, and ICT experts, e.g., a security checklist for supervisory control and data acquisition for industrial control systems.[82] Some publications – specifically guidelines for ICT security, ICT use by end users – are also made available to the public on the NCSC website (www.ncsc.nl).[83] Awareness materials are produced in other forms and distributed via other types of media as well.[84]

- *Alerting service.* The NCSC, in cooperation with the Ministry of Economic Affairs and ECP, a platform for the information society and Dutch industry, operates an online public alerting service at www.veiliginternetten.nl, where up-to-date cyber threat and incident information, awareness materials and security advice on software updates are posted for public consumption. The website is aimed at citizens and SMEs and is free of charge.[85]
- *Tailored security advice and services.* The NCSC may also provide tailored security advice and services such as penetration testing for critical infrastructure or security policy reviews in areas where private, commercially provided services do not meet the demand.[86]

The NCSC activities in crisis management are addressed in section 3.4.2 of this report. With regard to crisis preparedness, the NCSC further provides training and conducts national cyber crisis exercises.[87]

Cyber Security Assessment

One of the starting tasks which NCSS 2011 instigated was the creation of a comprehensive catalogue of current ICT threats and risks, updated annually, and the identification of capacities needed to conduct threat prevention and response in a more targeted manner.[88] The report built upon earlier periodic assessments on trends in cybercrime and digital security, which had been conducted since 2010.[89] The report is intended to provide policy makers and, increasingly, the vital sectors with insight, enabling decisions which strengthen the nation's resilience to cyber threats and improve existing cyber security programmes.[90] The initial Cyber Security Assessment Netherlands (CSBN/CSAN) was published in 2011 and subsequent releases have expanded in both scope and depth.[91] The assessment analyses various categories relating to the cyber threat landscape, including

[80] National Cyber Security Centre, 'Trend Reports', 2014 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports>; National Cyber Security Centre, 'Whitepapers', 2014 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/whitepapers.html>; National Cyber Security Centre, 'Factsheets', 2014 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/factsheets>; National Cyber Security Centre, 'Knowledge Sharing', 2014 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing>.
[81] National Cyber Security Centre, 'Expertise & Advice', 2014 <https://www.ncsc.nl/english/services/expertise-advice>.
[82] 'Expertise & Advice' (n 81); CSAN (n 27); 'The Cyber Index: International Security Trends and Realities' (n 57) 37.
[83] 'Expertise & Advice' (n 81).
[84] National Cyber Security Centre, 'Security Advisory', 2014 <https://www.ncsc.nl/english/services/incident-response/security-advisory.html>.
[85] National Cyber Security Centre, 'Over Deze Website', 2014 <https://www.waarschuwingsdienst.nl/Over+deze+website>; Veilig internetten, 'Over veiliginternetten.nl', 2014 <https://veiliginternetten.nl/uitleg/>.
[86] National Cyber Security Centre, 'Tailored Advice', 2014 <https://www.ncsc.nl/english/services/expertise-advice/tailored-advice.html>; 'Expertise & Advice' (n 81).
[87] NCSC (n 73) 11.
[88] CSAN (n 27) 9.
[89] ibid.
[90] CSBN-2 (n 42) 13; CSAN-3 (n 68) 7; CSAN (n 27) 10.
[91] CSBN-2 (n 42) 13. CSAN-3 (n 68) 7.

actors, threats, methods used, and factors of vulnerability (technical, human and organisational).[92] The document also includes an analysis on the status quo of threat resilience and mitigation measures.[93]

From the beginning, the preparation process of the CSAN has been a close cooperation between public and private parties,[94] including the police, special investigative and intelligence services, sectoral regulators and government inspectorates (telecommunications, consumer protection, healthcare), but also including private parties such as ISPs and security vendors, and national and international knowledge and research institutions.[95] The growing number of input providers and the increasing depth of their contribution can be seen in the subsequent reports.[96]

The Cyber Security Assessment is presented by the Minister of Security and Justice to the Cabinet, the Cyber Security Council and the Lower House of Parliament; a public version is presented to contacts and interested parties and published on the website of the NCSC.[97]

3.3. Military cyber defence capabilities

The Netherlands has explicitly communicated a proactive approach towards building up cyber operational capabilities in its Armed Forces. As expressed in the Defence Minister's accompanying letter to the 2012 Defence Cyber Strategy, the Netherlands considers cyberspace a fifth domain for military operations alongside air, sea, land, and space, and digital assets are foreseen to become an integral part of military operations.[98] For that reason the Defence Cyber Strategy lays out six focal areas for developing and strengthening the cyber capabilities of the Dutch Ministry of Defence and the Netherlands Armed Forces in a comprehensive approach: defence, offence, intelligence, adaptiveness and innovation, and cooperation (see section 2.3).[99]

3.3.1. Resilience

The **Joint Information Management Command** (*Joint InformatieVoorzienings Commando*, JIVC), operational since 2013, is responsible for ensuring the resilience of the networks and systems of the defence organisation.[100] The **Defence Computer Emergency Response Team** (DefCERT), fully operational with an expanded capacity since 2012, is a part of the JIMC and holds the responsibility for the security of the defence main networks.[101]

The task of the DefCERT is to supervise and ensure the reliability and unhindered functioning of information systems in support of military operations.[102] To that end, the DefCERT is operational around the clock and

[92] CSAN (n 27).
[93] CSBN-2 (n 42) 13.
[94] CSAN (n 27) 15.
[95] ibid 9.
[96] Including the Dutch ministries, the Dutch Defence Intelligence and Security Service (MIVD), the General Intelligence and Security Service (AIVD), National High Tech Crime Unit (NHTCU) of the Dutch police, the National Public Prosecution Service, Authority for Consumers and Markets (ACM), the Dutch Forensic Institute (NFI), Statistics Netherlands (CBS), members of the Information Sharing and Analysis Centres (ISACs), Dutch ICT sector (Nederland ICT), Internet Domain Registration Foundation (SIDN), the Confederation of Netherlands Industry and Employers (VNO-NCW), the Dutch Banking Association (NVB), the National Coordinator for Security and Counterterrorism (NCTV), academic institutions including universities, and individual experts from the cyber security workplace. CSBN-2 (n 42) 2.
[97] ibid 7.
[98] 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 4.
[99] ibid 6.
[100] Ministry of Defence, 'Defence Cyber Strategy', 2014 <http://www.defensie.nl/english/topics/cyber-security/contents/defence-cyber-strategy>; 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 4.
[101] CSAN-3 (n 68) 40; Verheid.nl, 'Brief van de minister van defensie', Nr. 164, 2010 <https://zoek.officielebekendmakingen.nl/kst-26643-164.html>.
[102] CSAN-3 (n 68) 40.

carries out threat and vulnerability assessment, advising the Armed Forces on security measures.[103] DefCERT may also support civil authorities in the coordination of cyber threat response.[104] DefCERT has concluded a memorandum of understanding with the NCSC to formalise the intensive cooperation regarding information exchange and mutual support.

As of 2013, the DefCERT's capabilities were to be further expanded by expertise in industrial control systems (ICS) and SCADA systems in order to strengthen the protection of arms and sensor systems.[105]

3.3.2. Cyber operational capabilities

The Defence Cyber Strategy emphasises the need to 'invest substantially' to strengthening cyber capabilities in order to make operational cyber capabilities an integral part of the overall military capability of the Armed Forces.[106] Between 2011 and 2015, €50 million were allocated to implementing the cyber security strategy.[107]

A military Task Force Cyber was set up in January 2012 to establish the capability to apply cyber in military operations, including offensive capacity.[108] The unit was tasked with defining a doctrine for operations in cyberspace, developing deployment scenarios, and identifying effects and consequences of offensive assets.[109] Task Force Cyber was also intended to coordinate cyber operations, cyber defence, and cyber intelligence within military operations in cyberspace.[110] The Section of Operations of the Task Force was engaged with the development of the Netherlands Defence Cyber Doctrine, the development of a standard operating procedure for cyber incidents, and the creation and development of cyber operational capacity. In addition, the Task Force was also responsible for arranging training and education in cyber and for providing learning environments.[111]

The Task Force Cyber completed its activity with the creation of the joint **Defence Cyber Command** in September 2014. The newly launched Cyber Command is the overarching lead for the comprehensive cyber approach in the Dutch Armed Forces taking over from the Cyber Task Force. It incorporates cyber capabilities from all four Services (army, navy, air force, and military police) under the single-service management of the Royal Netherlands Army.[112]

The Defence Cyber Command will have a threefold focus on defence, intelligence and offence.[113] It is expected to ensure the deployment readiness of offensive cyber capabilities in military operations by 2015.[114] Offensive cyber capabilities will be administered under the responsibility of the Chief of Defence (CDS).[115]

---

[103] Ministerie van Defensie. 'Defensie Computer Emergency Response Team' <http://www.defensie.nl/onderwerpen/cyber-security/inhoud/defcert>; CSAN-3 (n 68) 40.
[104] 'Defensie Computer Emergency Response Team' (n 103).
[105] CSAN-3 (n 68) 40.
[106] 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 8.
[107] Ministerie van Defensie, 'Taskforce Cyber komt van de grond', Defensiekrant, nummer 38, 2011, 1 <http://www.defensie.nl/binaries/defensie/documenten/magazines/2011/11/10/defensiekrant-nr.-38-2011/defensiekrant-2011-38.pdf>.
[108] CSAN-3 (n 68) 40; 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 11; 'Taskforce Cyber komt van de grond' (n 107) 1.
[109] 'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace' (n 34) 11.
[110] T. A. Middendorp, 'Modernising The Dutch Armed Forces', keynote speech at the Future Force Conference, 2013 <http://www.defensie.nl/binaries/defensie/documenten/toespraken/2013/11/28/toespraak-cds-bij-de-future-force-conference-engels/toespraak-cds-bij-de-future-force-conference-engels.pdf>.
[111] Ministerie van Defensie, Elnt Joost Ploegmakers, 'Met 'cyber'-zelfvertrouwen achter de computer', Defensiekrant, nummer 32, 2012, 3 <http://www.defensie.nl/binaries/defensie/documenten/magazines/2012/10/25/defensiekrant-nr.-32-2012/defensiekrant-2012-32.pdf>; CSAN-3 (n 68) 40.
[112] 'Taskforce Cyber komt van de grond' (n 107) 1; CSAN-3 (n 68) 40. The initially planned launch date of 2015 was brought forward to 2014.
[113] Ministry of Defence, 'Cyber Command', 2014 <http://www.defensie.nl/english/topics/cyber-security/contents/cyber-command>.
[114] Defence Cyber Strategy (n 34) 11; CSAN-3 (n 68) 40.
[115] CSAN-3 (n 68) 40.

3.4. Cyber intelligence

Owing to the national understanding of cyberspace as a military domain, the role of the **Netherlands Defence Intelligence and Security Service** (*Militaire Inlichtingen- en Veiligheidsdienst*[116], DISS) has been expanded.[117] Alongside the regular mandate to provide intelligence and security information to the Ministry of Defence and the Netherlands Armed Forces,[118] DISS is further tasked with the gathering and analysis of militarily relevant information in Computer Network Defence (threat prevention and detection), Computer Network Exploitation (strengthening the intelligence position in the digital domain, *inter alia* in support of military operations) and with participating in developing a Computer Network Attack (CNA) capability in the Armed Forces.[119]

According to the Netherlands' Defence White Paper, the cyber intelligence capacity of the DISS will be strengthened.[120] Its partnership with the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst*[121], GISS), which focuses on domestic non-military threats to national security[122] has recently been upgraded by bundling the signals intelligence (SIGINT) and cyber components of GISS and DISS into a new **Joint Sigint Cyber Unit** (JSCU) in June 2014.[123] Rather than an independent entity, the JSCU is a support unit of the DISS and GISS, where both retain joint management and funding.[124] The JSCU has the purpose of improving intelligence capability by pooling cyber expertise and information of the DISS and GISS, strengthening innovation, and improving the international position of the two agencies.[125] Within the joint unit, the services are entitled to provide each other with technical and other forms of support, but each retains its distinct legal responsibilities and powers under law (Intelligence and Security Services Act 2002) and provide personnel to the JSCU.[126] The unit will be governed by an Executive Board consisting of the Secretaries-General of the Ministry of General Affairs (chair), the Interior and Kingdom Relations, and Defence.[127] The DISS is directly subordinated to the Secretary-General of the Ministry of Defence.[128]

3.5. Cyber aspects of crisis management

3.5.1. Cyber crisis prevention

Threats to national security are addressed in the National Safety and Security Strategy (*Programma Nationale Veiligheid* 2007), which examines all threats against the vital interests of society in a single framework, encompassing both prevention and management.[129] The Ministry of Interior and Kingdom Relations is

[116] Dutch abbreviation MIVD.
[117] CSAN-3 (n 68) 40.
[118] Ministry of Defence, 'Organisation', 2014 <http://www.defensie.nl/english/organisation>; Ministry of Defence, 'Central Staff', 2014 <http://www.defensie.nl/english/organisation/central-staff>.
[119] Ministerie van Defensie, 'Jaarverslag Militaire Inlichtingen- en Veiligheidsdienst 2013', 2013, 21-23 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/jaarverslagen/2014/04/23/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2013/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2013.pdf>; CSAN-3 (n 68).
[120] Ministerie van Defensie, 'Aanvulling op de nota 'In het belang van Nederland'', 2013, 25 <http://www.defensie.nl/documenten/beleidsnotas/2013/10/25/aanvulling-op-de-nota-in-het-belang-van-nederland>.
[121] Dutch abbreviation AIVD.
[122] 'Jaarverslag Militaire Inlichtingen- en Veiligheidsdienst 2013' (n 119); Ministerie van Defensie, 'Militaire Inlichtingen- en Veiligheidsdienst' <http://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd>.
[123] Ministerie van Defensie, 'Convenant Joint Sigint Cyber Unit (JSCU)', 2014 <http://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu/kamerbrief+en+convenant+gecombineerd.pdf>.
[124] ibid.
[125] ibid.
[126] Ibid; Ministerie van Defensie, 'AIVD en MIVD slaan handen ineen tegen cyberdreigingen', 2014 <http://www.defensie.nl/onderwerpen/cyber-security/nieuws/2014/07/03/aivd-en-mivd-slaan-handen-ineen-tegen-cyberdreigingen>.
[127] ibid.
[128] 'Organisation' (n 118); 'Central Staff' (n 118).
[129] Government of the Netherlands, 'National Security' <http://www.government.nl/issues/crisis-national-security-and-terrorism/national-security>; 'Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security

responsible for comprehensive risk management in central government,[130] while the **National Coordinator for Counterterrorism and Security** (NCTV), part of the Ministry of Security and Justice, is responsible for coordination of the national crisis and disaster preparedness and response.[131] The NCTV also has cyber security in its portfolio.[132] The highest level of strategic policy planning and inter–ministerial policy coordination with regard to crisis management occurs within the Netherlands Government Cabinet.[133]

The National Safety and Security Strategy employs a three-phase security method: (1) a government-wide all-hazards risk assessment phase; (2) a strategic planning phase consisting of capability analysis of existing and required resources; and (3) a follow-up stage, monitoring the measures and responsibilities for reinforcing national safety and security.[134] The risk assessment process relies on the development of relevant risk scenarios which consider a certain incident's likelihood, potential impact, and particular resources and measures for prevention and mitigation.[135] The findings of this process are meant to provide policy makers with insight into the potential risks and assist in specifying capability implications, formulating policy, and defining priorities for disaster and threat preparedness.[136]

In support of the implementation of the National Safety and Security method, the Ministry of Security and Justice has published guidelines, defined with the participation of a group of experts from government, research institutes and the business sector.[137] Findings of the assessment are periodically published in the National Risk Assessment report.

Since 2007, forty-seven scenarios linked to seven threat themes have been developed and scored for likelihood and impact using this methodology.[138] The threat of ICT breakdowns have been analysed in several scenarios, including malicious ICT disruption in critical sectors, IP network failure, internet exchange failure, cyber conflict, cyber espionage of sensitive economically relevant information, and cyber hacktivism.[139]

The National Risk Assessments are developed by the Network of Analysts for National Security (ANV) for the National Steering Committee for National Safety and Security (SNV), which is a knowledge network consisting of a permanent core and an extended network of knowledge institutions, services, private companies, research

---

Strategy of the Netherlands', The Hague: The Ministry of Security and Justice, 2009, 11 <http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf>; Erik Pruyt and Diederik Wijnmalen, 'National Risk Assessment In The Netherlands: A Multi-Criteria Decision Analysis Approach', 133-143. In Matthias Ehrgott *et al*, 'Multiple Criteria Decision Making For Sustainable Energy and Transportation Systems: Proceedings Of The 19th International Conference On Multiple Criteria Decision Making, Auckland, New Zealand, 7th - 12th January 2008', Springer Science & Business Media, Vol. 634 of Lecture Notes in Economics and Mathematical Systems, 2010.

[130] OECD, 'Innovation In Country Risk Management', 2009, 10 <http://www.oecd.org/futures/ifppublicationsandstudies.htm>.

[131] Rijksoverheid, 'Crises en rampen voorkomen', 2014 <http://www.rijksoverheid.nl/onderwerpen/veiligheid-en-terrorismebestrijding/crises-en-rampen-voorkomen>.

[132] 'Crises en rampen voorkomen' (n 131).

[133] 'Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands' (n 129) 13.

[134] ibid 11-12; 'National Risk Assessment In The Netherlands: A Multi-Criteria Decision Analysis Approach' (n 129).

[135] 'Using National Risk Assessment To Develop Risk Management Capabilities At The Country Level' , IRGC Workshop held at the OECD Headquarters, Paris, 2012, 2 <http://www.irgc.org/wp-content/uploads/2013/02/IRGC_12December2012_workshop_15Feb.pdf>; M. G. Mennen (Ed), 'National Risk Assessment 2011', National Institute for Public Health and the Environment (RIVM), 2013, 9 <https://english.nctv.nl/Images/national-risk-assessment-2011_tcm92-538995.pdf>.

[136] 'National Risk Assessment 2011' (n 135) 9.

[137] 'Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands' (n 129).

[138] 'National Risk Assessment 2011' (n 135) 9, 11; Verheid.nl, 'Strategie Nationale Veiligheid -Bevindingenrapportage-', Kamerstuk, 2013, 6-7 <https://zoek.officielebekendmakingen.nl/blg-262755>.

[139] 'National Risk Assessment 2011' (n 135) 11-12, 23-25; 'National Security' (n 129); 'Strategie Nationale Veiligheid - Bevindingenrapportage-' (n 138); Verheid.nl, 'Strategie Nationale Veiligheid Bevindingenrapportage', Kamerstuk, 2012 <https://zoek.officielebekendmakingen.nl/blg-171866>; Verheid.nl, Nationale Risicobeoordeling Bevindingenrapportage 2010', Kamerstuk, 2011 <https://zoek.officielebekendmakingen.nl/blg-101376>.

agencies, and consultancy firms.[140] All government departments are involved in the capabilities assessment phase. While this facilitates comprehensive insight into the state of resiliency for various threats, it also makes the entire process remarkably time-consuming.[141]

Critical infrastructure protection in general falls within the responsibility of the Netherlands Ministry of Security and Justice.[142] A Critical Infrastructure Strategic Consultative Body (*Strategisch Overleg Vitale Infrastructuur,* SOVI) was established by the Ministry of the Interior and Kingdom Relations in 2006. It comprises members from the public and business sectors and has an initiating and monitoring role in critical infrastructure protection at strategic level, including the mapping of vulnerabilities and inter-dependencies, both risk and crisis management.[143] Furthermore, there is close cooperation among public bodies, specifically emergency and intelligence services, and private enterprise in critical infrastructure protection. For example, the National Coordinator for Counterterrorism and Security (NCTV), the GISS and the police all provide training on threat identification.[144]

3.5.2. Crisis management

Crisis and disaster management is directed by a disaster management team, consisting of relevant public bodies under the responsibility of the Ministry of Security and Justice.[145] The **National Cyber Security Centre** has an upgraded mandate in a cyber crisis (that is, in the event that cyber incidents have a disruptive effect on society), whereupon NCSC becomes part of the national crisis structure. Cyber crisis responses are not specifically differentiated from NCSC's regular tasking, involving the gathering of cyber threat information, as well as information exchange, awareness and advice, but the focus and resources of the NCSC will be prioritised toward crisis management, while other tasks will be scaled back to a functional minimum.[146] The NCSC will then primarily bear an operational coordinating role.[147]

In case of a cyber crisis, the **ICT Response Board** (see section 3.2.1) will be activated as needed and will take responsibility for 'conceptualisation, interpretation and advice', advising the national crisis management structures.[148] The advice can also be used by the private parties of the IRB, and the capacities of the partners involved in the IRB can also be used.[149] In practice, the IRB was used during the *DigiNotar*[150] incident.

The NCSC may also give advice in the event of an imminent crisis or in case of the detection of major vulnerabilities.[151]

---

[140] 'National Risk Assessment 2011' (n 135) 9.
[141] 'Innovation In Country Risk Management' (n 130) 41.
[142] Government of the Netherlands, 'Protecting Critical Infrastructure' <http://www.government.nl/issues/crisis-national-security-and-terrorism/protecting-critical-infrastructure>.
[143] '5 Vragen Over Het Strategisch Overleg Vitale Infrastructuur (SOVI)', Ministerie van binnenlandse zaken en koninkrijksrelaties, 2010 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi/5vragenoversovi-1.pdf>.
[144] 'Protecting Critical Infrastructure' (n 142).
[145] Government of the Netherlands, 'Who Does What In A Disaster' <http://www.government.nl/issues/crisis-national-security-and-terrorism/who-does-what-in-a-disaster>.
[146] National Cyber Security Centre, 'Coordination Durning Crisis', 2014 <https://www.ncsc.nl/english/services/crisis-management-reinforcement/coordination-during-crisis.html>.
[147] Van den Heuvel and Klein Baltink (n 44) 120.
[148] 'ICT Response Board' (n 67).
[149] 'ICT Response Board' (n 67); 'Coordination Durning Crisis' (n 146).
[150] DigiNotar was a Dutch certificate authority whose systems were breached, resulting in the issuing of fraudulent SSL certificates. The intrusion was discovered in August 2011, after which the Dutch government took over operational management of DigiNotar's systems. GOVCERT.NL, 'Factsheet FS 2011-06. Fraudulently Issued Security Certificate Discovered', Version 2.2, 2011 <https://www.ncsc.nl/binaries/content/documents/ncsc-en/services/expertise-advice/knowledge-sharing/factsheets/factsheet-fraudulently-issued-security-certificate-discovered/1/Factsheet%2BFraudulently%2Bissued%2Bsecurity%2Bcertificate%2Bdiscovered.pdf>.
[151] CSAN (n 27) 19.

References

'5 Vragen Over Het Strategisch Overleg Vitale Infrastructuur (SOVI)', Ministerie van binnenlandse zaken en koninkrijksrelaties, 2010 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2009/06/23/5-vragen-over-het-strategisch-overleg-vitale-infrastructuur-sovi/5vragenoversovi-1.pdf>.

Amsterdam Internet Exchange, 'About AMS-IX', 2014 <https://ams-ix.net/about/about-ams-ix>.

'Beschrijving producten en diensten NCSC', Nationaal Cyber Security Centrum, The Hague: Ministry Of Security and Justice, Version 1.0, 2013 <https://www.ncsc.nl/binaries/content/documents/ncsc-nl/dienstverlening/producten--en-dienstencatalogus-pdc-2013/1/NCSC%2BProducten%2Ben%2BDiensten.pdf>.

Binnenlands Bestuur, 'Potentie Overheidscloud Zit Vooral In Shared Services', 2013 <http://www.binnenlandsbestuur.nl/digitaal/partners/cgi/potentie-overheidscloud-zit-vooral-in-shared.9161777.lynkx>.

Capgemini, 'Online Availability Of Public Services: How Is Europe Progressing? ', European Commission, Directorate General for Information Society and Media, 2005.

Capgemini, Sogeti, IDC, RAND Europe and the Danish Technological Institute, 'Digitizing Public Services In Europe: Putting Ambition Into Action. 9th Benchmark Measurement', European Commission, Directorate General for Information Society and Media, 2010.

Data Center Map, 'Colocation The Netherlands', 2014 <http://www.datacentermap.com/the-netherlands/>.

Deloitte, 'Digital Infrastructure In The Netherlands – The Third Mainport', 2013 <http://ecp.nl/item/3937>.

DigiD, 'About DigiD' <https://www.digid.nl/en/about-digid/>; DigiD, 'Wie Doen Mee?' <https://www.digid.nl/nl/over-digid/wie-doen-mee/>.

Dijk, Jan van et al, 'E-Services For Citizens: The Dutch Usage Case', Electronic Government, 2007, Vol. 4656, 155-166. In Maria A. Wimmer et al, 'Electronic Goverment: 6th International Conference, EGOV 2007, Regensburg, Germany, September 3-7, 2007, Proceedings', Springer Science & Business Media, 2007 <http://dx.doi.org/10.1007/978-3-540-74444-3_14>.

Dutch National Cyber Security Centre, 'Cyber Security Assessment Netherlands (CSAN-3)', The Hague: Ministry Of Security and Justice, 2013 <https://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands/>.

Dutch National Cyber Security Centre, 'The National Cyber Security Strategy (NCSS): Strength Through Cooperation', The Hague: Ministry of Security and Justice, 2011 <https://www.ncsc.nl/english/current-topics/news/national-cyber-security-strategy-launched.html>.

eGovernment Factsheets. 'eGovernment in The Netherlands', Edition 16.0, 2014 <https://joinup.ec.europa.eu/sites/default/files/55/a8/5e/eGov%20in%20NL%20-%20April%202014%20-%20v.16.pdf>.

EU Digital Agenda, 'Country Ranking Table, On A Thematic Group Of Indicators — Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"ref-area":"NL","time-period":"2013"}>.

Google Europe Blog, 'Expanding Our Data Centres In Europe', 2014 <http://googlepolicyeurope.blogspot.be/2014/09/expanding-our-data-centres-in-europe.html>.

GOVCERT.NL. Dutch National Cyber Security Centre. 'Cyber Security Assessment Netherlands (CSAN)', The Hague: Ministry of Security and Justice, 2011 <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/trend-reports/cyber-security-report-2011.html>.

GOVCERT.NL, 'Factsheet FS 2011-06. Fraudulently Issued Security Certificate Discovered', Version 2.2, 2011 <https://www.ncsc.nl/binaries/content/documents/ncsc-en/services/expertise-advice/knowledge-sharing/factsheets/factsheet-fraudulently-issued-security-certificate-discovered/1/Factsheet%2BFraudulently%2Bissued%2Bsecurity%2Bcertificate%2Bdiscovered.pdf>.

GOVCERT.NL, 'Operational Framework NCSC-NL.' Version 28, 2011 <https://www.ncsc.nl/binaries/content/documents/ncsc-en/organisation/about-the-ncsc/operational-framework/1/Operational%2BFramework%2BNCSC%2BCSIRT%2B%2B28%2B11%2B2011%2B.pdf>.

Government of the Netherlands <http://www.government.nl>.

Heuvel, Elly van den and Gerben Klein Baltink, 'Coordination And Cooperation In Cyber Network Defense: The Dutch Efforts To Prevent and Respond'. In M. E. Hathaway (ed), 'Best Practices in Computer Network Defense: Incident Detection and Response', IOS Press, 2014.

Interxion, 'Netherlands', 2014 <http://www.interxion.com/locations/netherlands/>.

Mennen, M. G. (Ed), 'National Risk Assessment 2011', National Institute for Public Health and the Environment (RIVM), 2013, 9 <https://english.nctv.nl/Images/national-risk-assessment-2011_tcm92-538995.pdf>.

Middendorp, T. A., 'Modernising The Dutch Armed Forces', keynote speech at the Future Force Conference, 2013 <http://www.defensie.nl/binaries/defensie/documenten/toespraken/2013/11/28/toespraak-cds-bij-de-future-force-conference-engels/toespraak-cds-bij-de-future-force-conference-engels.pdf>.

Mijnoverheid, 'Uw persoonlijke website voor overheidszaken' <https://mijn.overheid.nl/?r=1>.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Betreft i-strategie rijk', 2011 <http://www.nationaalarchief.nl/sites/default/files/docs/nieuws/kamerbrief-informatiseringstrategie-rijk.pdf>.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 'Visiebrief digitale overheid 2017', 2013 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017/visiebrief-digitale-overheid-2017.pdf>.

Ministerie van Defensie <http://www.defensie.nl>.

Ministerie van Defensie, 'Convenant Joint Sigint Cyber Unit (JSCU)', 2014 <http://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu/kamerbrief+en+convenant+gecombineerd.pdf>.

Ministerie van Defensie, Elnt Joost Ploegmakers, 'Met ‘cyber’-zelfvertrouwen achter de computer', Defensiekrant, nummer 32, 2012 <http://www.defensie.nl/binaries/defensie/documenten/magazines/2012/10/25/defensiekrant-nr.-32-2012/defensiekrant-2012-32.pdf>.

Ministerie van Defensie, 'Jaarverslag Militaire Inlichtingen- en Veiligheidsdienst 2013', 2013 <http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/jaarverslagen/2014/04/23/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2013/jaarverslag-militaire-inlichtingen-en-veiligheidsdienst-2013.pdf>.

Ministerie van Defensie, 'Taskforce Cyber komt van de grond', Defensiekrant, nummer 38, 2011 <http://www.defensie.nl/binaries/defensie/documenten/magazines/2011/11/10/defensiekrant-nr.-38-2011/defensiekrant-2011-38.pdf>.

Ministry of Defence <http://www.defensie.nl>.

Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Nieuw hoofd Nationaal Cyber Security Centrum (NCSC)', 2014 <http://www.nctv.nl/actueel/nieuws/nieuw-hoofd-nationaal-cyber-security-centrum-(ncsc).aspx?cp=126&cs=60005>.

National Coordinator for Security and Counterterrorism (NCTb), 'Cyber Security Council Invested', 2011 <http://english.nctb.nl/currenttopics/press_releases/2011/press-release-110630.aspx>.

National Cyber Security Centre <https://www.ncsc.nl/english>.

National Cyber Security Centre, 'Cyber Security Assessment Netherlands (CSBN-2)', The Hague: Ministry Of Security and Justice, 2012 <https://english.nctv.nl/Images/cybersecurityassessmentnetherlands_tcm92-480116.pdf>.

National Cyber Security Centre, 'Operational Framework NCSC-NL', The Hague: Ministry Of Security and Justice, Version 30, 2013 <https://www.ncsc.nl/organisatie/wat-is-het-ncsc/operational-framework.html>.

National Cyber Security Centre, 'Over Deze Website', 2014 <https://www.waarschuwingsdienst.nl/Over+deze+website>.

'National Cyber Security Strategy (NCSS) 2: From Awareness To Capability', The Hague: Ministry of Security and Justice, 2013 <https://english.nctv.nl/Images/national-cyber-security-strategy-2_tcm92-520278.pdf>.

OECD, 'Innovation In Country Risk Management', 2009, 10 <http://www.oecd.org/futures/ifppublicationsandstudies.htm>.

Ondernemers Plein, 'Over Ondernemersplein.Nl' <http://www.ondernemersplein.nl/over-ondernemersplein/>.

Pruyt, Erik and Diederik Wijnmalen, 'National Risk Assessment In The Netherlands: A Multi-Criteria Decision Analysis Approach', 133-143. In Matthias Ehrgott et al, 'Multiple Criteria Decision Making For Sustainable Energy and Transportation Systems: Proceedings Of The 19th International Conference On Multiple Criteria Decision Making, Auckland, New Zealand, 7th - 12th January 2008', Springer Science & Business Media, Vol. 634 of Lecture Notes in Economics and Mathematical Systems, 2010.

Rijksoverheid <http://www.rijksoverheid.nl>.

'Special Eurobarometer 396 - E-Communications Household Survey', 2013 <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2629>.

TeleGeography, 'Submarine Cable Map', 2014 <http://www.submarinecablemap.com>.

'The Defence Cyber Strategy. Defence Strategy For Operating In Cyberspace', Ministry of Defence, 2012 <https://ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf>.

UNIDIR, 'The Cyber Index: International Security Trends and Realities', New York and Geneva, 2013 <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>.

United Nations Department of Economic and Social Affairs, 'United Nations E-Government Survey 2012: E-Government For The People', New York, 2012 <http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2012-Survey/unpan048065.pdf>.

'Using National Risk Assessment To Develop Risk Management Capabilities At The Country Level' , IRGC Workshop held at the OECD Headquarters, Paris, 2012, 2 <http://www.irgc.org/wp-content/uploads/2013/02/IRGC_12December2012_workshop_15Feb.pdf>.

Veilig internetten, 'Over veiliginternetten.nl', 2014 <https://veiliginternetten.nl/uitleg/>.

Verheid.nl <https://zoek.officielebekendmakingen.nl>.

'Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands', The Hague: The Ministry of Security and Justice, 2009 <http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf>.

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