THE NETHERLANDS
CYBER READINESS AT A GLANCE

Melissa Hathaway and Francesca Spidalieri

May 2017

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: *CyberReadinessIndex2.0@potomacinstitute.org*

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

This country profile was made possible through funding provided by the Dutch Government's National Coordinator for Security and Counterterrorism. The Potomac Institute for Policy Studies and the authors would like to thank the Dutch Government and other European experts who provided insights and contributions for this profile. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

THE NETHERLANDS
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

THE NETHERLANDS

CYBER READINESS AT A GLANCE

Country Population	16.9 million
Population Growth	0.4%
GDP at market prices (current $US)	$750.284 billion
GDP Growth	2%
Year Internet Introduced	1982
National Cyber Security Strategy	2011, 2013
Internet Domain	.nl
Internet users per 100 users	93.1
Fixed broadband subscriptions per 100 users	41.7
Mobile cellular subscriptions per 100 users	124

Information and Communications Technology (ICT) Development and Connectivity Standing

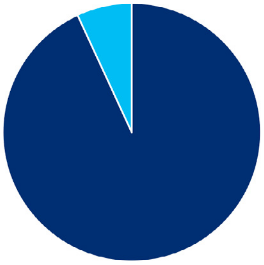
International Telecommunications Union (ITU) ICT Development Index (IDI)	8	World Economic Forum's Network Readiness Index (NRI)	6

Sources: World Bank (2015), ITU (2016), NRI (2016), and Internet Society.

INTRODUCTION

Early instantiations of Internet services, including email and a bulletin board system called USENET, were first introduced in the Netherlands by the European UNIX network (EUnet) in 1982.[1] These first connections inspired scientists at the Centrum Wiskunde & Informatica (CWI)[2] – the Netherlands' national mathematics and computer science research institute – to accelerate Internet initiatives and create the first fiber network to operate on the Transmission Control Protocol/Internet Protocol (TCP-IP) in Europe. This first Internet infrastructure, however, was not part of an overall government strategic plan for the Netherlands, rather it was a bottoms-up initiative advanced by scientists who believed in the opportunity of the Internet. CWI and its parent organization – the Netherlands Organization for Scientific Research (NWO) – began to see the enormous potential of the Internet and cultivated this nascent network, which ultimately led to the establishment of NLnet. Despite the initial lack of Internet standards that originally hindered global communications, the Netherlands established connectivity with the United States in November 1988 and later became one of the key Internet gateways for all of Europe.

Over the next decade, the Netherlands, like many other countries, recognized that telecommunications liberalization was necessary to provide universal access at lower cost to consumers. The Netherlands also saw strategic value in becoming the Internet gateway to Europe, and in the early 1990s, established the Amsterdam Internet Exchange (AMS-IX) as a not-for-profit, neutral, and independent peering organization. Today, AMS-IX interconnects more than 800 communication networks by offering professional peering services to Internet Service Providers (ISPs), international carriers, mobile operators, content providers, web hosting and cloud companies, application providers, TV broadcasters, gaming companies, and other related businesses. AMS-IX has expanded to four, and soon five continents, and is currently the world's largest Internet exchange.[3]



Netherlands Internet Penetration: 93.1%

Building on these historical foundations, and strengthened by some of the fastest and strongest broadband connections in Europe, the Netherlands has become one of the most technologically advanced and highly connected countries in the world – it ranks among the top 10 most connected countries globally. It has an Internet penetration rate of over 93 percent and more than 95 percent of households are connected to the Internet. Additionally, the Netherlands is a frontrunner in online banking with more than 80 percent uptake, and its citizens and businesses represent the fourth largest market for e-commerce in Europe.[4] The Netherlands' information communications technology (ICT) sector contributes to almost 5 percent of total Dutch gross domestic product (GDP), and the country is one of the top 10 exporters of ICT goods and telecommunication services around the world (although the global share of export of Dutch ICT services has been decreasing in recent years).[5] In 2015, it was estimated that the Dutch broader digital economy accounted for 22.9 percent or €158.01 billion (~$172.2 billion) of the total Dutch economy, and it is projected to reach 25 percent or €190.4 billion (~$207.5 billion) by 2020.[6]

The Netherlands, however, is not just an Internet gateway to Europe. Rotterdam hosts

Europe's largest port and the Amsterdam Schiphol Airport is one of the world's busiest airports for both international passengers and cargo. The government of the Netherlands understands the importance of these two other gateways of commerce (i.e., Rotterdam and Schiphol Airport) and is intensifying its industry relationships to enhance their respective security postures.[7] As such, the Netherlands recognizes that, despite its comparatively modest size and population, as the country becomes more connected and its economic future becomes more digitally dependent, it must also address cyber security and become a "safe place to do business."

Becoming "the" country to do business in is perhaps more important now than ever because the Netherlands has the opportunity to bridge the United Kingdom and Europe during the United Kingdom's transition with Europe, as a result of Britain's decision to exit the European Union (EU). The Netherlands has also the opportunity to position itself as a more politically stable country for conducting business during a time of increased populist movements throughout Europe.

The Netherlands established the foundations to realize these opportunities in its ambitious 2011-2015 digital strategy – the "Digitale Agenda." The digital strategy highlighted that the country must "make smarter use of ICTs to generate growth and prosperity, [and] boost innovation and economic growth."[8] In line with the objectives set by the 2010 European Digital Agenda – one of the seven pillars of the "Europe 2020 Strategy" – the Dutch digital strategy identified priorities and specific actions to help foster wider use of ICTs, enhance fast broadband connectivity, promote a free and open Internet, and remove "barriers to international trade on the Internet," which in turn "could result in a minimum 4 percent increase of EU GDP."[9] Following the objectives set in this digital strategy, the Netherlands sees its digital future through the lens of twin responsibilities: economic progress, underpinned by trust and resilience. Economic progress is enabled by ICT uptake, innovation, and infrastructure modernization, and embracing the Internet of Things (IoT). Yet, to achieve its growth potential, Dutch infrastructure must become more resilient, and the Internet and the transactions that take place in and through cyberspace must be secure and trusted.

The Dutch digital strategy acknowledged that the necessary prerequisites to benefit from all possibilities ICT has to offer and "increase the competitiveness of the Netherlands" are: (1) a safe, secure, and reliable ICT infrastructure; (2) "an open and accessible high-speed [Internet]" trusted by users; and (3) "a population with the digital skills needed to use ICTs." The document recognized the direct link between national security and economic well-being, and warned that "measures to address threats to the security and safety of the Internet [were necessary to] prevent a lack of trust slowing the uptake of ICTs and thus acting as a constraint on the pace of economic growth and innovation."[10] In July 2016, the Dutch government submitted a report to the Parliament indicating that many of the goals and targets from the 2011 digital strategy had been accomplished, and presented an updated 2016-2017 Digital Agenda on "innovation, trust, and acceleration." While the focus of the previous digital strategy had been predominantly on the reinforcement of prerequisites for everybody to benefit from ICTs and on the further digitization of the Dutch government (i.e., e-governance services for citizens and businesses), the 2016 updated version of the digital strategy included a comprehensive approach and a broader scope to further digitize other sectors, such as healthcare and mobility.[11] A new national digital strategy is expected to be published in 2018 by the new government and increased funding is likely to be allocated for innovation and cyber security.

Yet, the Netherlands, like many other European countries, faces high levels of cyber crime, industrial espionage, disruption of critical services, and other malicious cyber activities. In 2010, a study conducted by the Netherlands Organisation for Applied Scientific Research (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO) estimated that the Netherlands lost at least €10 billion (~$11 billion) – or 1.5 to 2 percent of its national GDP – to cyber crime.[12] (A similar estimate was published by Deloitte in April 2016, highlighting that the Netherlands' most relevant economic sectors had at least €10 billion value-at-risk to cyber crime and malicious activities.)[13] In response to the growing scope, volume, and sophistication of cyber threats, the Dutch government stated its intent to protect the value of the Netherlands' digital investments and to preserve its national and economic security. In 2010, the Parliament of the Netherlands requested the development of a National Cyber (Defense) Strategy – referred to as the Amendment Knops to create a National Cyber Strategy. As a result, the Dutch Ministry of Security and Justice coordinated a whole-of-government approach that resulted in the publication of the Netherlands' first "National Cyber Security Strategy: Success through Cooperation," in February 2011.[14]

This strategy appointed the Minister of Security and Justice as the lead for policy coordination, to be executed by the office of the National Coordinator for Security and Counterterrorism (NCTV). It also called for the establishment of a National Cyber Security Center (NCSC) reporting to the NCTV to serve as a platform for private-public partnership. Finally, the strategy advocated for the creation of a Dutch Cyber Security Council to serve as a national and strategic advisory body. The strategy was put to the test when the country faced its first known cyber crisis. The incident occurred in June 2011 at DigiNotar – a Dutch certificate authority that issued cryptographic keys to create digital (signed) certificates for "secure" communications, especially for domains owned by the Dutch government. DigiNotar's corporate network servers were successfully breached and hackers gained administrative rights to its system, which resulted in the issuing of fraudulent certificates that undermined the integrity, authenticity, and security of the Dutch government's communications.[15] DigiNotar's fraudulent certificates were used in other nations as well, calling into question the veracity of two-factor authentication. This event not only raised awareness across the entire Dutch government, but it affected citizens' trust in conducting business over the Internet or sharing information with the government. Moreover, it accelerated the creation and operationalization of the NCSC, which opened in January 2012.

Following the DigiNotar crisis, the Dutch government began revising its approach to cyber security by embracing a risk-based approach based on balancing the protection of Dutch interests with the threats to those interests and acceptable societal risks.[16] It was modeled using an incident management principle that every Dutchman knows – water management and containing the sea. After the great flood of 1953, the government launched the Delta Plan, which institutionalized a whole-of-nation approach and responsibility of every citizen to protect the Netherlands through a warning and alert system to monitor water levels and contain the sea.[17] In 2013, the Netherlands published its second strategy entitled, "National Cyber Security Strategy 2: from Awareness to Capability (NCSS2)," which expanded the country's view of cyber security beyond technology and isolated cyber incidents. The strategy tried to harness that same sense of responsibility toward water management for use with cyber security by advocating that every citizen has a responsibility to ensure the resilience of the country by preventing and containing threats coming over and through the Internet and ensuring the viability, trust, and resilience of the Internet as a platform for the free flow of goods, services, capital, and data across borders. It was a 21st century Digital Delta Plan that is both inward and outward focused.[18] It also established a triangular relationship between cyber security, economic and social growth, and freedom and privacy. This second national cyber security strategy included a 38-item action plan intended for completion by the end of 2016.

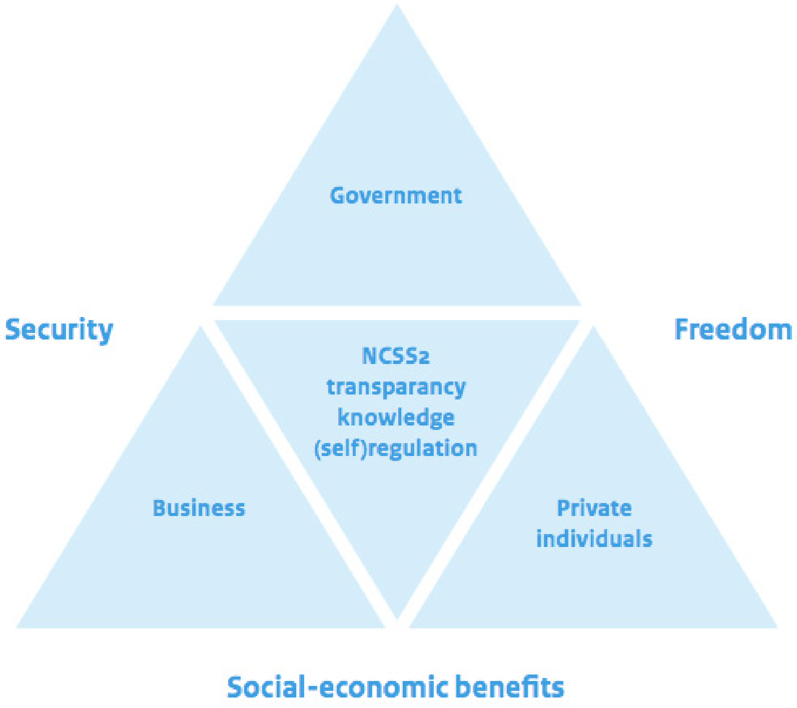


*Figure 1: "National Cyber Security Strategy (NCSS 2): from Awareness to Capability."**

Subsequent to the DigiNotar crisis and concurrently with the development of the NCSS2 strategy, the Dutch Ministry of Defense (MoD) began to discuss publicly its role in cyber defense and its plans to invest in the development of cyber warfare capabilities despite budget cuts in other areas. Building upon the intentions already detailed in the 2012 Cyber Defense Strategy, the Netherlands reiterated its intentions to develop military operational and offensive capabilities and announced the creation of a dedicated Defense Cyber Command within the Dutch MoD.[19] The standing

* *Image reprinted here with permission from the Dutch Ministry of Security and Justice.*

up of this new Command led to the development of robust capabilities based on the objectives of early detection, active defense, and, if necessary, intervention.[20] Moreover, the MoD recently established a dedicated Security Operation Center, demonstrating its operational commitment to defending the MoD and the Netherland's economy in and through cyberspace. In addition, the Dutch government has been working to ensure that cyber security is further prioritized within their intelligence and security communities, as well as striving to expand capabilities and provide additional tools and authorities to investigate and combat advanced cyber attacks. The Netherlands understands the importance to retain sufficient scope to carry out lawful, necessary, and proportional cyber operations, and is still negotiating two draft bills – one that would revise the law governing intelligence and security services and another that would grant special powers to police and other investigative services to remotely access suspects' computers without a warrant.

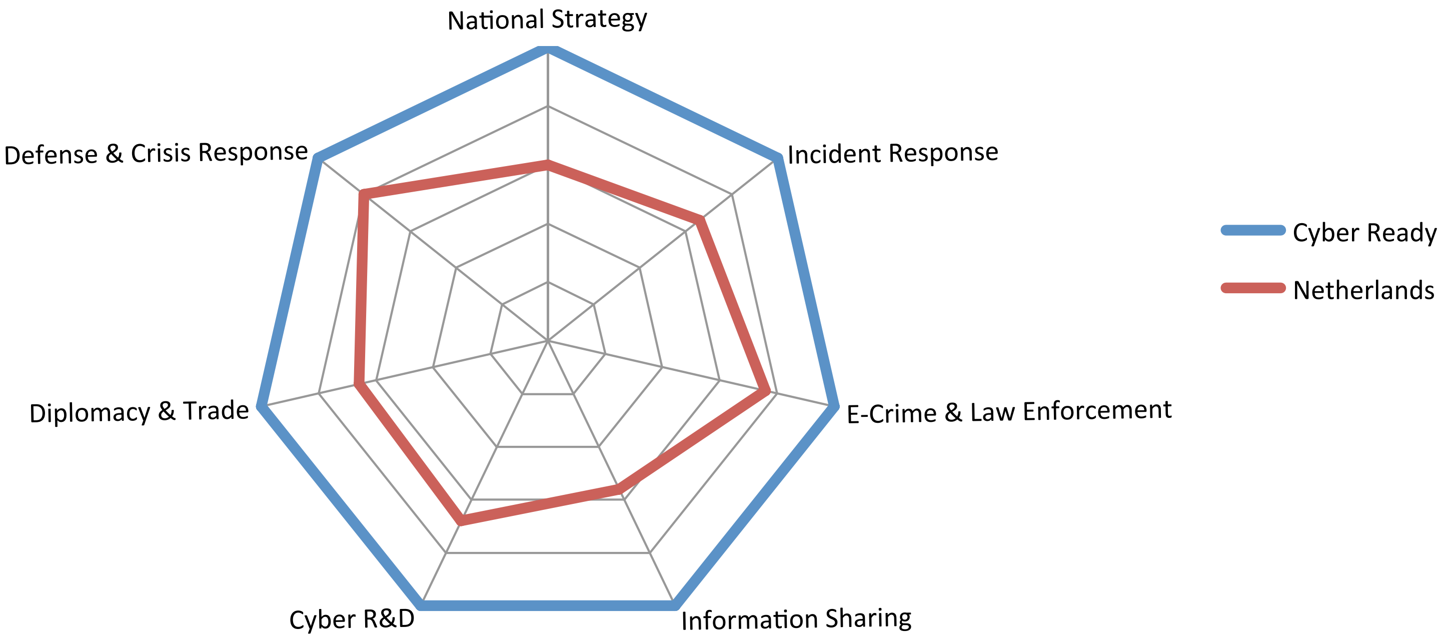
In 2015, Dutch Prime Minister Mark Rutte recognized that the country was facing "a serious cyber security challenge" and encouraged domestic and international partners, including businesses, universities, and other governments "to work together … to make sure the Internet remains free, open, and secure.… [in order to] protect our prosperity, our privacy and our quality of life."[21] Yet, despite the publication of two comprehensive national cyber security strategies, the development of a strong national cyber security architecture with military and intelligence services contributing to a whole-of-nation cyber defense, and proactive efforts to shape cyber policy discussions in multiple international fora, the Netherlands is still grappling with how to best embrace ICT technologies and IoT, while simultaneously managing the risks associated with its digital agenda and strengthening the overall cyber resilience of the nation.

The Ministry of Security and Justice, and more specifically the NCSC, have been challenged with mission integration. Currently, there are at least 20 bodies with individual and collective responsibilities for enhancing the cyber security posture of the Netherlands, but no one agency has overarching authority to ensure the national cyber security architecture is achieved. Successful outcomes rest on the famous Dutch polder model process of cooperation between the different ministries even when there may be differing views. As the cyber threat to the Netherlands continues to grow in scope, volume, and sophistication, it will be essential to accelerate civil-military cooperation and perhaps more clearly identify responsibilities.

Moreover, the Dutch government has put forward multiple plans and strategies, but often without allocating the necessary resources (e.g., money, materiel, and people) for the implementation of the initiatives that it deems important. In fact, the Netherlands continues to spend less than 0.01 percent of its GDP on cyber security – considerably less (as a portion of national GDP) than other developed countries like the United States, United Kingdom, Australia, Germany, and France.[22] Moreover, many organizations in both the public and private sectors are still struggling with how to replace complex and outdated legacy systems – upon which critical services depend – in a cost-effective way. And many other organizations still lack a sufficiently qualified cyber security workforce to tackle cyber threats. A shift in mind-set is needed, from knowing the risks and opportunities afforded by ICT innovations and Internet uptake to managing those risks and investing in their security appropriately, so that the country can continue to reap the benefits associated with the digital economy and reach the ambitious goals set forth in its strategies.

The March 2017 national elections confirmed that four parties will be required to form a coalition with a majority (76 seats). It is probable that the incumbent Prime Minister Mark Rutte will retain his position in the new government. While immigration, integration, and national identity were the central issues in the electoral campaign, all four political parties of the forming coalition recognized cyber security as an important issue for national security and economic prosperity. The new government should provide the Netherlands with a renewed opportunity to update the Dutch cyber security strategy and strengthen the overall cyber security capacity and resilience of the country. It will also test whether the Netherlands is prepared to enhance its position as the gateway to Europe and become "the" country to do business in while navigating its long-standing relationship with the United Kingdom and maintaining a broader leadership role in Europe.

The Cyber Readiness Index (CRI) 2.0 methodology has been employed to evaluate the Netherlands' current preparedness levels for cyber risks.[23] This analysis provides an actionable blueprint for the Netherlands to better understand its Internet-infrastructure dependencies and vulnerabilities and to assess the country's commitment and maturity in closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows:



The Netherlands Cyber Readiness Assessment (2017)

1. NATIONAL STRATEGY

The 1st Dutch National Cyber Security Strategy was published in 2011 and the 2nd iteration was released in 2013.

In 2011, the Dutch government responded to the increasing number of device infections, cyber crime cases, and distributed denial of service (DDoS) attacks by releasing its first "National Cyber Security Strategy: Success through Cooperation." The document acknowledged that a "safe and reliable ICT" was fundamental "for the prosperity and well-being" of Dutch society and should be a "catalyst for further sustainable economic growth." The strategy also articulated the country's ambitious goal of becoming the "Digital Gateway to Europe."[24]

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, and advocating that any proposed measures taken toward ICT security be necessary and proportionate.[25] To achieve these goals, it laid out five basic principles for the country to follow: (1) linking and reinforcing existing initiatives and avoiding duplication of efforts; (2) taking steps to strengthen private-public partnerships; (3) promoting individual responsibility to secure one's own ICT systems and networks and prevent security risks for others; (4) pursuing international cooperation; and (5) striking a balance between self-regulation and legislation. It also called for the publication of annual national threat and risk analyses – known as Cyber Security Assessment Netherlands (CSAN) to remain abreast of current trends and challenges facing the country. Moreover, the strategy called for the creation of a National Cyber Security Center to oversee the coordination of whole-of-nation initiatives and a Dutch Cyber Security Council to serve as a national and strategic advisory body. The strategy's action plan set out a number of priorities, including reinforcing the country's resilience against ICT disruptions and cyber attacks; developing a capacity for rapid response; intensifying law enforcement capabilities; increasing cyber security awareness across society; and vigorously pursuing research, development, and education.

Despite the long list of action lines, however, the strategy did not allocate dedicated funding for these initiatives in 2011. Indeed, it stated that the activities described would "be dealt with within the existing budgets."[26] Some institutions did re-allocate funds within their existing budgets to provide for capabilities and personnel, and grow existing initiatives. Yet, additional progress remained difficult to achieve given competing priorities and resources. Moreover, it was not until after the cyber attack on DigiNotar and other highly publicized cyber incidents[27] that the government finally inaugurated the National Cyber Security Center (National Cyber Security Centrum, (NCSC)) in January 2012 under the leadership of the Ministry of Security and Justice and the National Coordinator for Security and Counterterrorism (NCTV). The NCSC centralized cyber activities under one command and serves as a platform for private-public partnership.

Some of the activities in the 2011 strategy, in particular the launch of the CSAN annual reports and the establishment of the Dutch Cyber Security Council (Nederlandse Cyber Security Raad, CSR), accelerated a strategic understanding about cyber threats and vulnerabilities. These programs and advisors also highlighted that the Netherlands needed to alter its approach and take on a stronger, more deliberate leadership position with various actors, especially in the international arena.[28]

The CSR became operational in June 2011 and was tasked with providing strategic guidance to the Dutch Cabinet on cyber security matters and overseeing the implementation of the national cyber security strategy. This Council is a unique private-public partnership comprised of 18 members – seven from government, seven from industry, and four from the scientific community.[29] The CSR is co-chaired by the NCTV, who represents the government, and the CEO of KPN – the Netherlands largest telecommunications provider, who represents the private sector. The CSR is an independent national and strategic advisory body responsible for providing guidance to the government and private businesses on cyber threats and cyber defenses. It does not have an operational role. Rather, it advises the government on the implementation and development of the national cyber security strategy; contributes to the Dutch cyber security research agenda by highlighting future requirements for national research and development (R&D); and promotes cyber security awareness among senior leaders in the private sector through a series of board room dialogues.[30]

Building on the initiatives developed in the first national cyber security strategy, the Dutch Ministry of Security and Justice published the country's second "National Cyber Security Strategy 2: from Awareness to Capability" (NCSS 2) in 2013. The drafting process for this second strategy involved a number of different stakeholders, from the public and private sectors, academia, and civil society. The new cyber security strategy clarified the relationships between various stakeholders; encouraged private-public participation and international cooperation; asserted the government's role in establishing the necessary cyber security requirements, regulations, and standards to protect and improve the security of ICT products and services; and adopted a risk-based approach based on balancing the protection of Dutch interests with the threats to those interests and acceptable risks in society. This new approach harnessed the same sense of responsibility and risk awareness that made the 1953 Delta Plan effective and successful. This strategy created a 21st century "Digital Delta Plan," advocating for individuals, businesses, and the government to have clear responsibilities in cyber security. In fact, citizens are expected to follow basic "cyber hygiene" practices and take some responsibility for their own cyber security; businesses are expected to uphold their duty of care towards their clients and offer more secure ICT products and services; and the government should facilitate these efforts by "raising awareness among citizens, businesses, and organizations" about cyber security, improving citizens' digital skills, and increasing transparency about users' data collection and protection.

Moreover, the Dutch government declared an ambitious goal of further increasing its e-governance services delivery and "enabling all citizens and businesses to digitally and safely handle their affairs with the government by 2017."[31] Currently, the Netherlands ranks seventh in the world and fourth in Europe for e-government development and online service delivery, falling short of its goals set to be achieved by 2017.[32]

The NCSS 2 reiterated the government's commitment to creating "a safe and secure digital domain," making the Netherlands more "resilient to cyber attacks and [able to] protect its vital interests" in cyberspace, and strengthening and extending "alliances with public and private parties, both nationally and internationally." It highlighted several activities to better combat the Netherlands' cyber threat environment and achieve the right balance between security, freedom, and social-economic benefits of cyber security. The underlying fundamental principles in this strategy are: (1) "responsibilities that apply in the physical domain should also be taken in the digital domain," and (2) "(self)regulation, transparency, and knowledge development" should be at the base of every cyber security-related discussion with the various stakeholders identified in the strategy. It also showed a broader government view of cyber security beyond an isolated technical problem and placed it in the context of other foreign policy and economic issue areas like human rights, Internet freedom, privacy, economic growth and sustainable development, and innovation.[33] The strategy acknowledged the interconnections between "having a secure digital domain" and being able to take full advantage of the economic and social "opportunities offered by digitization to society," and recognized that "due to the increased complexity of, dependence on, and vulnerability of ICT-based products and services, the [country's] digital resilience to these and other cyber threats [was still] insufficient."[34]

The NCSS 2 Strategy recognized that the Netherlands' digital resilience to cyber threats was insufficient.

In addition, the NCSS 2 elevated the position of the NCSC to the "expert authority" for cyber security in the Netherlands, responsible for the digital security and cyber resilience of the country, with a focus on central government and critical infrastructure processes. Its mission was expanded to create "a safe, open, and stable information society" through three primary roles and divisions: (1) advising both public and private entities, both on request and on its own initiative, and shaping information security policies and activities (Expertise and Advisory Division); (2) serving as the central information hub and center of cyber expertise for cyber security (Market Development and Partnership Division); and (3) providing operational coordination for major ICT crisis and cyber incidents response measures for the Dutch government and critical infrastructures (Monitoring and Response Division).[35]

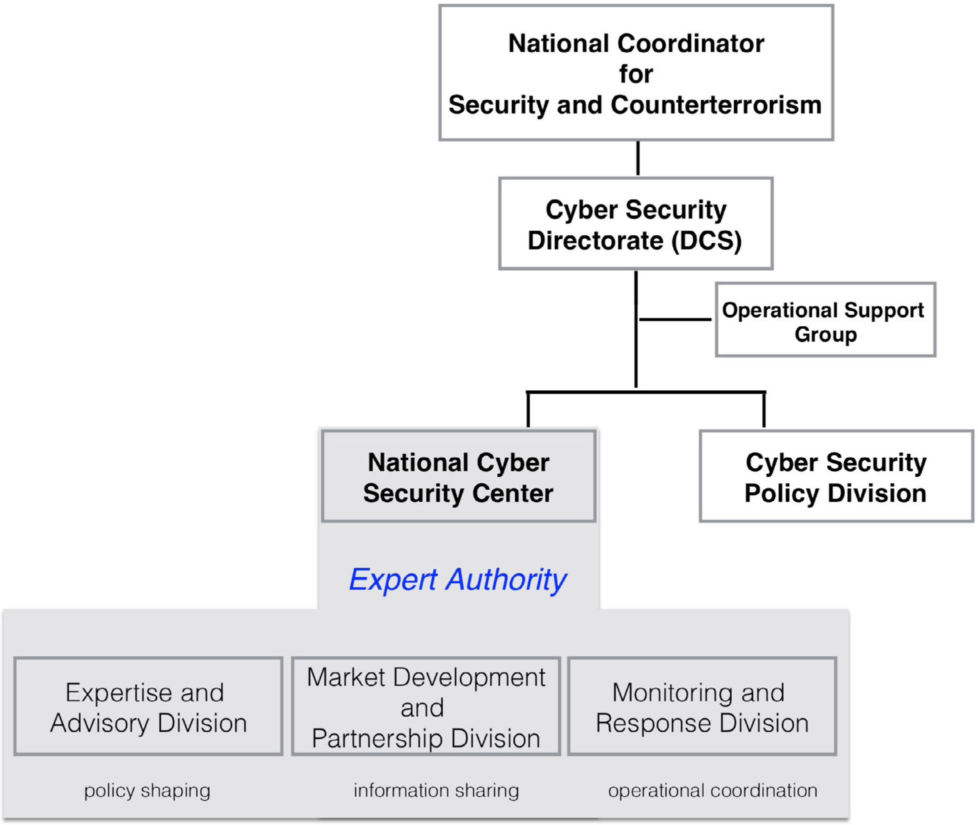

National Coordinator for Security and Counterterrorism
Cyber Security Directorate (DCS)
Operational Support Group
National Cyber Security Center
Cyber Security Policy Division
Expert Authority
Expertise and Advisory Division
Market Development and Partnership Division
Monitoring and Response Division
policy shaping
information sharing
operational coordination

Figure 2: Organizational Chart of the Netherlands National Cyber Security Center.

Organizationally, and in terms of mandate, the NCSC is a division of the Cyber Security Directorate (DCS) and sits under the authority of the National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Security and Justice. The Director of Cyber Security is also the deputy National Coordinator for Security and Counterterrorism.[36]

Yet, responsibility for cyber security does not solely rest with the Ministry of Security and Justice. This ministry and the NCSC oversee most of the cyber security-related initiatives occurring in the Netherlands but, given the decentralized form of government, they do not have the responsibility nor the mandate to direct the activities of other Ministries, such as the Ministry of Economics or the Ministry of Foreign Affairs. The NCSS 2 identified at least 20 bodies with individual and collective responsibilities for achieving the cyber security objectives outlined in the document. On the government side, these include the Dutch Ministry of Security and Justice that is responsible for coordinating interdepartmental cyber security between various civilian and military units that have cyber responsibilities; the Ministries of Interior and Kingdom Relations; Economic Affairs; Defense; Foreign Affairs; and Education, Culture and Science; and other governmental agencies like the National Police Service, and the Intelligence and Security Services. On the private sector side, the bulk of responsibilities defined in the NCSS 2 falls on the financial services and telecommunications sectors, and to providers of other critical services. Academia is also involved via the Netherlands Organisation for Scientific Research (Nederlandse Organisatie voor Wetenschappelijk Onderzoek, NWO) – an independent research council under the auspices of the Ministry of Education, Culture and Science – and through government financing of independent research organizations such as the Netherlands Organisation for Applied Scientific Research (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO). When there are this many actors working various aspects of the cyber mission space, it becomes critical to establish a whole-of-government strategy and coordination mechanism to ensure harmony of efforts.

The annex to NCSS 2 contained a detailed 2014-2016 action plan (programme) to achieve the strategic goals and long-term ambitions set forth in the strategy. The action plan itemized specific measures to be taken by established timelines and identified entities responsible for ensuring successful completion by said dates. However, even this second national cyber security strategy did not pledge any specific funds to support all the initiatives and measures discussed. Instead, it stated that "the government [would] implement the broader strategy through participation, reprioritisation, smart coalitions and an integrated approach" with all parties involved, and that the activities described would have to fall within "the scope of regular departmental budgets and the partners' budgets." Thus, it concluded "the details regarding the implementation of the actions stated in the annexes" could only be decided "in consultation and/or coopera-

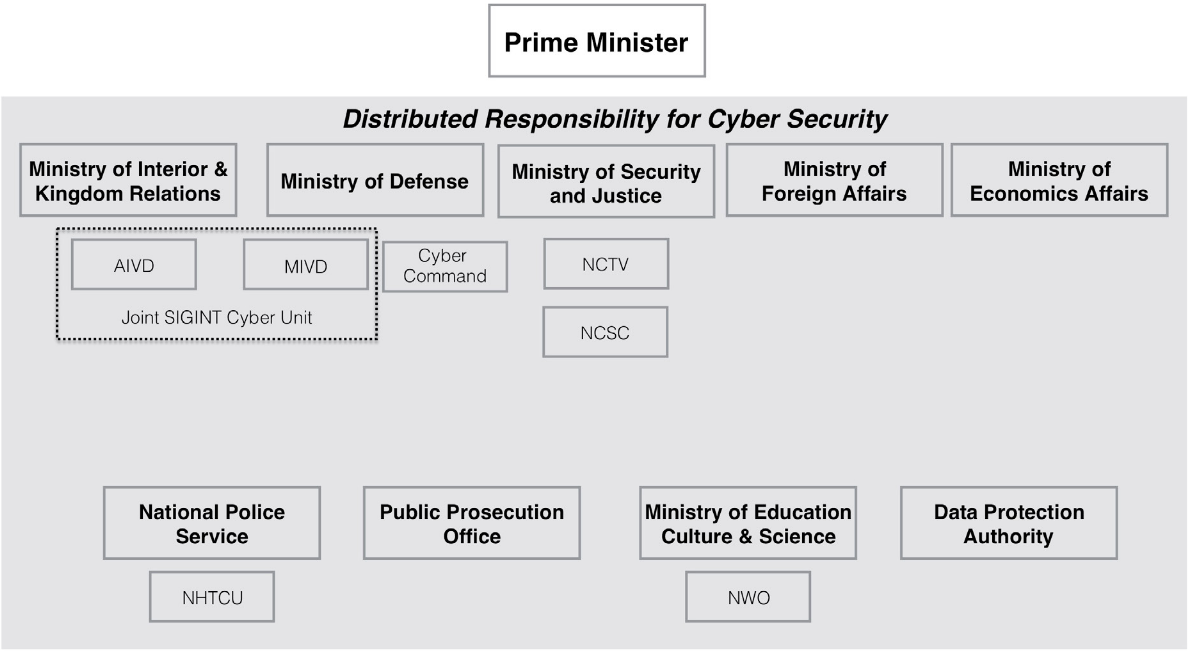

Prime Minister
Distributed Responsibility for Cyber Security
Ministry of Interior & Kingdom Relations
Ministry of Defense
Ministry of Security and Justice
Ministry of Foreign Affairs
Ministry of Economics Affairs
AIVD
MIVD
Joint SIGINT Cyber Unit
Cyber Command
NCTV
NCSC
National Police Service
Public Prosecution Office
Ministry of Education Culture & Science
Data Protection Authority
NHTCU
NWO

Figure 3: Organizational Chart of the Netherlands' Cyber Security National Architecture.

tion with private parties and the government bodies involved."[37] The distributed nature of the execution of the NCSS 2 objectives combined with inefficient funding mechanisms can undermine the intended outcomes of the strategy. The Dutch government has stated that cyber security is a priority, yet it is not funding the programs or institutions chartered with the execution of those initiatives as if they were strategically important to the economic well-being or national security of the country.

In fact, in 2015, of the publicly announced budgets,[38] the Dutch government only invested €28 million (~$30.5 million) or 0.004 percent of its GDP in cyber security for civilian, military, and law enforcement agencies. That year, the NCSC received funding of €2.7 million (~$2.9 million) – increased to €12.4 million (~$13.5 million) in 2016 – for the forward deployment of a national detection network. While the total defense budget is classified, the Dutch Ministry of Defense received an allocation of €5 million (~$5.4 million) – increased to €9 million (~$9.8 million) in 2016. The Dutch National Police received €13.8 million (~$15 million) to combat cyber crime and strengthen its security capabilities. Finally, the same year the Dutch government made a one-off investment of €6.5 million (~$7.1 million) to organize the 4th Global Conference on Cyberspace (in addition to the €2 million spent in 2014).[39] All remaining cyber security initiatives within the Netherlands depended on off-sets from existing programs. At the end of the 2016 cyber security awareness week "Alert Online," Herna Verhagen, CEO of PostNL, presented an advisory report ("Digitaal Droge Voeten") at the request of the CSR to Prime Minister Mark Rutte in which she urged the Dutch government as well as businesses to invest 10 percent of their annual ICT budget for specific cyber security measures.[40]

While cyber security investments are not receiving adequate funding, it is clear that the Dutch are investing in the ICT capacity of the country. Nearly 1 percent of Dutch GDP or over €23 billion (~$25 billion) are invested by the government and private sector on ICT infrastructure. The Dutch 2011-2015 digital strategy ("Digitale Agenda") committed additional funding to the modernization of the country's ICT infrastructure and echoed similar elements of the 2011 and 2013 national cyber security strategies by recognizing the importance of ICT for economic growth while also acknowledging the need for increased security in cyberspace. In this document, the Dutch government reaffirmed its intention to use ICTs to increase economic growth and prosperity, and reiterated that having an open, reliable, safe, and secure ICT infrastructure, and sufficient ICT knowledge and expertise were the necessary preconditions to achieve its goals. In order to increase ICT security and resilience, nationally and internationally, both the digital strategy and the national cyber security strategy mention the need for a comprehensive and multi-stakeholder approach to building a safe, secure, free, and peaceful cyberspace.

Moreover, the digital strategy emphasized that ICT trust is essential for digital communication, e-commerce, and the achievement of Europe's Digital Single Market. The Dutch government acknowledged that citizens and businesses' concerns about the security and reliability of ICTs and doubts about the protection of personal data might hamper expansion of e-commerce and e-governance, and stated that "greater public confidence in ICT could generate more than €1 billion (~$1.1 billion) in additional turnover from online trade."[41]

However, despite these strategies' close alignment, there continues to be a mismatch between the government's current cyber security spending and the necessary financial and human resources needed to strengthen the security and resilience of the country in the face of emerging ICT threats related to increasing digitization of critical services across the nation's economy. The Dutch government has been reviewing its national cyber security strategy for the past year and is expected to publish an updated version by 2018.[42] Also, the publication of a new national digital strategy is expected by 2018 once the new government is in place. In addition to persistent challenges with funding and devising an effective execution plan, it also remains to be seen whether the new government will be able to put forward a more balanced approach that aligns the country's national economic visions with its national security priorities in an increasingly interconnected and conflict-prone geopolitical system.

2. INCIDENT RESPONSE

As the national cyber security authority for the Netherlands, the NCSC shapes information security policies and activities through whole-of-government and whole-of-society prevention, detection, mitigation, and response, and serves as the central national cyber incident reporting office.

The NCSC became operational in January 2012 and has been devoted to private-public partnerships in several capacities since its inception. Today, the NCSC is the main body responsible for cyber incident response management and coordination for Dutch government institutions as well as for operators of critical infrastructure (vital operators or categories of vital operators of products and services whose availability and reliability are of critical importance to the Dutch society). In this capacity, the NCSC incorporated the Computer Emergency Response Team's (CERT) functions of the superseded GOVCERT.NL.[43]

The Netherlands' national cyber incident response plan (National Crisis Plan – ICT) is a subset of the Manual of Decision-making in Crisis Situation, and has been recently updated in March, 2017. The Manual provides a reference guide and generic procedures for all kinds of crisis situations including "large-scale cyber crises."[44] These plans are tested both during smaller exercises involving parts of the national crisis management structure and at the national level every two years. In the event of a major ICT disruption or cyber crisis, the NCSC would use its decentralized structure to respond and, if required, set up ad-hoc partnerships with other institutions and

The National Cyber Security Centre is responsible for cyber incident response management and coordination, and is the central national incident reporting office.

private partners based on the type and severity (e.g., duration, geographic spread, number of people/businesses affected) of the incident, sector(s) affected, and economic, physical, or societal impacts.[45] The Ministry of Security and Justice's Director of Cyber Security within the National Coordinator for Security and Counterterrorism (NCTV) is the primary civil servant responsible for coordinating incident response activities[46] and managing the crisis organization within the national crisis structure. In June 2015, the NCTV conducted a national level exercise to test the cyber preparedness of the Netherlands – operation ISIDOOR convened 30 public and private partners and featured a number of simulated cyber incidents, including data leaks and system vulnerabilities. The government worked with these public and private parties in determining the appropriate operational response to each incident.[47]

The Department for Cyber Security handles crises at strategic and tactical level, and the NCSC offers incident response and operational coordination, in addition to its "advising and informing role towards the crisis decision-making structure."[48] If multiple ministries are involved in tackling a cyber incident, the national crisis structure is evoked. The NCSC would also activate the ICT Response Board (IRB). The IRB is a private-public partnership between government agencies and critical sectors that was established in 2010. It serves as an advisory board for the national crisis management structure and is charged with analyzing the situation and providing recommendations to national crisis management bodies and affected parties on mitigation strategies.[49] For instance, the IRB was activated during the 2011 DigiNotar incident, and continues to play an essential role in the national crisis response structure of the country.

In July 2015, the National Coordinator for Security and Counterterrorism conducted a "Review of Policy on Critical Infrastructure." In that review, the government defined critical infrastructure "as a set of products, services, and underlying processes that is necessary for the functioning of the country [and that] must be secure and able to withstand and rapidly recover from all hazards... The loss or compromise of critical infrastructure affects national security and causes detrimental impact."[50] As a result of this review, the Netherlands has updated and conducted a more rigorous approach to critical infrastructure protection. This includes a stronger focus on the impact of criticality and level of disruption of critical processes within key sectors, as well as a classification of critical infrastructure in two categories, A and B, based on the degree of criticality/impact of potential disruptions, to prioritize them more effectively during incidents and to customize solutions for resilience-enhancing measures. For example, CATEGORY A includes infrastructure in which disruption, damage, or failure would cause approximately €50 billion (~$54.5 billion) in damage; or more than 10,000 dead, seriously injured, or chronically ill; or more than one million afflicted by emotional problems or serious problems with basic survival; or cause disruption or breakdown of at least two other critical sectors. A CATEGORY B infrastructure is one in which disruption, damage, or failure would cause approximately €5 billion (~$5.4 billion) in damage; or more than 1,000 dead, injured, or chronically ill; or more than 100,000 people afflicted by emotional problems or serious problems with basic survival.[51] The planning process identified 10 critical sectors under the authority of five different Ministries.

In May 2016, an international exercise was conducted to help stress test the cross-border dependency of electric utility availability. An energy shortage – whether caused by a power outage or other means – can have national and international economic and social impacts. Accordingly, the National Coordinator for Security and Counterterrorism organized, with funding for the Internal Security Fund (ISF) of the European Commission, the exercise "VITEX 2016" to help raise awareness and test crisis management procedures of government bodies and transport system operators across the EU during circumstances of low or no production capacity of electric power utilities. The exercise reinforced the importance of cooperation between EU member states in protecting critical infrastructures.[52]

Building upon the review of critical infrastructures and understanding possible thresholds for disruption, damage, and death, through exercises like VITEX 2016, the Dutch government realized that it needed to continue to plan and develop crisis scenarios. Exercises, war gaming, and crisis planning mechanisms help create institutional capacity to perform incident response effectively. They also require substantial planning and resources. In 2016, the Dutch government developed four hypothetical scenarios to guide it through the planning and development of institutional capabilities and response mechanisms.[53] Those scenarios are being used to inform the development of the new national cyber security strategy.

As stated earlier, national-level cyber security exercises are performed every two years and include both private and public entities. In addition to the internal planning exercises and incident response preparation, the Netherlands regularly participates in multi-national exercises organized by the EU (e.g., Cyber Europe exercise), NATO (e.g., Cyber Coalition and Cyber Atlantic exercises), the European Defense Agency (EDA), and the European Network and Information Security Agency (ENISA), and the US Department of Homeland Security (e.g., Cyber Storm), with the goal of strengthening cyber incident response capacity among states and improving international preparedness levels.[54]

In addition to its cyber incident coordination function, the NCSC issues threat alerts and warnings on malware and security vulnerabilities in ICT products and services, distributes information to both concerned parties and the general public, and recommends countermeasures. The NCSC has also developed various applications to monitor large number of information sources such as websites, social media, and notifications by trusted partners, as well as a network of sensors and honeypots to monitor network traffic and analyze Internet-based threats and their attack vectors. For example, the "Taranis" application (an open-source software used by several other CERTs) is used internally to collect, analyze, and publish warnings about ICT vulnerabilities, while the "Beita" program consists of a number of honeypots and a network of sensors installed at government organizations used to monitor automatic Internet attacks on those organizations.[55]

Building on its detection capability and its triage role during cyber crises, the NCSC is developing additional capabilities to improve awareness, resilience, detection, alerting, reporting, and crisis management. In 2015, the NCSC in cooperation with the General Intelligence and Security Service (Algemene de Inlichtingen- en Veiligheidsdienst, AIVD) and the Military Intelligence and Security Services (Militaire Inlichtingen en Veiligheidsdienst, MIVD) set up a National Detection Network (NDN) as a pilot program for the central government and other vital sectors to provide real-time analysis and sharing of cyber threat information in order to prevent their cascading effects. This network of sensors installed in different organizations monitors indicators of compromise for advanced persistent threats (APTs). The pilot program received positive feedback, and was further extended in 2016 as a standard managed security service offered by the NCSC. Currently, approximately 30 central government organizations have been attached to this network. Once fully operational, the NDN will connect 250 organizations.[56]

In line with the objectives set in the 2013 national cyber security strategy – making the Netherlands a "safe place to do business," increasing e-governance services delivery, and enabling all "citizens and businesses to digitally and safely handle their affairs with the government"[57] – the Dutch government has taken several steps to become more digitally secure and allow most government transactions with citizens and businesses to be conducted electronically. For instance, the Internet Standards Platform – a collaboration between the Dutch Government and the Internet community – launched a website (internet.nl) to enable users to check whether their Internet connection, e-mail, or web server complies with modern secure Internet standards, including IPv6 (sustainable reachability), HTTPS (secure website connections), DNSSEC (authentic domain information), DomainKeys Identified Mail (DKIM), a Sender Protection Framework (SPF), and a Domain-based Message Authentication Reporting and Conformance (DMARC) (to help mitigate e-mail spoofing), and START-TLS and DANE (to help mitigate e-mail eavesdropping).[58] This website tests servers for the connection security of both web and e-mail traffic, and indicates the extent to which it satisfies the "comply or explain" list on the Dutch Standardization Forum.[59] Moreover, the website has proved to be an effective means to help parties improve their use of secure Internet standards, and over 50 percent of the websites that were tested by visitors of internet.nl have improved their security scores in the past year.[60]

Government entities are required to choose from the open standards in the "comply or explain" list when investing in ICT systems. This

The Dutch government is promoting open standards and implementing a form of soft regulation – a "comply or explain" list – to encourage quick adoption.

is a form of soft regulation, which means that the rules that apply to implementing these security standards are not strongly enforced and, aside from reputation risk, there is no penalty for non-compliance. Moreover, all government agencies are required to comply with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) "27001: Information Security Management System" standards and with some government specific measures contained in the Dutch Baseline Information Security for the National government (Baseline Informatiebeveiliging Rijksoverheid, BIR), which are based on the ISO/IEC "27002: Information Security [Controls]" standards. State and local agencies must comply with the measures contained in the Baseline Information Security for Local Government (Baseline Informatiebeveiliging Nederlandse Gemeenten, BIG).

In 2016, the National Council for Digital Government agreed to include additional security standards like the ones promoted by the Internet Standards Platform to the "comply or explain" list. These requirements are intended to help authenticate senders of e-mails, ensure integrity and confidentiality of e-mail traffic, and combat spam and phishing. The National Council for Digital Government would like all government organizations to adopt these standards by 2018. The monitoring by the Standardization Forum shows clear adoption growth, although it still is a challenge for the government to meet the goal set by the National Council for Digital Government.

In addition to the "comply or explain" list, the NCSC regularly publishes guidelines and other factsheets for many industry-specific security standards, (e.g., the "Protect domain names from phishing" and "Secure the communications of mail servers" factsheets).[61] The Dutch government is also working with private sector partners to provide organizations with criteria and standards for basic cyber security and to help them better protect and improve the security of ICT products and services. For example, an increased number of .nl-domains and central government's websites in recent years have adopted DNS Security Extensions (DNSSec) – a protocol for checking whether a domain name refers to the correct IP address – which adds extra authenticity and integrity monitoring capability. While the Dutch government has yet to provide vendors of software and digital services with real incentives to increase the security of their products, or impose legally required minimum product liability, the CSR has recently issued a guidance document for businesses addressing these matters.[62] There are also questions on whether EU-wide regulations would be more appropriate in the long run to help balance between Dutch economic growth and security.

In order to better interact with citizens and businesses in an increasingly digital, secure, and standardized manner, the Dutch government has also expanded its eID scheme – a standard online identification system to securely access e-government services – and set up a personalized environment (MijnOverheid.nl) to allow citizens to receive correspondence from government agencies such as the Tax and Customs Administration, electronically. An increasing number of government agencies, municipalities, and pension funds are now using this Digital Message Box to send messages to their constituencies. The ultimate goal of the new eID system will be both to allow citizens and businesses to select a preferred authentication solution to access digital government services, and to avoid a single point of failure. Within this digital identity framework, there will be several authentication solutions available, such as DigiD (public sector), iDIN (banks), and Idensys (commercial). All these solutions would apply with a strict set of common requirements if they want to be used in the public sector.

To counter the adverse effects of DDoS attacks, different stakeholders and ICT providers launched two other initiatives in recent years: the Trusted Networks Initiative (TNI), which never became operational, and the Dutch Continuity Board (DCB) – a collaboration of ISPs that also incorporated members of the former TNI project.[63] The aim of this initiative is to limit the impact of DDoS attacks on Dutch critical infrastructure and make disrupted services available again to Dutch users as soon as possible. The DCB has been operational since the end of 2016 and offers participating parties the possibilities to separate the communication between members from all other Internet traffic in the event of a large DDoS attack.[64] Another initiative launched in 2014 to handle large scale Internet attacks on specific targets – known as the NaWas initiative – has been effective in thwarting DDoS attacks during the recent national elections.[65]

Finally, the NCSC regularly publishes cyber security-related white papers, factsheets, guidelines, and reports, such as the annual Cyber Security Assessments Netherlands (CSAN), which are drawn up in cooperation with other institutions and private partners, and include cyber incident data and analyses of global cyber threats.[66] While this is a good example of joint work between the government and other stakeholders and is highly valued by all partners, the CSAN reports do not appear to fulfill all the initial intentions set in the first NCSS – to provide an annual detailed and quantitative analysis of cyber threats faced by the government, critical infrastructure, and critical commercial services networks in the Netherlands. Instead, the CSAN reports offer a qualitative overview of international cyber risks and threats and global cyber security trends and incidents, and some updates on cyber security-related initiatives implemented outside the country.

In an effort to begin quantifying the costs of cyber insecurity, a new and additional Cyber Security Risk Assessment (CSRA), submitted in July 2016 by the Dutch Central Planning Bureau for Economic Policy Analysis and the NCSC to the Dutch Parliament, attempted to provide an economic analysis of cyber threats faced by the country, "with a focus on market failure limiting cyber security and the ensuing risks to [Dutch] businesses and consumers."[67]

The Netherlands is building capacity for incident response and has taken a number of positive steps to identify critical sectors and exercise crisis response mechanisms. Raising awareness regarding the threats that are aimed at and succeeding against Dutch critical infrastructure and services is essential toward strengthening the country's resilience. Measuring the true costs of cyber insecurity in the Netherlands would also help industry prioritize their investments and provide government leaders with powerful information to advocate for the appropriate resources needed to meet an overarching national goal: to drive economic progress underpinned by trust and resilience, while becoming "the" country to do business in.

3. E-CRIME AND LAW ENFORCEMENT

The Netherlands has demonstrated international commitment to protect society against cyber crime by signing (2001) and ratifying (2006) the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention), as well as by working domestically to enforce it and pass additional cyber crime and data protection laws (e.g., Electronic Signatures Act, Personal Data Protection Act, and Computer Crime Act of 2014).

In its 2013 national cyber security strategy (NCSS 2), the Dutch government recognized the need to make efficient use of limited resources to tackle cyber crime and reaffirmed its commitment to work toward international harmonization in criminal law based on the Budapest Convention. In order to promote these efforts, the Netherlands actively participates in various international meetings and related activities aimed at countering cyber crime activities, enhancing effectiveness of strategies against cyber crime, and strengthening international partnerships. The NCSC and the Dutch National Police actively work with Europol's European Cyber Crime Centre (EC3), Interpol, the Council of Europe' Committee of Contracting States, the EU policy cycle to tackle organized crime, the Organisation for Security and Co-operation in Europe (OSCE), and the UN Office on Drugs and Crime (UNODC). Moreover, the Cabinet's Security Agenda 2015-2018 tasked the Ministry of Security and Justice with reinforcing international efforts to counter cyber crime and harmonizing the activities of the Dutch National Police and their national partners with other departments.

Domestically, the Dutch parliament is considering two new laws that would expand the capabilities of the intelligence and security communities, and provide them with additional tools and authorities to investigate and combat advanced cyber attacks. The Data Processing and Compulsory Reporting Cyber Security Act (Wet Gegevensverwerking en Meldplicht Cybersecurity) would increase the police's authority to detect serious cyber crimes and compel key organizations to report cyber intrusions to the NCSC. This legislation also strengthens the legal basis of the NCSC.[68] The new Computer Crime Act III (Wet Computercriminaliteit III) would grant special powers to police and other investigative services to remotely infiltrate – or hack – the computers of suspects under certain conditions, if a crime is committed. After significant criticisms that this law afforded broader powers to the police to exploit software vulnerabilities, an amendment was added requiring the police to responsibly and immediately disclose any software vulnerability discovered, including zero day vulnerabilities, to the software developers. If the police want to keep the vulnerability discovered a secret, a court must give its consent and conduct an "independent review" to make sure that the interests of the police investigation are not unnecessarily placed above the safety of the software.[69] Both laws have already passed in the House of Representatives, but have yet to pass in the Senate.

While data breach notification requirements still vary among European countries, the Dutch government has already adopted most of the prescriptions contained in the 1995 EU Data Protection Directive and in the 2016 EU Network and Information Security (NIS) Directive and 2016 EU General Data Protection Regulation (GDPR), aimed at improving cyber security capabilities and cooperation across Europe. For example, the Netherlands has already established a Data Protection Authority (DPA, former Data Protection "college") to ensure compliance with laws that regulate the use of personal data and has recently strengthened its powers. In January 2016, an extension to the Dutch Data Protection Act came into force, which makes data breach reporting mandatory. The new law requires all organizations in the Netherlands to report incidents involving possible breaches of personal data to the Dutch DPA within 72 hours from discovery – as mandated by the GDPR. The Dutch DPA can initiate investigations and, where appropriate, impose fines up to €820,000 (~$893,510) or 10 percent of yearly revenue for violation of certain provisions in the law.[70] While thousands of reports were submitted by Dutch organizations to the DPA within a few months of passing this new law, many other organizations may still be reluctant to report incidents if they believe that the expected damages to their reputation outweigh the possible DPA fines for failing to report them.[71] Moreover, the ability to fine organizations for violating this law may be particularly troublesome for companies that transfer data to the United States following the invalidation of the Safe Harbor regime in 2014 and the subsequent controversy over Privacy Shield. Another data breach reporting obligation under the new Data Processing and Compulsory Reporting Cyber Security Act applies specifically to organizations engaged in critical infrastructure, and requires notifications of cyber incidents to the NCSC.

In terms of law enforcement capabilities, the Netherlands has established a mature institutional ability to address different elements of cyber crime, and has made several efforts to thwart cyber crimes domestically and internationally and bring criminals to justice. The Ministry of Security and Justice is responsible for combating cyber crime, but the Dutch National Police and the Public Prosecution Service (OM) are the main law enforcement entities responsible for cyber crime prevention, investigation, and prosecution. In recent years, they have detected, arrested, and convicted a growing number of people for cyber-related crimes, including wire fraud, money laundering, ransomware attacks, phishing scams, swatting activities, using banking malware to extort money, and launching DDoS attacks.[72] In addition, the Dutch

The Dutch National Police and the Public Prosecution Service are responsible for cyber crime prevention, investigation, and prosecution.

National High Tech Crime Unit (NHTCU) – a team within the Dutch National Police Agency dedicated to investigating advanced forms of cyber crime – tackles cases classified as "high tech crime" involving forms of crime that are "organized, target computer systems, and use sophisticated new technology or methods."[73] The NHTCU cooperates with international counterparts to fight transnational cyber crime, and launched "the Dutch Electronic Crimes Task Force, a new cooperation with financial and other [private sector organizations] to institutionalize private-public partnership as a means to actively combat certain types of cyber crime."[74] Additional law enforcement specialists are also being trained to investigate online child pornography, selling of counterfeit or stolen merchandise online, and radical Internet postings.[75] As of 2015, the Dutch government had allocated €13.8 million (~$15 million) to its National Police to combat cyber crime and strengthen its security capacity for multiple years.

Recognizing that cyber crime can increase as high-speed Internet becomes more available and as more connected devices become avenues for infection and exploitation, in 2013 the Dutch Ministry of Economic Affairs, in collaboration with various ISPs, co-founded the Abuse information Exchange (AbuseHUB) initiative – a clearinghouse for collecting, analyzing, and correlating information on botnet infections and other Internet abuse.[76] Members of AbuseHUB include the main ISPs in the Netherlands, hosting providers, SIDN (the registry for the ".nl" top-level domain), and SurfNet (the national research and education network operator), which are collectively responsible for more than 95 percent of all Internet connections in the Netherlands and more than 75 percent of all ".nl" domain registrations. Via this platform, a large number of national and international sources ("reliable notifiers") can feed information on security risks, botnet infections, and other Internet abuses directly into the automated incident response processes of member ISPs, who can subsequently work with their customers on swift, targeted actions to clean up their machines. Similarly to the European Advanced Cyber Defence Centre (ACDC) project – a non-profit initiative funded by the European Commission to improve the prevention, detection, and mitigation of botnets by offering an infrastructure of interconnected support centers across Europe linked to a central clearinghouse, the AbuseHUB initiative has proven quite successful at mitigating botnets and lowering infection levels, and is highly valued within the community.[77]

The Dutch government has also launched a "Netherlands Clean" project to raise the awareness of hosting providers about malicious activities carried out by some of their customers on their infrastructure and to encourage them to clean-up their infrastructure. For example, the Netherlands is home to a large percentage of malicious command-and-control domains hosted within the EU. The Netherlands also hosts a large percentage of the onion router (TOR) networks that enable anonymous communications often associated with illicit and illegal activities.[78] These types of measurements used to assess the "badness" of different Dutch hosting providers are based on public and private information. Sources of data and threat intelligence are emerging everywhere, and the government has strong partnerships with the Internet Hotline against Child Pornography and the National Centre for International Legal Assistance (LIRC), the Dutch Public Prosecution Office, and the Authority for Consumers & Markets (ACM). The police have even confronted some of the top "bad" hosting providers to point out how they may be facilitating cyber crime and to offer measures to take against it.[79]

The Netherlands is also working to increase its capacity and has joined various law enforcement cyber training programs, such as the Council of Europe's "Cybercrime@Octopus," launched in 2014, to assist countries in implementing the Budapest Convention and strengthening data protection and rule of law safeguards. Among other activities, the program includes courses for judges and law enforcement agents on cyber crime and electronic evidence. There are also a few other domestic programs to educate police officers, but it is unclear whether there are sufficient initiatives to train prosecutors, lawyers, and other investigators.

While the Netherlands is already the European center for criminal justice and capabilities to fight cyber crime, and is the home to one of the world's largest Internet exchanges, there is still further progress to be made to successfully implement all its ambitions in this important area. The Netherlands has a tremendous opportunity to pair its vision and ambitions with the capabilities that reside within the country in order to reduce cyber crime and accelerate innovation and trust in the digital economy. The end of 2017 will indicate to what extent the new Dutch government will commit to work toward these initiatives.

4. INFORMATION SHARING

As stated in the 2013 national cyber security strategy, the Dutch National Cyber Security Centre (NCSC) is responsible for both incident response coordination and information sharing. The NCSC acts as the center point of information flow between the government and private industry, manages threat information to develop new strategies and tactics discussed with stakeholders, and responds to reported cyber incidents.[80]

> *The Dutch National Cyber Security Centre is responsible for both incident response coordination and whole-of-society information sharing.*

The NCSC facilitates several Information Sharing Analysis Centers (ISACs), divided by sector, that share sector-specific threat information. Shared information includes, but is not limited to weaknesses and vulnerabilities of ICT-based products and services, forms of cyber attacks, profiles of perpetrators, and so forth. The various sectorial ISACs are led by members of each sector and include an Energy ISAC, Financial ISAC, Drinking Water ISAC, Health ISAC, etc. Several other liaisons between the NCSC and partner organizations, both in the public and private sector, meet on a weekly basis to discuss and share cyber security-related information. NCSC also promotes cyber security awareness and education, nationwide. Other relevant cyber security and information sharing private-public partnerships include the Platform on Information Society (ECP)[81] – a platform for promoting the safe use of ICTs in the Netherlands – and the National Continuity Forum (NCO-T) – a partnership between the Dutch government and suppliers of telecommunication networks.

Moreover, the Netherlands participates in various intra-state and inter-agency partnerships to foster information sharing, such as the NATO's malware information sharing platform (MISP), the EU's initiatives to improve threat data exchange among CERTs, the International Watch and Warning Network (IWWN), the Forum for Incident Response and Security Teams (FIRST), the Task Force on Computer Security Incident Response Teams (TF-CSIRT), and the National Cyber Forensics and Training Alliance (NCFTA) – a US non-profit corporation with a mission to facilitate collaboration among private industry, academia, and law enforcement to identify, mitigate, and neutralize complex cyber-related threats.[82] It has also signed a memorandum of understanding with neighboring countries Belgium and Luxemburg, which include cyber security cooperation and expertise-sharing on the development of private-public partnerships.

The Dutch government considers responsible disclosure as "an important step toward enhancing the security of information systems, software, and other ICT products."[83] A set of responsible disclosure guidelines have been developed by the Ministry of Security and Justice in collaboration with industry victims and ICT software/hardware developers. These guidelines "facilitate responsible reporting and handling of vulnerabilities" and "help organizations draft their own responsible disclosure policies."[84] During the Dutch Presidency of the European Union in the first semester of 2016, the CIO-Platform Nederland and Rabobank initiated a mechanism of cooperation for coordinated vulnerability disclosure. This process is important because more and more commercial products are being targeted, exploited, and harnessed for illegal and illicit activities. This effort led to the development and adoption of a "Coordinated Vulnerability Disclosure Manifesto," which recognizes the importance of engaging researchers and the hacker community in reporting vulnerabilities to the owner of the information system, allowing organizations the opportunity to diagnose and fix vulnerabilities in an early stage. Since its publication in May 2016, the manifesto has been signed by over 30 multi-national companies in the transportation, healthcare, energy, banking, and technology sectors. It has also been embraced by the Global Forum on Cyber Expertise's initiative on Responsible Disclosure as a global best practice.[85]

Building on the responsible disclosure initiative, KPN in partnership with the NCTV began to inventory ICT vulnerabilities. The reported vulnerabilities are provided with proposed solutions, so the amount of time that these vulnerabilities can cause harm is significantly reduced. [86] Additionally, the industry alliance that represents the voice of business in the Netherlands – the Confederation of Netherlands Industry and Employers (known as VNO-NCW)[87] – launched an initiative with the Ministry of Economics to spread knowledge on security threats and solutions within and across sectors.

The volume, scope, sophistication, and velocity of cyber threats to the Netherlands have the potential to cause even more harm as the country becomes more digitally dependent and adopts inherently vulnerable ICTs into its core businesses and critical services. There are a number of different paths being explored to share information using the NCSC, ISACs, sector specific leads, and even industry associations. The urge to increase resilience, reduce the attack surface, and create a climate for businesses to thrive are all essential first steps. The NCSC is an excellent platform to facilitate information sharing. However, it is unclear whether the necessary incentives are in place to accelerate the timely and actionable exchange of data. The Netherlands' two key commercial ports (the Schiphol Airport and the port of Rotterdam) and their security are critical areas to strengthen, and could be used as case studies to demonstrate how and why private-public information sharing is necessary to both businesses and the economy.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The Netherlands views R&D, innovation, and collaboration between the "golden triangle" of businesses, knowledge institutions, and government bodies as essential to its future competitiveness and economic strength. As such, the Netherlands is pursuing a modernized industrial policy – the Top Sector Policy – to harness sector specific economic strength and market share that would keep the Netherlands' economic growth thriving. The Top Sectors are seen as critical to contributing to the Netherlands' National Science Agenda (NWA) as well as the EU's Horizon 2020 strategy. The characteristics of the Top Sectors include a high labor productivity, export orientation, large size of R&D spending, and increased focus on solving social challenges. The Netherlands has identified nine innovative Top Sectors in which it is a world leader and is using specific policies to maintain its premier status in the following key sectors: (1) agriculture and food; (2) chemistry; (3) creative industries; (4) energy; (5) high tech systems and materials; (6) life sciences and health; (7) logistics; (8) horticulture and source materials; and (9) water.[88] The nine sectors are jointly responsible for 90 percent of the (private) R&D expenditure in the country.

In the Top Sector Policy, ICT is considered a cross-sectoral theme "in order to initiate and stimulate ICT innovation with and between Top Sectors."[89] In late 2014, a special task force (Team ICT) was established to evaluate and target the development of knowledge and talents for applications, services, products, work processes, and jobs for tomorrow and beyond. Subsequently, in late 2015, an ICT Knowledge and Innovation Agenda (KIA) for 2016-2020 was published that detailed the ICT challenges

The Netherlands is pursuing a modernized industrial policy – the Top Sector Policy – to stimulate ICT innovation and drive economic growth.

relevant to all sectors and Top Sectors, such as big data and cyber security. Today, discussions are also underway to determine whether to identify ICT as a tenth Top Sector.

The Netherlands has defined three central ambitions as part of its Top Sector Policy and vision for 2020. First, it wants the Netherlands to continue to be among the world's most entrepreneurial and competitive economies (today, the Netherlands ranks in the top five most competitive economies globally). Second, it sets a goal for the Netherlands to lead the Top Consortia for Knowledge and Innovation (TKIs), in which public and private parties participate and contribute to R&D in excess of €800 million (~$872 million) – of which at least 40 percent is from private financing. Finally, it challenges the Netherlands to grow its R&D activities to 2.5 percent of its GDP (from ~2 percent in 2014).[90]

The Ministry of Economic Affairs offers various tax incentives as part of the Top Sector Policy to promote software development, information and communication technology, and information security solutions. These include: the WBSO (R&D tax credit), which reduces wage tax and social security contributions for employees engaged in R&D activities; an R&D allowance that functions as a super deduction for qualifying non-wage expenses directly attributable to qualified research activities; and an innovation box (formerly known as a patent box).[91] While none of these tax incentives are specifically dedicated to cyber R&D, the WBSO, RDA, and innovation box are quite broad and open to all industries, which includes cyber security innovation. In addition, a dedicated Innovative Future Fund was specifically designed to make investment available to small and medium-size enterprises (SMEs) for innovation and vital research for the future. The 2016 Ministry of Economic Affairs' budget included €200 million (~$218 million) for this fund.[92]

The Top Sector Policy is loosely linked to the Dutch digital strategy (Digitale Agenda) and even less aligned with the national cyber security strategies, albeit they all recognize the importance of investing in cyber security innovation, and R&D. In line with the objectives outlined in the first NCSS and national digital strategy, and with the recommendations of the 2008 EU advisory board on Research & Innovation on Security, Privacy, and Trustworthiness in the Information Society, the 2013 Dutch National Cyber Security Research Agenda (NCSRA) II focused on two specific areas: (1) security and trust of citizens (to include privacy protection, security of mobile services, data and policy management, and accountability); and (2) security and trustworthiness of the ICT infrastructure (to include malware detection and removal, intrusion detection and prevention, software security, security of industrial control systems, and secure operating systems).[93] This research agenda highlighted the importance of basic and applied research in universities and academic institutions – including training of doctoral students – and encouraged a multi-stakeholder approach to facilitate innovation.

Moreover, the NCSS2 stressed the need for more coordination between the supply and demand of cyber talent so that creative people and experts could meet and work together, and suggested linking innovation initiatives with leading sector policy. It also encouraged the pursuit of a broad educational program "ranging from primary education to higher education, and from work-based training to university, and from the board room to the coalface" in order to enlarge the pool of cyber security experts and enhance users' cyber security proficiency.[94] With this goal in mind, the Dutch government, the business community, and academia decided to join forces to improve the quality and breadth of ICT education at all academic levels, and launched a cyber security platform for companies, students, policy makers, consumers, producers, and researchers to "connect, inspire one another, and attune research supply and demand." This platform, called the Dutch Cyber Security Platform for Higher Education and Research or "Dcypher," was established in 2016 by the Dutch Ministries of Security and Justice, Economic Affairs, Education, Culture and Science, and the Netherlands Organisation for Scientific Research (NWO).[95] Dcypher's mission supports the national agenda for research and education with particular emphasis in higher education in the area of cyber security to create sufficient cyber security knowledge, skills, and inspire innovation. This private-public partnership on cyber security education is still in its incipient stages and consultations between the government and the business community on improvements in computer sciences and cyber security curricula are starting but results have yet to be achieved. The NCSS 2 strategy noted that the NCSRA II and additional private-public partnerships would contribute to this development, as well.

In 2010, a consortium comprised of the Netherlands Organisation for Applied Scientific Research (TNO) and other academic and private sector organizations initiated a project ("Pieken in de Delta project") aimed at developing an innovation hub in The Hague to address some of the most pressing national, urban, and cyber security issues. This first project led to the establishment of The Hague Security Delta (HSD) in 2013 – a security cluster with hubs in The Hague, Twente, and Brabant. HSD was designed to harness Dutch innovation and help drive economic growth by bringing together Dutch businesses, government, and academic institutions to work collaboratively on cyber security and ICT innovation.[96] The HSD Campus in The Hague is the national innovation center for security with state-of-the-art labs, education and training facilities, and multiple office spaces – which have made this city one of the main cyber security hubs in Europe. At the end of 2016, TNO officially opened a Cyber Threat Intelligence lab in the HSD campus to experiment with new technologies that can improve early cyber threats detection and information gathering, and confidential data exchanges.[97] TNO and HSD are also working on the design of a new National Cyber Testbed to address cyber threats to critical infrastructures. The Metropolitan Region of Rotterdam and the Hague (MRDH) have made an initial investment of €200.000 (~$217.930) toward the realization of this plan.[98]

The 2012 NCSRA underscored the importance of small business innovation research (SBIR) and funded short-term research projects designed to progress from feasibility to prototype. The initial SBIR program allocated €2.7 million (~$2.9 million) resulting in prototypes for eight areas including business forensics, real time monitoring, and grid security. The second NCSRA allocated another €2.7 million (~$2.9 million) in funding to SBIR for the years

2013-2014. Funding came from six ministries for 21 feasibility projects that progressed to six prototypes in the areas of bring-your-own-device (BYOD) digital identity, forensics, digital identity, and network reconnaissance for offensive and defensive purposes.[99] In 2016-2017, the European Commission's Internal Security Fund was the primary funder (at over 90 percent) of the NCSRA's SBIR. An additional €3.3 million (~$3.6 million) is being allocated to the newest priorities of the Ministry of Security and Justice in this area.[100]

The Dutch government understands the importance of collaborating in R&D and innovation. In addition to its initiatives with the European Commission, the Netherlands has a number of bi-lateral engagements, as well. For example, the US-Netherlands Agreement on Cooperation in Science and Technology Concerning Homeland and Civil Security Matters fosters bilateral cooperation in fields that have a direct impact on national security. Starting in 2012, the two countries agreed to collaborate on cyber security, including incident management and response activities, control systems security, and cyber security exercises.[101] Strong international cooperation and experience sharing facilitates cost and knowledge sharing, which spurs the development of innovative and effective (national) cyber security capabilities.

Dutch investments in cyber R&D are overseen by several Dutch ministries such as Defense, Economic Affairs, Security and Justice, and Infrastructure and Environment, and other entities such as the CSR – the independent national cyber security council responsible for advising the government on the implementation and development of the national cyber security strategy and the execution of the Dutch cyber security research agenda, among other things. The TNO and NWO also provide significant contributions to cyber R&D in the Netherlands. The NWO receives about €400 million (~$436 million) a year, of which €300 million (~$326 million) directly comes from the Ministry of Education, Culture and Science. The NWO has a dedicated Cyber Security Programme focusing on connecting academia and the business community to promote development of products, services, and knowledge to increase the security of Dutch digitized society.[102]

For example, Dutch industry and academic centers are also pursuing various initiatives on both the materials sciences of quantum computing and the information protocols and algorithms that comprise quantum software. Countries around the world are racing to be the first with breakthroughs in quantum information technology – an emerging technology with important applications that will change the security, privacy, and integrity of networked infrastructures and the transactions running through them. One of these initiatives, called QuTech, was founded by TU Delft and TNO, and receives funding from a wide variety of sources including the Dutch

Dutch investments in cyber R&D are overseen by multiple Dutch ministries and the TNO and NWO provide significant contributions.

Ministries of Economic Affairs and Education, Culture and Science, TNO, TU Delft, NWO, and the private sector. This advanced research institute is focused on quantum technologies and materials sciences, and has received over €135 million (~$148.5 million) of funding from the Dutch government for a period of 10 years.[103] Moreover, technology companies like Microsoft and Intel are also making significant investments in QuTech's quantum research. In addition to QuTech, NWO through CWI,[104] in partnership with the University of Amsterdam, the Free University of Amsterdam, and the private sector are collectively funding research programs for new protocols and algorithms for use in quantum computing, and have recently launched QuSoft – a new research center for quantum software.[105] QuSoft will also participate and contribute to the EU strategy for investment in Quantum Science and Technologies, which is part of the Horizon 2020 Work Programme. The EU has stated that it wants to have quantum capabilities by 2035.[106]

The NWO's program is aligned with both the NCSRA II and the Dutch Digital Delta's 2016-2019 ICT Knowledge and Innovation Agenda (KIA), and features interdisciplinary collaboration with international scientists, local and global businesses, and higher education institutions.[107] NWO funding for cyber security-related projects is distributed among nine research themes of the NCSRA II that include: identity, privacy, and trust management; malware and malicious infrastructure; and offensive cyber capabilities, among others. Their budget for long-term research in the first round of funding in 2011, however, consisted of a mere €3.5 million (~$3.8 million) and about the same amount was allocated for the second round of funding in 2013.[108] The Dutch government funding almost doubled that amount for short-term research projects in the first round of funding in 2011 to a total of €6.5 million (~$7 million), but decreased it to €5.5 million (~$6 million) in the second round of funding in 2013. In these rounds, the government funded 40 cyber security-related projects in total. In the period from 2014-2016, NWO did not invest substantially in cyber security research projects.

In addition, the Netherlands participates in the EU's "Horizon 2020" program, and leverages its Top Sector Policy to enhance collaboration between the private and public sectors through ground-breaking R&D in order to generate growth in the ICT sector. The International Research and Innovation Cooperation team, part of the Netherlands Enterprise Agency (RVO) under the Ministry of Economic Affairs, is the Dutch national contact point for this EU program.[109]

Despite all published innovation plans and ambitious goals to promote the Netherlands as a "safe place to do business" and as the "Digital Gateway of Europe," the country faces a significant shortage of cyber security professionals able to protect its critical infrastructure and digital assets. In response to the shortage of cyber security talent, the 2011 national cyber security strategy set up a Cyber Education and Training Center to start developing the human capital necessary to bolster the country's growing digital economy.[110] The NCSS 2 reiterated the country's need to train a sufficient number of qualified cyber security professionals, and warned that the Netherlands would have a shortage of over 6,800 IT personnel by 2017.[111] In 2016, the Dutch Cyber Security Council signaled again that there still was a major shortage of cyber security professionals in the country, and recommended increasing emphasis on cyber security education at all levels.

Various universities and academic institutions in the Netherlands offer undergraduate and graduate degrees with cyber security concentrations, but most of the existing programs, including at elite universities like the University of Amsterdam and the University of Leiden,[112] are still highly technical or lack a multidisciplinary approach that combines technology with policy, law, economics, ethics, and other social sciences. Some universities have recently launched masters degree programs that combine technology, legal, criminal, and psychological issues, including privacy, intellectual property rights, cyber crime, and the human factor in computer-related crimes. For example, the University of Leiden, Delft University of Technology, and the Hague University of Applied Sciences, with the support of the Municipality of The Hague, launched a multidisciplinary research center – a Cyber Security Academy – that offers a part-time academic executive master's program, short courses, and tailored tracks on a wide array of cyber security issues.[113] Current cyber security programs, however, should be further expanded and incorporated into all major technical and non-technical academic programs, and universities should work to optimize their campus-wide resources to offer comprehensive curricula that synthesize technical, policy, economic, sociological, and legal components of the study of cyber security.[114]

Finally, the NCSS 2 recognized that progress has been made in the Netherlands to increase awareness of cyber risks, but that more needs to be done to raise awareness of cyber threats and increase cyber hygiene across society. In response to this need, the Dutch government – and the NCSC in particular – regularly sponsors and participates in multiple cyber security awareness campaigns throughout the year. These include: the European Cyber Security Month during the month of October; the "Alert Online" campaign – a two-week long public effort in which different stakeholders join forces to promote cyber security among Dutch citizens, government, and the private sector by organizing workshops, meetings, presentations, and other activities; the "Hang up, click away, call your bank" campaign – an effort promoted by the Dutch Payments Association to inform Dutch citizens about ways to protects themselves from online fraud; and Safer Internet Day. Nonetheless, the degree to which these awareness campaigns effectively prevent phishing or other cyber crimes is unknown.[115] More recently, the Dutch Consumers Association (Consumentenbond) started an "Update!" campaign to encourage manufacturers of Android smartphones to make software updates available to consumers and inform them about vulnerabilities in their devices. As part of this campaign, the Dutch Consumers' Association filed a lawsuit against Samsung in 2016 accusing them of having "poor software update policy" and demanding that the company respect its duty of care and make updates available to customers for at least two years after purchase of devices.[116]

At the end of the 2016 cyber security awareness week "Alert Online," Herna Verhagen, CEO of PostNL, presented an advisory report ("Digitaal Droge Voeten") at the request of the CSR to Prime Minister Rutte in which she urged the Dutch government as well as businesses to invest 10 percent of their annual ICT budget for specific cyber security measures.[117] The report received widespread coverage in Dutch media due to its alarming message about increased cyber threats and recommendation for the Cabinet to appoint a high-level official for cyber security, but it did not provide additional insight into the state of Dutch investments in cyber R&D.[118]

The Netherlands' Top Sector Policy recognizes that ICT R&D is important, but in order to meet the challenge stated by Ms. Verhagen to the Prime Minister and for the Netherlands to effectively seize its economic vision, it will need to elevate ICT to a dedicated tenth sector and harness the power of private and public funding for additional R&D. Currently, cyber R&D is fragmented across multiple institutions and thus likely sub-optimized for a broader, more impactful vision. Moreover, there is a serious shortage in cyber specialists, and university programs still lack a comprehensive approach to cyber education extending beyond simply technical methods. The joint initiatives that the Netherlands has with the European Commission, the US, and others present an opportunity to harness the global innovation communities. The Hague Security Delta and TNO's Cyber Threat Intelligence Lab may prove to be important foundations to foster cyber security solutions for the digital future.

6. DIPLOMACY AND TRADE

The Dutch government has recognized cyber security as a Tier One priority of its foreign policy and has been actively engaged in diplomatic and trade and commerce negotiations related to cyber security and the promotion of practical cooperation in cyberspace, as well as initiatives related to data protection and privacy within the EU. The Netherlands is currently engaged in a variety of international discussions on cyber security, cyber crime detection and prosecution, CSIRTs cooperation and Critical Information Infrastructure Protection (CIIP), confidence building measures (CBM), cyber capacity building, Internet governance, digital rights, and international norms for responsible state behavior in cyberspace.

Cyber security is a Tier One priority for the Netherlands' foreign policy agenda.

During the 2016 International Security Conference in Munich, Dutch Minister of Foreign Affairs, Bert Koenders, recognized that "as societies become more and more dependent on cyber infrastructure, the opportunities for growth and innovation seem endless and promising. But so does our vulnerability to cyber incidents, attacks [and] highly disruptive or even destructive cyber operations."[119] He stressed the Netherlands' commitment to "strengthen our cyber defenses, build international consensus to protect critical infrastructure, like energy, telecom, and banking as well the Internet itself, … defend digital rights, promote innovation, improve cyber security, [and use cyber diplomacy to develop] a common normative framework that regulates state behavior in cyberspace and maintains international stability."[120]

In addition, cyber security was an important theme in the 2013 Dutch "International Security Strategy," which identified various actions undertaken by the Netherlands abroad and in cooperation with other countries to secure its interests domestically and internationally, and to promote the development of international standards and regulations on cyber security.[121] In the 2013 national cyber security strategy (NCSS 2), the Dutch government reiterated its strong commitment to work with international partners to "create a secure and open digital domain" and "protect fundamental rights and values."[122] It also reaffirmed its desire "to play a prominent role in the search for new coalitions for defense, diplomacy, and development," and to serve as "cyber security mediator and hub" for international cooperation in the digital domain.[123] In February 2017, the Dutch Ministry of Foreign Affairs (MFA) published the document "Building Digital Bridges" – the MFA's "International Cyber Strategy: Toward an integrated international cyber policy" – which stressed the importance for the Netherlands to work on diplomacy, defense, and development in order to tackle the threat of cyber attacks from hostile countries and cyber criminals. The strategy echoed previous documents in supporting a "secure, free, and open Internet" and encouraging the Netherlands to play a leadership role in improving international agreements on cyber security.[124] It also emphasized the need to strengthen the Netherlands' role within various international fora by setting forth "a clear vision on Dutch international cyber policy to ensure that all parts of the government operate in a coherent and effective manner."[125]

The Dutch Ministry of Foreign Affairs published its own International Cyber Strategy that recognizes the need for an ongoing, open, and pragmatic dialogue between all stakeholders.

In order to foster stability in cyberspace and reach internationally accepted standards in which all parties involved are represented, the Netherlands has been advocating for a multi-stakeholder "Internet governance model that takes account of the interests of the various actors"[126] and investing in various formal and informal alliances, both within and outside the EU. The Netherlands has been very active in the international arena, including collaboration with the United Nations (UN), the Council of

Europe, NATO, the Organization for Economic Co-operation and Development (OECD), Europol, and other multinational organizations. The multi-stakeholder theme expressed in both the national cyber security strategy and the 2011-2015 digital strategy ("Digitale Agenda") is actively pursued during the Global Conference(s) on Cyberspace – a series of inter-ministerial gatherings held in London, Budapest, Seoul, and The Hague since 2011 and known as the "London Process;" by developing confidence building measures (CBMs) between states, similar to those agreed upon by members of the Organisation for Security and Cooperation in Europe (OSCE);[127] and by participating in other multi-stakeholder settings like the International Telecommunication Union (ITU), the Internet Governance Forum (IGF), and the World Economic Forum (WEF). One important outcome of the 4th Global Conference on Cyberspace held in The Hague in 2015 was the launch of a Global Forum on Cyber Expertise (GFCE) – a global platform for governments, inter-governmental organizations, the tech community, and academia to exchange best practices and expertise on cyber capacity building. The mission of the GFCE is to "identify successful policies, practices and ideas" that can be replicated on a global scale, and "develop practical initiatives to build cyber capacity."[128]

In addition, the Netherlands started The Hague Process – a series of consultation meetings and activities between over 50 states and the authors of the Tallinn Manual 2.0 on peacetime international law. The main objective of this initiative is to promote interstate discussions and shared understanding about how international law applies in cyberspace. The Netherlands also initiated a Cyber Norms Platform with Estonia to discuss input for the UN Group of Governmental Experts (UN GGE) on international law and joined the UN GGE as a full member for the 2016-2017 period. In addition, the Dutch government played a critical role in the establishment of a new Global Commission on the Stability of Cyberspace (GCSC) – a global body tasked with developing proposals for norms and policy initiatives to improve the stability and security of cyberspace. The new GCSC is based in The Hague and is comprised of prominent international experts from over 15 different countries, including diplomats, academics, and representatives of private sector companies, civil society, and the tech community. Dutch MFA Koenders announced the establishment of the GCSC at the Munich Security Conference in February 2017. He stated: "This is a unique initiative to ensure that we drive [existing] activities in the right direction. … It requires greater coordination among us all. It needs the development of norms to provide a stable and secure environment" for the benefit of all.[129]

With The Hague as the recognized city of international peace and security, the Netherlands aims to develop into an "international center for cyber diplomacy" that brings together international experts, policymakers, diplomats, military personnel, and NGOs in order to promote the peaceful use of cyberspace. The country is already combining knowledge from existing Dutch centers, and creating a strong network of multidisciplinary expertise to tackle different topics, such as international standards for conflict prevention, civil-military cooperation, and non-proliferation in cyberspace. These efforts would form the basis for a series of multi-stakeholder, high-level meetings.[130]

Another example of the multi-stakeholder approach to building a safe, secure, free, and peaceful cyberspace championed by the Netherlands is the Freedom Online Coalition (FOC) – a joint effort initiated by the Dutch MFA in 2011 to support Internet freedom and promote democracy and human rights online.[131] Today, the coalition has 30 member countries from all over the world and the Netherlands is pushing for additional countries to join. In addition to providing a platform for multi-stakeholder meetings and conferences, Coalition members share information on violations of human rights online, work together to voice concern over measures that curtail freedom of expression online, and engage civil society and the private sector on pressing issues related to Internet freedom while encouraging the incorporation of agreed upon standards into the design of new and innovative products and services.

The 2011 Dutch digital strategy reinforced the connections between economics, cyber security, ICT trust, and capacity building. In fact, the Netherlands routinely addresses development cooperation issues and participates in projects dedicated to cyber capacity building, cyber security capacity building, and cyber confidence building in developing countries. In addition, the Netherlands was the first country to speak out in favor of encryption and against limitations to the development, availability, and/or use of encryption algorithms.

Cyber security issues are often entangled in trade negotiations and security treaties, as well. The Netherlands has participated in many of these discussions and negotiations in the various international fora mentioned above, and has been implementing and enforcing international agreements at the domestic level. The Netherlands approaches negotiations on trade as a champion for data privacy and also advocates for nations to remain technology agnostic in order to promote the free flow of goods, services, data, and capital across borders. For example, the Netherlands has engaged in many of the international dialogues concerning encryption, export regulations for intrusion software and "dual use" technologies, such as those covered in the "Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," and has been a pioneer in the promotion of responsible disclosure.

Cyber issues are emerging in many different traditional international relations areas including human rights, economic development, trade agreements, arms control and dual use technologies, security, stability, and peace and conflict resolution. The Dutch MFA serves as the office responsible for coordinating Dutch participation and efforts in various multinational fora of discussion on cyber security issues. Nonetheless, the more technical discussions that occur in international fora like the TF-CSIRT and the CSIRTs Network are outside the purview of the MFA. When cross-cutting issues arise needing multiple sets of expertise to engage, the Netherlands establishes ad hoc task forces. For example, a Task Force Cyber was established in 2015 as part of both the Security Policy Department and the Multilateral Organizations and Human Rights Department of the MFA, to develop and advocate a Dutch integrated international cyber policy. The Netherlands has also established a Special Envoy for International Cyber Policies position within the ministry with the direct responsibility of negotiating cyber security-related foreign policy agreements and "further disseminating the results of the GCCS and the Dutch ambitions and priorities in the field of cyber."[132] For economic and trade negotiations, the Ministries of Economic Affairs, Security and Justice, Foreign Affairs, and the NCSC assemble to discuss and develop a common position to ensure the economic/trade missions achieve their desired outcomes.[133] The Netherlands intends to enhance its diplomatic initiatives by activating a network of cyber diplomats at a number of embassies. This network will fall under the existing budget of the MFA.[134]

In addition to its own foreign and economic policy positions, the Netherlands used its 2016 presidency of the EU to advance the cyber security dialogue more broadly. Through Dutch leadership, new initiatives in the field of international cooperation in cyber crime were spawned and the importance of an overarching EU cyber security strategy was reaffirmed. By the end of 2017, the EU Commission is expected to publish a second European Cyber Security Strategy.

Clearly, the Netherlands has fundamental international interests in this area and has been an advocate of free, open, and secure Internet. Economically, the country is one of the top 10 exporters of ICT goods and telecommunication services and the broader Dutch digital economy is growing beyond 22 percent. Its diplomatic initiatives are focused on strengthening international cooperation and reinforcing legal frameworks while reducing crime, espionage, human rights violations, and other harmful on-line activities. Moving forward, the Dutch government should pursue a more integrated approach that focuses the expertise from the Ministries of Foreign Affairs, Economic Affairs, and Security and Justice to achieve both the economic goals of the Netherlands along with assuring its security priorities. The Dutch government strives to ensure consistency between its domestic and foreign policy agendas so that it does not undermine its credibility at the negotiating table. The Dutch have established a brand and are recognized through the city of The Hague, as an international leader for peace and security. Today, the Netherlands is continuing to build on that brand and extending it to be known as a leader in cyber security by leveraging EUROPOL's Cyber Crime Center, establishing the Hague Security Delta for cyber innovation, and initiating the Hague Process to clarify how international law applies to cyber operations.

7. DEFENSE AND CRISIS RESPONSE

In the late 2000s, the use of military grade weapons against national critical infrastructures and the use of cyber in military operations catalyzed the Dutch Ministry of Defense (MoD) to undertake initiatives to better train, organize, and equip its Armed Forces in order to protect the Netherlands and enhance its military posture. Despite the military drawdown and broad-based budget cuts in other areas, the MoD started to proactively invest in cyber operational capabilities within its Armed Forces. At the same time, the MoD started to discuss publicly the importance of the mission and the necessity to create a more robust cyber security posture. In order "to protect the nation, the Netherlands is developing robust capabilities based on the objectives of early detection, active defense, and if necessary intervention," and it is building-up these capabilities in support of Dutch interests.[135]

Prompted by the 2010 NATO Summit in Lisbon and the publication of the "NATO Cyber Defense Concept, Policy, and Action Plan," the Dutch government began reflecting some of the same concepts and commitments in their first national cyber security strategy in 2011 and subsequent cyber defense plans.

The 2012 Dutch "Defence Cyber Strategy" acknowledged that military and civil, public and private, national and international actors had become more intertwined in cyberspace. The Defense Minister's accompanying letter to this strategy declared cyberspace as a "fifth domain for military operations alongside air, sea, land, and space."[136] The 2012 defense cyber strategy described the role of the Netherlands Armed Forces in the digital domain and laid out six focal areas of action: (1) adopting a comprehensive approach; (2) strengthening the cyber defense of the Defense organization (defensive element); (3) developing the military capabilities to conduct cyber operations (offensive element); (4) strengthening the intelligence position in cyberspace (intelligence element); (5) strengthening the knowledge position and innovation strength of the Defense organization in cyberspace, including the recruiting and retention of qualified personnel (adaptive and innovative elements); and (6) intensifying cooperation both nationally and internationally (cooperative element).[137]

Building on the 2012 strategy, the 2015 Defense Cyber Strategy expanded the Netherlands' approach to holistic cyber operations and highlighted seven key initiatives to "create the right conditions for success [of the Netherlands] in cyberspace." These include: (1) attracting knowledgeable cyber professionals; (2) expediting capability development and facilitating rapid acquisition; (3) strengthening national digital resilience through partnerships; (4) training and educating personnel about the opportunities and danger of the digital world; (5) strengthening and hardening defense networks, IT services, and systems; (6) modernizing the 2002 Intelligence and Security Services Act to enlarge the cyber intelligence capacity; (7) building the operational cyber capacity of the Armed Forces.[138]

In order to accomplish these objectives, the Dutch organized and divided their lines of responsibilities in this field into these primary functional areas:

- The Joint Information Management Organization (Joint InformatieVoorzienings Commando, JIVC), operational since 2013, is responsible for protecting and monitoring all military networks, IT services, and systems in the Netherlands and areas of operations. Its primary role is to protect and defend. The Dutch Defense CERT (DefCERT) – part of JIVC – is responsible for supervising and ensuring the reliability and unhindered functioning of information systems in support of military operations. DefCERT is the first point of contact for reporting and responding to cyber incidents within the MoD and carries out threat and vulnerability assessments, advising the Armed Forces on security measures.

- The Military Intelligence and Security Services (MIVD) is responsible for cyber intelligence, along with the General Intelligence and Security Service (AIVD) within the Ministry of Interior and Kingdom Relations. In 2015, AIVD and MIVD combined their signal intelligence and cyber capabilities into the Joint SIGINT Cyber Unit (JSCU) – a unit tasked with protecting national security and the Dutch Internet against cyber threats, while also providing better support to the Armed Forces during their missions.[139] In addition, MIVD actively cooperates with DefCERT in the field of computer network defense (CND) and on investigations related to cyber incidents within the MoD.[140]

- The Defense Cyber Command (DCC) is the direct liaison for the Commander of the Armed Forces for the cyber mission. The DCC is also responsible for coordinating all tasks within the Ministry of Defense for all four services (army, navy, air force, and military police) for operations and operational cyber capacity to include offensive capability development and deployment.

The Netherlands announced the creation of its dedicated DCC in September 2014.[141] Today, the DCC is an integral component of military operations and provides both defensive and offensive capabilities to the full range of missions, including peace-time operations, crisis management, and humanitarian assistance.[142] The Netherlands was the first NATO country to openly discuss the importance of offensive cyber operations as an element of national power. "As with the deployment of other types of force, when it comes to the deployment of offensive cyber capabilities, the Netherlands believes in exercising extreme restraint and only taking action if there is an adequate basis for such action in national or international law."[143] As the Commander of DCC, Brigadier General Hans Folmer, stated:

> The mission of the Dutch Cyber Command is to contribute to the freedom of maneuver in cyberspace and to the fighting power of the Dutch armed forces by preparation, training, and deployment of operational cyber teams. These teams provide integrated military operational cyber capabilities in support of the Dutch Armed Forces in the full spectrum of military cyber operations. They plan, coordinate, and execute as part of a Joint Task Force Cyber Operations from defensive cyber operations to offensive cyber operations, with direct effects or supporting effects.[144]

In addition to protection, intelligence, and operations, the DCC has a coordinating role for all DOTMLPF activities (involving any combination of doctrine, organization, training, materiel, leadership and education, personnel and facilities). It "coordinates and facilitates these cyber activities and capabilities within the Dutch MoD and with military and civilian national and international partners. Furthermore, the Command obtains, disseminates, and manages cyber expertise for the entire

The mission of the Dutch Cyber Command, established in 2014, is to contribute to the freedom of maneuver in cyberspace and to the fighting power of the Dutch armed forces.

Dutch Armed Forces by contributing to education, training, and exercises."[145]

The Dutch DCC has openly discussed six different types of cyber operations, some comparable to what other countries have developed and some are new and more unique:

1. Cyber security operations – passive and defensive measures focusing on protection, prevention of damage, and restoration;

2. Defensive counter cyber operations or proactive countermeasure – actions to neutralize active threats within the Netherlands' own networks, such as detecting or obtaining information about cyber intrusions, cyber attacks, or impending cyber operations, or for determining the origin of an intruder's operations or terminating such adversary malicious cyber activity – these operations do not extend beyond the Netherlands MoD's perimeter;

3. Offensive counter cyber operations conducted outside the perimeter of the Dutch MoD networks. These are military cyber operations executed in response to attacks, including launching preemptive and preventive counter operations against the source of a cyber threat;

4. Cyber intelligence, surveillance, and reconnaissance operations – cyber operations at a lower level that have the sole purpose of collection of general data or information regarding other actors' activities in cyberspace. These operations do not include the activities of the defense intelligence and security services;

5. Supporting cyber operations – small-skill operations in support of other more tactical level activities in peace-time, crisis, or conflict situations. Due to its versatility, these operations are particularly useful in support of the information warfare capacity, such as psychological operations, deception, operational security, lawfare, and electronic warfare;

6. Offensive cyber operations or combat operations – either supporting an operation in another domain or executed in cyberspace only to achieve a military objective (giving commanders the ability to achieve an operation).

During the 2016 International Conference on Cyber Conflict, Brigadier General Folmer acknowledged that "the Netherlands includes the options of offensive cyber actions in all its military operations," and stressed that "cyber operations must now be integrated in military missions and become just another tool in the toolbox of the mission commander. When developing military offensive capabilities, we should focus on using them against legitimate targets and mitigat-

> *"Cyber operations must now be integrated in military missions and become just another tool in the toolbox of the mission commander."*
>
> *– Brigadier General Hans Folmer*

ing negative collateral effects. This means that emphasis should be placed on planning, decision-making, logging, testing, training, and so on."[146] In addition to its domestic efforts, the Netherlands is participating in NATO's Multinational Cyber Defence Capability Development Program with NATO's Communication and Information Agency, together with Canada, Denmark, Norway, and Romania.

The Dutch MoD participates in the bi-annual national level crisis response exercise. Moreover, the Dutch Armed Forces are active participants in multi-national and allied cyber exercises – as noted in the incident response section – and especially in all those associated with NATO such as "Cyber Coalition" and "Cyber Atlantic." It also participates in bi-lateral collaborative exercises with Germany and other NATO countries. Additionally, the Dutch government has been leading the scenario development and discussions within NATO about integrating cyber into its formal military processes. During the July 2016 Warsaw Summit, NATO member states agreed to enhance the cyber defenses of national networks and infrastructures, improve their resilience and ability to respond quickly and effectively to cyber attacks, and adapt their cyber defense capabilities. NATO also agreed that cyberspace was a fifth domain of warfare.

The DCC and MoD writ large are supporting the cyber mission out of existing budgets. While much of the MoD's budget is classified, the 2017 defense budget showed an increase of €17 million (~$18.5 million) for cyber.[147] That same budget allocated a total of €412 million (~$449 million) for IT, but it is unclear how much of these funds are allocated for cyber defensive or offensive capabilities. The Netherlands is investing in training and recruitment activities, focused R&D, and international cooperation to support its cyber defense mission. The Dutch MoD is using recruitment techniques to attract ethical hackers, and highlighting that these missions are legal if conducted under the right authorities. They are also partnering with key industry leaders to develop a skills development program for training motivated soldiers to become cyber skilled experts. Finally, recognizing that top talent is scarce and the necessity of finding ways to optimize, led to the bundling of AIVD and MIVD efforts into the Joint SIGINT Cyber Unit. Pooling scarce knowledge and resources (funding and personnel) is essential in these ever-changing and increasingly challenging fields.

The Netherlands has declared cyberspace as a "fifth domain for military operations" and is organizing to execute upon this mission. The country clearly recognizes that security is a prerequisite not only for a functioning society but for also the future of its economy. Yet, its vision and ambitious plans are not financed with sufficient money, materiel, or manpower. This means that the Dutch must capitalize on their pragmatic outlook and find creative means by which to attract, develop, and retain personnel; partner and leverage the EU, NATO, and other alliances to gain capability; and convince the new government to invest in their ambitious agenda with dedicated funds.

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, the Netherlands is on a path to becoming cyber ready and is currently partially operational in most of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As the Netherlands continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is currently being applied to 125 countries.

The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, the United Kingdom, and the United States can be found at the following link: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

Legend

● **Fully Operational**

◐ **Partially Operational**

○ **Insufficient Evidence**

IDI Rank		NRI Rank	GDP Rank	National Strategy	Incident Response	E-Crime & Law Enforcement	Information Sharing	Investment in R&D	Diplomacy & Trade	Defense & Crisis Response
8	Netherlands	6	17	◐	◐	◐	○	◐	◐	◐

ENDNOTES

1. Robert Hobbes Zakon, "Hobbes' Internet Timeline 24," https://www.zakon.org/robert/internet/timeline/.

2. The Centrum Wiskunde & Informatica (CWI) is part of the Netherlands Organization for Scientific Research (NWO) and, at that time, was fully funded by the Dutch Ministry of Education, Culture and Science.

3. AMS-IX, "Linking Amsterdam to the World," https://ams-ix.net/about/historical-timeline/linking-amsterdam-to-the-world.

4. Dutch Ministry of Security and Justice, "National Cyber Security Strategy 2: from Awareness to Capability," (October 2013): 13, https://english.nctv.nl/binaries/national-cyber-security-strategy-2_tcm32-84265.pdf.

5. OECD, "OECD Digital Economy Outlook 2015," (July 15, 2015): 38-39, http://www.oecd.org/internet/oecd-digital-economy-outlook-2015-9789264232440-en.htm, and The Hague Center for Strategic Studies, "Dutch Investments in ICT and Cybersecurity," (December 2016): 9-20.

6. Mark Knickrehm et al., "Digital Disruption: The Growth Multiplier," Accenture Strategy Report, 2016, https://www.accenture.com/us-en/insight-digital-disruption-growth-multiplier.

7. National Coordinator for Security and Counterterrorism (NCTV), Ministry of Security and Justice, "Beleidsreactie Cyber Security Beeld Nederland 2016," September 5, 2016.

8. Ministry of Economic Affairs, Agriculture and Innovation, "Digital Agenda.nl – ICT for innovation and economic growth" (2011): 4.

9. *Ibid*, 5; and European Policy Centre, "Establishing the Digital Single Market: policy recommendations," 1, http://www.epc.eu/dsm/6/Policy_recommendations.pdf.

10. Ministry of Economic Affairs, Agriculture and Innovation, "Digital Agenda.nl – ICT for innovation and economic growth" (2011): 5.

11. Ministry of Economic Affairs, "Progress through Renewal: 2016 Enterprise Policy Report," 27.

12. Netherlands Organisation for Applied Scientific Research (TNO), "Cost of Cyber Crime Largely Met by Business," accessed on November 5, 2013, www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2012-04-10%2011:37:10.0&Taal=2 .

13. Deloitte, "Cyber Crime Costs Dutch Organisations 10 Billion Euros each Year," April 4, 2016, https://www2.deloitte.com/nl/nl/pages/about-deloitte/articles/cybercriminaliteit-kost-nederlandse-organisaties-10-miljard-euro-per-jaar.html. English press release: https://www2.deloitte.com/nl/nl/pages/about-deloitte/articles/cyber-crime-costs-dutch-organisations-10-billion-euros-each-year.html.

14. Dutch Ministry of Security and Justice, "National Cyber Security Strategy: Success through Cooperation" (February 2011), https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.

15. Kim Zetter, "Diginotar Files for Bankruptcy in Wake of Devastating Hack," *Wired*, September 20, 2011, https://www.wired.com/2011/09/diginotar-bankruptcy/.

16. Dutch Ministry of Security and Justice, "National Cyber Security Strategy (NCSS 2): from Awareness to Capability" (October 2013): 28, https://english.nctv.nl/binaries/national-cyber-security-strategy-2_tcm32-84265.pdf.

17. Deltawerken, "The Delta Works," http://www.deltawerken.com/Deltaworks/23.html; and Dutch Digital Delta, "About us," https://www.dutchdigitaldelta.nl/en/about-us.

18. *Ibid*.

19. Hans Folmer announcing the creation of Dutch Defense Cyber Command, The Hague, September 25, 2014, https://cyberwar.nl/d/20140925_Toespraak+Minister+Hennis-Plasschaert+bij+lancering+van+het+Defensie+Cyber+Commando+in+Den+Haag.pdf.

20. Ministry of Foreign Affairs, "International Cyber Strategy: Toward An Integrated International Cyber Policy," February 13, 2017, Section 3.2 on "Cyber Defense and Security."

21. Government of the Netherlands, "Speech by Prime Minister Mark Rutte at the Cybersecurity Matching Forum," November 10, 2015, https://www.government.nl/documents/speeches/2015/11/10/speech-by-prime-minister-mark-rutte-at-the-cybersecurity-matchmaking-forum-tokyo.

22. The Hague Center for Strategic Studies, "Dutch Investments in ICT and Cybersecurity," 20. For more on other countries' cyber security spending as a portion of their national GDP, see: Melissa Hathaway et al., country profiles in the "Cyber Readiness at a Glance" series, *Potomac Institute for Policy Studies,* http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

23. Melissa Hathaway et al., "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index," *Potomac Institute for Policy Studies,* November 2015, http://www.potomacinstitute.org/images/CRIndex2.0.pdf.

24. Dutch Ministry of Security and Justice, "National Cyber Security Strategy (NCSS 1)," 2.

25. *Ibid*, 5-6.

26. *Ibid*, 9.

27. In addition to the attack on DigitNotar, the Netherlands suffered other highly publicized incidents such as the hack on a municipal waste water system and the Pobelka botnet.

28. Kadri Kaska, "National Cyber Security Organisation: the Netherlands," *NATO Cooperative Cyber Defense Center of Excellence*, Tallinn, (2015): 8.

29. To be able to provide independent and well-considered advice, the CSR has a balanced composition, made up of an equal number of representatives of public and private parties (each hold seven seats). Scientific institutions hold four additional seats. The council has two co-chairmen: the government and private sector alternate with each other every meeting.

30. Dutch Cyber Security Council, "Home," https://www.cybersecurityraad.nl/index-english.aspx.

31. Dutch Ministry of Security and Justice, "National Cyber Security Strategy (NCSS 2)," 8.

32. United Nations Department of Economic and Social Affairs, "United Nations E-Government Survey 2016: E-Government for Sustainable Development," New York, (2016): 111 and 116, http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf.

33. Dutch Ministry of Security and Justice, "National Cyber Security Strategy (NCSS 2)," 3.

34. *Ibid*, 7.

35. National Cyber Security Centre, "What is the NCSC?", https://www.ncsc.nl/english/organisation.

36. *Ibid*.

37. Dutch Ministry of Security and Justice, "National Cyber Security Strategy (NCSS 2)," 26-28.

38. Some security-related investments are classified or not officially announced.

39. Global Conference on Cyberspace, "GCCS 2015," https://www.gccs2015.com. This event brought together senior leaders and decision makers from governments, private sector, and civil society around the world to The Hague in 2015 to promote practical cooperation in cyberspace, enhance cyber capacity building, and discuss norms for responsible behavior in cyberspace.

40. "Cyber Threats Call for Additional Measures," *The Hague Security Delta*, October 6, 2016, https://www.thehaguesecuritydelta.com/news/newsitem/749-cyber-threats-calls-for-additional-measures.

41. Ministry of Economic Affairs, Agriculture and Innovation, "Digital Agenda.nl," 28.

42. Melissa Hathaway's interview with Dutch officials, Washington D.C., December 11, 2016.

43. National Cyber Security Centre, "What is the NCSC?"

44. National Coordinator for Security and Counterterrorism, "National Manual on Decision-making in Crisis Situations – The Netherlands," https://english.nctv.nl/binaries/national-manual-decision-making-in-crisis-situations_tcm32-84092.pdf .

45. National Coordinator for Security and Counterterrorism, Ministry of Security and Justice, "Critical Infrastructure (Protection)," January 20, 2017, https://english.nctv.nl/topics_a_z/critical_infrastructure_protection/index.aspx.

46. Melissa Hathaway's interview with Dutch government officials, Washington D.C., March 28, 2017.

47. National Coordinator for Security and Counterterrorism, "ISIDOOR: Operational Cyber Exercise with Public and Private Partners," June 25, 2015, https://english.nctv.nl/current_topics/news/2015/ISIDOORoperationalcyberexercisewithpublicandprivatepartners.aspx.

48. National Cyber Security Centre, "ICT Crisis Management," https://www.ncsc.nl/english/Incident+Response/ict-crisis-management.html.

49. National Cyber Security Centre, "ICT Response Board," https://www.ncsc.nl/english/Cooperation/ict-response-board.html.

50. National Coordinator for Security and Counterterrorism, "Review of Policy on Critical Infrastructure," (July 2015).

51. *Ibid.*

52. National Coordinator for Security and Counterterrorism, "Successful international Exercise VITEX, May 13, 2016, https://english.nctv.nl/current_topics/news/2016/SuccessfulinternationalexerciseVITEX.aspx.

53. Among the four hypothetical scenarios: (1) the first one served to test the bounds of encryption and privacy policy and evaluated how the government might access key data sets or technologies during a national security crisis; (2) the second scenario highlighted a future of insecure IoT devices that are infected and harnessed to knock businesses off-line and affect citizens' safety; (3) the third scenario involved a significant breach of citizen data in which the government was the custodian – similarly to the breach of the Office of Personnel Management in the United States or other similar events in the United Kingdom or Canada; and (4) the fourth scenario evaluated an environment of government regulations and interventions in critical infrastructures, in which the government would challenge itself to not only consider future incident response challenges, but also the relevant policy implications of decisions it was making today and what outcomes might be achieved by 2021.

54. European Defense Agency, "Complex Cyber Crisis Management Exercise in Vienna," September 16, 2015, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2015/09/16/complex-cyber-crisis-management-exercise-in-vienna; and NATO, "NATO Holds Annual Cyber Exercise in Estonia," December 2, 2016, http://www.nato.int/cps/en/natohq/news_138674.htm.

55. National Cyber Security Centre, "Monitoring," https://www.ncsc.nl/english/Incident+Response/monitoring.html.

56. Melissa Hathaway's interview with Dutch government officials, Washington D.C., March 28, 2017.

57. Dutch Government, "National Cyber Security Strategy 2," 8.

58. Cyber Threat Assessment Netherlands, (2016): 10.

59. The Dutch Standardization Forum was established by the Minister of Economic Affairs in 2006 to ensure implementation of policies on electronic data exchange and (re)use of data and electronic services. This Forum supports the Dutch government in the development, use, and establishment of open standards for electronic information exchange. It also promotes interoperability within the Dutch government system and in the relations between government agencies, citizens, and enterprises, and it prevents vendor lock-in and reduces costs in government spending on ICT. For more see: "Dutch Standardisation Forum," https://www.forumstandaardisatie.nl/content/english.

60. Cyber Threat Assessment Netherlands, (2016): 62.

61. National Cyber Security Centre, "Factsheets," https://www.ncsc.nl/english/current-topics/factsheets.

62. Central Planning Bureau, "Cyber Security Risk Assessment for the Economy," (2016): 2; and Dutch Cyber Security Council, "Bedrijven doen nog te weinig aan digitale veiligheid," April 5, 2017, https://www.cybersecurityraad.nl/010_Actueel/Advies_zorgplichten_bedrijven.aspx.

63. The Hague Security Delta, "Trusted Networks Initiative," https://www.thehaguesecuritydelta.com/projects/project/60-trusted-networks-initiative.

64. National Cyber Security Centre, "Cyber Security Assessment Netherlands (CSAN) 2016," 60, and The Hague Security Delta, "Trusted Networks Initiative," October 22, 2014, https://www.thehaguesecuritydelta.com/projects/project/60-trusted-networks-initiative.

65. NLnet Foundation, "Collective Approach to Internet Attacks Big Success in the Netherlands," *Press Release*, June 30, 2014, https://nlnet.nl/press/20140630-nawas-en.html.

66. National Cyber Security Centre, "Cyber Security Assessment Netherlands," https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2016.html.

67. Central Planning Bureau, "Cyber Security Risk Assessment for the Economy," July 6, 2016.

68. Central Planning Bureau, "Cyber Security Risk Assessment for the Economy," (2016): 11.

69. Janene Pieters, "Dutch Parliament Approves Bill to Hack Criminal Suspects," *NL Times,* December 21, 2016, http://nltimes.nl/2016/12/21/dutch-parliament-approves-bill-hack-criminal-suspects.

70. Lexology, "The Netherlands – More Stringent Data Protection Law and a DPA that is Ready to Act in 2016," February 29, 2016, http://www.lexology.com/library/detail.aspx?g=ad2e6ff6-3f68-4b74-bddf-ddffce701466.

71. National Cyber Security Centre, "Cyber Security Assessment Netherlands," (2016): 62, and CPB, "Cyber Security Risk Assessment for the Economy," (2016): 44.

72. National Cyber Security Centre, "Cyber Security Assessment Netherlands," (2016): 64.

73. NWO, "NHTCU," https://www.dcypher.nl/nl/content/nhtcu.

74. *Ibid*.

75. Government of the Netherlands, "Crime and Crime Prevention," https://www.government.nl/topics/crime-and-crime-prevention/contents/investigation-and-prosecution-of-criminals.

76. Abuse Information Exchange, "Home," https://www.abuseinformationexchange.nl/english.

77. Jeroen Pijpker and Harald Vranken, "The Role of Internet Service Providers in Botnet Mitigation," *European Intelligence and Security Informatics Conference,* (2016): 26.

78. LookingGlass, Threat Intelligence Data, April 2017, https://www.lookingglasscyber.com.

79. "Cyber Security Assessment Netherlands 2016," 62.

80. National Cyber Security Center, "Cooperation," https://www.ncsc.nl/english/Cooperation/public-private-partnership.html.

81. The Platform for the Information Society or ECP (Platform voor de Informatie-Samenleving) is an independent and neutral platform where government, business, and civil society work together and share knowledge on the impact on and responsible application of new technologies in the Dutch society.

82. National Cyber-Forensics & Training Alliance, "Become a NCFTA Partner," https://www.ncfta.net.

83. National Cyber Security Centre, "Safer Internet Day," https://www.ncsc.nl/english/current-topics/news/safer-internet-day.html.

84. National Cyber Security Centre, "Responsible Disclosure Guideline," https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html.

85. CIO-Platform Nederland and Rabobank, "Coordinated Vulnerability Disclosure Manifesto," May 12, 2016.

86. National Coordinator for Security and Counterterrorism (NCTV), Ministry of Security and Justice, "Beleidsreactie Cyber Security Beeld Nederland 2016," September 15, 2016.

87. Confederation of Netherlands Industry and Employers (known as VNO-NCW), https://www.vno-ncw.nl/over-vno-ncw/english.

88. Government of the Netherlands, "Encouraging Innovation," https://www.government.nl/topics/enterprise-and-innovation/contents/encouraging-innovation.

89. Ministry of Economic Affairs, "Progress through Renewal: 2016 Enterprise Policy Report," 71.

90. *Ibid*, 6.

91. Deloitte, "2014 Global Survey of R&D Tax Incentives," (2014): 32, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Tax/dttl-tax-global-rd-survey-aug-2014.pdf.

92. Government of the Netherlands, "Encouraging Innovation."

93. Herbert Bos, Sandro Etalle, Frank Franse, and Erik Poll, "National Cyber Security Research Agenda II," Government of the Netherlands and NWO, (2013): 3 and 16-18, https://www.dcypher.nl/files/mediabank/NCSRA-II.pdf.

94. Dutch Government, "National Cyber Security Strategy 2," 10.

95. Dcypher, "About Us," https://www.dcypher.nl/en/content/about-us.

96. HSD Foundation, "About HSD," https://www.thehaguesecuritydelta.com/about.

97. HSD Foundation, "Opening TNO Cyber Threat Lab at HSD Campus," December 21, 2016, https://www.thehaguesecuritydelta.com/news/newsitem/788-opening-tno-cyber-threat-lab-at-hsd-campus.

98. HSD Foundation, "Funding for Research to Design National Cyber Testbed," April 4, 2016, https://www.thehaguesecuritydelta.com/news/newsitem/614-funding-for-research-to-design-national-cyber-testbed.

99. SBIR, "SBIR Cyber Security," September 25, 2014, https://www.dcypher.nl/files/downloads/Digital_Intelligence_Group_projectCyberscan.pdf.

100. Dennis Huele, "SBIR Cyber Security Tender III," http://www.rvo.nl/sites/default/files/2016/11/Presentatie_SBIR_cyber_security_tender_III.pdf.

101. US Department of Homeland Security, "Secretary Napolitano and Dutch Minister of Security and Justice Ivo Opstelten Sign Letter of Intent on Cybersecurity Cooperation," February 22, 2012, https://www.dhs.gov/news/2012/02/22/secretary-napolitano-and-dutch-minister-security-and-justice-ivo-opstelten-sign.

102. NWO, "Programme: Cyber Security," http://www.nwo.nl/en/research-and-results/programmes/cyber+security, and Deloitte, "2014 Global Survey of R&D Tax Incentives," (2014): 32.

103. QuTech, "About Us," https://qutech.nl/about-us/.

104. The Dutch national research institute for mathematics and computer science, Centrum Wiskunde & Informatica (CWI), is an institute of the NWO.

105. QuSoft, "About," http://www.qusoft.org/about/.

106. European Commission, "European Commission will Launch €1 Billion Quantum Technology Flagship," May 17, 2016, https://ec.europa.eu/digital-single-market/en/news/european-commission-will-launch-eu1-billion-quantum-technologies-flagship .

107. NWO, "Background," http://www.nwo.nl/en/research-and-results/programmes/cyber+security/background.

108. NWO, "Government and NWO Invest More Than 6 Million Euros in Cyber Security Research," November 14, 2013, http://www.nwo.nl/en/news-and-events/news/2013/ew%5B2%5D/government-and-nwo-invest-more-than-6-million-euros-in-cyber-security-research.html.

109. Netherlands Enterprise Agency, "Horizon 2020," http://english.rvo.nl/subsidies-programmes/horizon-2020.

110. Dutch Ministry of Security and Justice, "National Cyber Security Strategy 1: Success Through Cooperation," 8.

111. Based on estimations from Nederland ICT.

112. University of Amsterdam, "Computer Science: Education," http://www.uva.nl/en/disciplines/computer-science/education; and Universiteit Leiden "Cyber Security," http://en.mastersinleiden.nl/programmes/cyber-security/en/introduction.

113. Cyber Security Academy, "About the CSA," https://www.csacademy.nl/en/about-csa.

114. Francesca Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," *Pell Center,* March 2013, http://pellcenter.org/wp-content/uploads/2015/05/One-Leader-at-a-Time.pdf.

115. "Cyber Security Assessment Netherlands 2016," 43.

116. Rene Millman, "Dutch Watchdog Sues Samsung Over Lack of Security Updates," *SC Magazine*, January 22, 2016, https://www.scmagazineuk.com/dutch-watchdog-sues-samsung-over-lack-of-android-security-updates/article/531383/.

117. "Cyber Threats Call for Additional Measures," *The Hague Security Delta*, October 6, 2016, https://www.thehaguesecuritydelta.com/news/newsitem/749-cyber-threats-calls-for-additional-measures.

118. "Dutch Investments in ICT and Cybersecurity," 19.

119. Government of the Netherlands, "Speech by Minister Koenders at International Security Conference in Munich," February 12, 2016, https://www.government.nl/documents/speeches/2016/02/12/speech-minister-koenders-at-munchner-sicherheitskonferenz.

120. *Ibid*.

121. Government of the Netherlands, "International Security Strategy," (June 2013): 14, https://www.government.nl/documents/policy-notes/2013/06/21/international-security-strategy.

122. Dutch Government, "National Cyber Security Strategy 2," 17.

123. *Ibid*.

124. Janene Pieters, "Dutch Govt. Launches International Cyber Security Strategy," *NL Times,* February 13, 2017, http://nl-times.nl/2017/02/13/dutch-govt-launches-international-cyber-security-strategy.

125. Ministry of Foreign Affairs, "Factsheet Task Force Cyber," 2017.

126. Government of the Netherlands, "International Security Strategy" (2013): 9.

127. OSCE, "Permanent Council Decision No. 1106," December 3, 2013, http://www.osce.org/pc/109168, and OSCE, "Permanent Council Decision No. 1202," March 10, 2016, http:// www.osce.org/pc/227281.

128. The Global Forum on Cyber Expertise, “Overview,” https://www.thegfce.com/about.

129. The Hague Centre for Strategic Studies, “The Global Commission on the Stability of Cyberspace,” February 17, 2017, http://hcss.nl/news/global-commission-stability-cyberspace.

130. Dutch Government, “National Cyber Security Strategy 2,” 25.

131. Freedom Online Coalition, “About Us,” https://www.freedomonlinecoalition.com/about/.

132. Ministry of Foreign Affairs, “Factsheet Task Force Cyber,” 2017.

133. Melissa Hathaway’s interview with Dutch government officials, Washington D.C., March 28, 2017.

134. Ministry of Foreign Affairs, “International Cyber Strategy: Toward an integrated international cyber policy,” Section 3.4.

135. Ministry of Foreign Affairs, “International Cyber Strategy: Toward an integrated international cyber policy,” Section 3.2.

136. Minister of Defense Hans Hillen’s letter accompanying the 2012 “Defence Cyber Strategy,” June 27, 2012.

137. Ministry of Defense, “Defence Cyber Strategy,” (June 2012): 6 https://ccdcoe.org/sites/default/files/strategy/NDL-Cyber_StrategyEng.pdf.

138. Ministry of Defense, “Defence Cyber Strategy,” (February 2015), https://www.defensie.nl/english/topics/cyber-security/contents/defence-cyber-strategy.

139. General Intelligence and Security Service, “Joint Sigint Cyber Unit,” https://english.aivd.nl/about-aivd/contents/the-aivd-who-we-are.

140. Netherlands Defence Intelligence and Security Service, “DISS Annual Report,” (June 2013): 12.

141. Royal Netherlands Army, “Minister of Defence launches Defence Cyber Command,” September 25, 2014, https://www.defensie.nl/english/organisation/army/news/2014/09/25/minister-of-defence-launches-defence-cyber-command.

142. NATO’s Information Assurance and Cyber Defense Symposium, Mons, Belgium, September 17, 2014.

143. International Strategy Section 3.2

144. NATO CCDCOE, Statements by Brigadier General Hans Folmer at the 2016 International Conference on Cyber Conflict, https://ccdcoe.org/cycon/content/international-cyber-conference-opens-tomorrow-tallinn.html.

145. *Ibid.*

146. *Ibid.*

147. “Rijksbegroting,” chapter X, 111, http://www.rijksbegroting.nl.

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cyber security. She served in two US presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. Today, she is a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies. She is also a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs, a Distinguished Fellow at the Centre for International Governance Innovation in Canada, a non-resident Research Fellow at the Kosciuszko Institute in Poland, and she is President of Hathaway Global Strategies LLC, her own consultancy.

Melissa developed a unique methodology for evaluating and measuring national levels of preparedness for certain cyber security risks, known as the Cyber Readiness Index (CRI). The CRI methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is being applied to 125 countries. The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, the United Kingdom, and the United States can be found at the following link: *http://www.potomacinstitute.org/academic-centers/cyber-readiness-index*.

Having served on the board of directors for two public companies and three non-profit organizations, and as a strategic advisor to a number of public and private companies, Melissa brings a unique combination of policy and technical expertise, as well as board room experience to help others better understand the intersection of government policy, developing technological and industry trends, and economic drivers that impact acquisition and business development strategy in this field. She publishes regularly on cyber security matters affecting companies and countries. Most of her articles can be found at the following website: *http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html.*

Francesca Spidalieri Francesca Spidalieri is the co-principal investigator on the Cyber Readiness Index Project at the Potomac Institute for Policy Studies. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, as a Distinguished Fellow at the Ponemon Institute, and as 2017 Transatlantic Digital Debates Fellow at New America and at the Global Public Policy Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

All her additional studies can be found at the following link:
http://pellcenter.org/cyber-leadership/.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

The CRI 2.0 methodology is available in Arabic, Chinese, English, French, Russian, and Spanish, and is currently being applied to 125 countries.

The CRI country profiles of France, Germany, India, Italy, Japan, the Netherlands, the United Kingdom, and the United States can be found at the following link:

http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org