Rathenau Instituut

A never-ending race

On cyberthreats and strengthening resilience

Report

A never-ending race

On cyberthreats and strengthening resilience

Geert Munnichs, Matthijs Kouw & Linda Kool

A never-ending race
On cyberthreats and strengthening resilience

Geert Munnichs, Matthijs Kouw & Linda Kool

Rathenau Instituut
Anna van Saksenlaan 51
Correspondence address: Postbus 95366
NL-2509 CJ The Hague
Phone: +31 (0)70-342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl
Publisher: Rathenau Instituut

Editor: Redactie Dynamiek

Preferred citation:
Munnichs, G., M. Kouw & L. Kool, *A never-ending race. On cyberthreats and strengthening resilience*. The Hague, Rathenau Instituut 2017

Foreword

The study *A never-ending race. On cyberthreats and strengthening resilience* shows that the Netherlands, one of the most IT-intensive economies in the world, is an easy target for cybercriminals, cyberspies and other malicious hackers.

The title, *A never-ending race,* points to the ongoing rat race between attacker and target. We will always be caught up in this struggle. The race will never end.

So should we simply drop out of the race altogether? No, of course not. We can strengthen our resilience against cybercrime if we follow the report's recommendations. For example, it recommends establishing an independent expertise and advisory centre for SMEs. It also advises critical sectors (e.g. energy, telecommunications and finance) to agree on conducting an annual 'hack test'. A further recommendation is to assess the mandate of regulatory bodies such as the Authority for Consumers and Markets and the Radiocommunications Agency Netherlands to take action against unsecured digital products. Finally, it advises government – which purchases around thirty percent of all security product and services sold in the Netherlands – to do more to set an example as a 'launching customer'.

The Rathenau Institute undertook this study at the request of the Netherlands' National Coordinator for Security and Counterterrorism (NCTV) and the General Intelligence and Security Service (AIVD). It conducted a study of the literature, interviewed more than 25 experts and stakeholders, and organised two workshops.

In 2016, the Dutch House of Representatives passed legislation expanding the power of investigative agencies and the intelligence and security services. Protecting the legal status of citizens is a key point of concern in this legislation. It is our duty as a society to see that our built-in system of checks and balances is satisfactory and that there is adequate protection of our public values and human rights

The Netherlands enjoys an advantageous position at the cutting edge of IT in many areas. However, it can only retain that position if users, businesses and government exercise more vigilance. As far as I am concerned, cybersecurity is not only about being safe. It is also about our health, our autonomy, equal treatment and honest information. In short, it is about the society that we want to create together with the help of digital technology.

Dr. ir. Melanie Peters
Director, Rathenau Instituut

Contents

Foreword 6
1 Introduction 9
1.1 Growing dependence on IT 9
1.2 New vulnerabilities 9
1.3 Research questions 10
1.4 Approach 10
1.5 Reader's guide 11
2 Cyberthreats 12
2.1 Cyberthreats are inescapable 12
2.2 Script kiddies 12
2.3 Terrorists 13
2.4 Cybercriminals 13
2.5 Cyberespionage by state actors 15
2.6 Damage caused by cybercrime and cyberespionage 16
2.7 Manipulating information 17
2.8 Cybersabotage 17
2.9 The Internet of Things & DDoS 18
3 Cyber-resilience 19
3.1 User-friendliness more important than security 19
3.2 The public: limited resilience 19
3.3 Support needed for small and medium-sized enterprises 20
3.4 Greater awareness at larger enterprises 21
3.5 Concern for critical infrastructure 21
3.6 Limited resilience against cyberespionage 22
3.7 Too little coordination by government 23
3.8 Chain dependencies 24
3.9 Existing measures protecting critical sectors and government 24
3.10 Security is never entirely fool proof 26
4 Measures 28
4.1 Improve digital literacy 28
4.2 Security precautions 29
4.2.1 Arrange basic security 29
4.2.2 Detection and response 29
4.2.3 Set up a Digital Trust Centre 29
4.2.4 Strengthen the resilience of critical infrastructure 30
4.2.5 Have government set an example 30
4.3 Statutory measures 31
4.3.1 Expand powers of intelligence and investigative agencies 31
4.3.2 Enforcement and oversight 32
4.3.3 Duty of care and liability legislation 33
4.3.4 Report cybercrime and increase likelihood of apprehension 34

4.4 Expertise, capacity and budget 35
4.4.1 Develop expertise and build capacity 35
4.4.2 Increase the budget for cybersecurity 36
4.5 Economic opportunities 36
4.6 International context 36
4.6.1 The Netherlands' standing 37
4.6.2 International agreements 38
5 Conclusions and recommendations 39
5.1 The Digital Dutch 39
5.2 Conclusions 39
5.2.1 Rising cyberthreats 39
5.2.2 Inadequate resilience 40
5.3 Recommendations for strengthening resilience 41
5.3.1 Recommendations to improve security 41
5.3.2 Recommendations for statutory measures 43
5.3.3 Recommendations related to expertise and capacity 45
5.4 Economic opportunities 46
5.5 Learning to live with insecurity 46
5.6 Summary of recommendations 47
Bibliography 49
Annex 1: Interviewees 56
Annex 2: Workshop participants 58

1 Introduction

1.1 Growing dependence on IT

Dutch society is digitalising rapidly and the Netherlands is already one of the most digitalised countries in the world. Almost everyone here owns a computer, and more than 90 percent of all households and businesses use the internet. Digitalisation has made inroads into virtually every aspect of our lives. Examples include the growing use of online banking, web shops, wearables, streaming services such as Spotify and Netflix, and the rise of smart homes and self-driving cars.

The Dutch capital, Amsterdam, hosts the largest internet exchange in the world (the Amsterdam Internet Exchange or AMS-IX) and there are high-speed broadband telecommunications networks throughout the Netherlands. IT-related activity makes a substantial contribution to the Dutch economy; according to research and consultancy firm Dialogic, it accounted for around 36 percent of the Netherlands' economic growth between 1990 and 2013 (Dialogic 2014).

The Netherlands is also an important location for IT businesses. According to Herna Verhagen – CEO of the international mail company PostNL – the Dutch digital infrastructure may be regarded as the Netherlands' third 'mainport', alongside Schiphol Airport and the Port of Rotterdam (Verhagen 2016).

Dutch society and the Dutch economy are therefore becoming increasingly dependent on a properly functioning IT infrastructure and IT services. Digitalisation is expected to supplant a growing number of analogue products and processes. One recent example is the announcement by the Dutch Tax and Customs Administration that it would be doing away with printed tax returns in favour of online filing. The rise of the Internet of Things is leading to a growing number of connected devices. And the arrival of the 5G network allows us to send ever larger quantities of data in an ever-shorter space of time.

1.2 New vulnerabilities

The growing importance of IT has a downside, however: system failures have an immediate impact on societal and operational processes. The ubiquity of debit-card payments and online banking means that if the online payment system is paralysed for a few hours, large segments of the Dutch economy are disrupted. And as processes of all kinds continue to digitalise, they become more attractive targets for cybercriminals, cyberspies and other hackers. Viruses, phishing e-mails and DDoS attacks threaten the cybersecurity of the public, government and businesses. IT is making everyday life easier not only for Dutch citizens, public officials and business owners, but also for those with malicious intentions.

Recent hacks show how our growing dependence on IT makes us more vulnerable. For example, cybersecurity expert Mary-Jo de Leeuw showed a flabbergasted group of senior military officials how easy it is to hack a talking doll connected to the internet by having it utter death threats (*Het Financieele Dagblad* 2016). A hack can also have a major impact on society. That became clear from the leaking of internal e-mails of the DNC, the US Democratic Party's governing body, an incident that the US Intelligence Community has ascribed to Russian hackers intent on influencing the outcome of the 2016 presidential election. And the fact that hackers were able to steal malicious software from the US National Security Agency (NSA) in 2016 shows that no one is immune to cyberattacks (Nakashima 2016).

1.3 Research questions

The question raised by the foregoing examples is: can the Netherlands cope with this new category of threat, which is closely associated with the digitalisation of society? It was with this question in mind that the National Coordinator for Security and Counterterrorism (NCTV) and the General Intelligence and Security Service (AIVD) asked the Rathenau Institute to undertake a study.

The key questions addressed in the study are: Which cyberthreats are on the horizon, up to the year 2020? How resilient is Dutch society against these threats? Does the level of resilience need to be strengthened, and if so, what steps should we be taking?

Further questions are also pertinent. Does cybersecurity represent an opportunity for the Dutch economy? Can we detect any trends based on existing statistics? How does the Netherlands compare with other countries when it comes to cybersecurity? What makes it distinctive, and what not?

The recommendations arising from this study are largely, but not exclusively, meant for the Dutch government and policymakers. This study does not cover cyberthreats as part of open conflict or situations of war.

1.4 Approach

We surveyed opinions concerning cyberthreats, resilience and possible measures by studying the literature and interviewing various experts and stakeholders in society. Bertruke Wein and Rob Willems, both affiliated with Radboud University, conducted most of the interviews. Jasper Veldman, Leonie Hermanussen, Tommy van der Vorst and Reg Brennenraedts of Dialogic performed the trend analysis (based on existing numerical data) and the international benchmark.

We organised two workshops with experts and stakeholders to discuss the provisional findings of our literature study and interviews, including those measures deemed necessary to improve our resilience against cyberthreats. The workshops took place on 13 December 2016 and 10 January 2017; for a list of interviewees and workshop participants, please see Annex 1 and Annex 2 respectively.

This study describes the findings of our research and the workshops. We have also incorporated the main findings of the trend analysis and international benchmark.

1.5 Reader's guide

The subsequent chapters describe the outcomes of the study. Chapter 2 identifies the most serious cyberthreats to Dutch society. Chapter 3 describes how resilient Dutch society currently is against these threats. Chapter 4 discusses possible measures to strengthen our resilience against cyberthreats and how they might also benefit the Dutch economy and the Netherlands' standing in that international domain. Chapter 5 summarises the report and presents its main conclusions and recommendations; a concise summary of the recommendations can be found in Section 5.6.

At various points, this report refers to 'interlocutors'. These are the interviewees or workshop participants.

2 Cyberthreats

2.1 Cyberthreats are inescapable

In theory, everything that contains IT can be hacked. IT is inherently insecure. Software consists of many lines of code, sometimes running into the millions, and errors and imperfections are unavoidable. These vulnerabilities – found in both software and hardware – often come to light only when they are exploited by malicious parties.

Chapter 1 already pointed out that IT not only makes the everyday life easier for ordinary people but also for criminals, spies and other subversives. This chapter describes the main threats associated with the progressive digitalisation of society. As our interviews and workshop discussions revealed, these threats have now become inescapable in our society. The threats that we encounter in the real world – vandalism, crime, espionage, terrorism – are also present in the digital domain. And the motives behind the attacks are as numerous as those in the real world. Criminals are intent on financial gain, spies want to ferret out valuable information, and terrorists aim to disrupt the system. But a workplace conflict or mischievous teenager are also likely sources of cyberattacks.

Compared with traditional types of crime and espionage, cybercriminals and cyberspies have an easier time undertaking large-scale, transfrontier operations. The internet transcends national borders, and a single attack may affect thousands or even millions of people. On top of this, it is often far from clear who is behind a particular attack and the evidence is hard to come by. That makes it difficult to go after the culprits (AIVD 2016; 2017).

The scale of the threat also depends on the attackers' skills and the tools that they have at their disposal. As we will see in this chapter, the average secondary school pupil or petty criminal possesses neither the cyberskills nor the efficiency of organised criminals or foreign intelligence services. Not all threats are the same, in other words, although a teenager's hack can still wreak considerable societal or economic havoc.

This chapter describes the various threats we face in ascending order of attack complexity and hacker skills, starting with 'script kiddies' (who have only limited cyberskills and tools) and ending with state actors, capable of mounting highly sophisticated hacks. It also addresses the societal and economic damage caused by cybercrime and cyberespionage.

2.2 Script kiddies

Cybervandals and script kiddies are usually minors who commit attacks from pure mischief or to flaunt their own skills. Cybervandals have varying levels of skill, and script kiddies (or 'skiddies') are generally low-skill. According to *Cyber Security Assessment Netherlands 2016,* they are a growing threat owing to the increasing availability of low-threshold tools for mounting digital attacks. For example, it is becoming easier for cybervandals and script kiddies to carry out DDoS attacks (distributed denial of service) that shut down entire websites by using services traded on the dark web (‘DDoS-as-a-service’). As a result, a lack of money and skill does not prevent them from carrying out an effective attack (NCSC 2016). According to Scott and Spaniel, commissioning a 24-hour attack against a designated target only costs between $ 25 and $ 150, on average (Scott & Spaniel 2016).

This low-threshold access to DDoS attack tools is part of a more general pattern. Attack tools that were once available only to advanced hackers eventually find their way to parties who have less knowledge and experience, such as petty criminals or even script kiddies.

2.3 Terrorists

Terrorist groups do not appear to have the IT skills necessary to commit serious cyberattacks yet, but it is only a question of time.

The Islamic terrorist organisation ISIS is taking the digital offensive more often, however, and its cyberattacks are becoming more targeted. For example, it has stepped up its doxing activity, i.e. it collects personal data on Western military and government personnel and publishes it online to single them out as targets for attack (AIVD 2016).

ISIS or its sympathisers are also having more success at defacement, i.e. hacking websites and replacing the original content with their own ideological content. Such attacks are not regarded as terrorist activities in themselves, but as propaganda (NCSC 2016).

2.4 Cybercriminals

Cybercrime is increasingly turning into a form of organised crime. Cybercriminals are becoming more professional, the methods they employ are growing more complex, and their revenue model is proving more profitable all the time. Malware infections are increasing in number, botnets are getting harder to detect and spear phishing is growing more common. This advanced form of phishing targets individual internet users and uses personal data, for example information that the targets themselves have posted on their Facebook or LinkedIn page. A seemingly innocent e-mail attachment that appears to come from a known source can thus lead to unpleasant surprises (NCSC 2014; 2015).

Ransomware has become extremely commonplace in recent years. Individuals, businesses and even hospitals have experienced a growing number of ransomware infections. In these attacks, the malware encrypts the computer files, making them inaccessible, and the attacker demands a ransom to decrypt the files. Businesses infected by ransomware are often prepared to pay the ransom to ensure the continuity of their operations. However, there are no guarantees that decryption will in fact take place after the ransom is paid. Ransomware appears to have become a successful revenue model for criminals. According to the Netherlands Bureau for Economic Policy

Analysis (CPB), ransomware costs very little to use but generates an estimated criminal revenue of € 70,000 to € 1,500,000 (CPB 2016).

Ransomware is growing more sophisticated. Untargeted ransomware infections are increasingly giving way to phishing e-mails aimed at specific users or organisations. The nature of the ransomware is also changing. For example, recent attacks also encrypted backups, which are intended precisely to protect against such infections (NCSC 2016).

A professional criminal class has emerged in recent years that delivers cybercrime-as-a-service. Such services permit less skilled criminals to carry out attacks, as we have already seen in the example of script kiddies. Services include stolen credit card information, e-mail account information, ready-made malware (including ransomware) and DDoS attacks. Some cybercrime service providers even run helpdesks that offer round-the-clock support. The rise of digital currencies like the bitcoin facilitates these services (NCSC 2014; 2016).

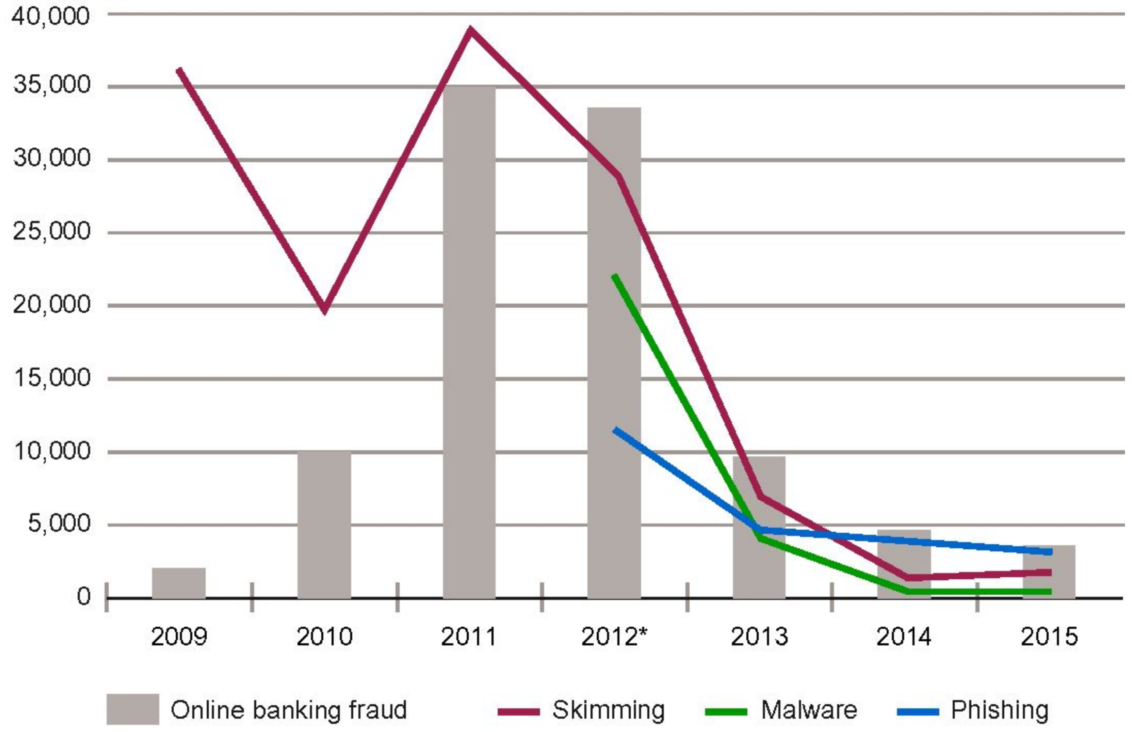
Banking sector a popular target

The banking sector is an interesting case in many respects. Banks have long been a popular target for cybercriminals, in part owing to the rapid growth of online banking in the Netherlands in recent years. As Figure 1 shows, online banking fraud skyrocketed between 2009 and 2011. In 2011, it caused 35 million euros worth of damage. After 2012, however, there was a sharp drop in this figure. By 2015, the damage had declined to 3.7 million euros (NVB 2016).

This decline is the result of steps taken by the Dutch financial sector, including public information campaigns warning account holders about fraud, and the tracking of suspect transactions. Criminals have responded by looking for other targets. Instead of attacking individuals or groups of private account holders, they now attack corporate clients and bank staff (NCSC 2016).

This example not only shows that cybercrime can be tackled successfully but also that criminals are constantly seeking new ways to attack. If ordinary phishing e-mails are no longer enough to relieve people of their money, they turn to more sophisticated methods such as spear phishing. And as soon as banks clamp down on attacks targeting their private account holders, the criminals shift their attention to the financial institutions themselves.

Figure 1: Damage caused by online banking fraud (x 1000 euros).



* Since 2012, fraud reporting has differentiated between phishing, malware and other types of fraud.

Source: NVB (2016), 'Factsheet Veiligheid en Fraude'.

2.5 Cyberespionage by state actors

In addition to cybercriminals, state actors – foreign intelligence services and allied groups – are extraordinarily active in the digital domain. Russian and Chinese intelligence services are particularly keen to collect political, military, scientific and technological information in the West. For example, the Russian intelligence services gather data on the West's views and positions on geopolitical issues. These intelligence services are highly professional and run extremely effective operations. It is estimated that Russia and China deploy upwards of a hundred thousand persons in cyberespionage worldwide, and other countries, including Iran, are also active. The Dutch government has long been the target of vast and advanced cyberespionage. Cyberattacks by state actors are thus a constant threat to national security (AIVD 2016; MIVD 2016).

Alongside political targets, espionage also commonly focuses on economic targets. The Chinese intelligence services are especially interested in economically sensitive business information that will help China gain an economic advantage. The targets include businesses that form part of the Netherlands' top economic sectors. According to the AIVD, those perpetrating the attacks seek specialist technology, and even experimental technology that has yet to demonstrate its market value (AIVD 2016). Economic espionage can therefore cause immeasurable damage to the organisations affected.

State actors use highly sophisticated methods that can circumvent most security systems and are often difficult to detect. The advanced nature of such attacks often obscures the identity of the attacker. Many of these hostile campaigns use spear phishing to gain access to a network. Once the attacker has gained a foothold, it may take months or even years before the espionage is discovered (NCSC 2015). The businesses targeted are often unaware of the espionage, while the attackers often manage to acquire the highest-level permissions giving them access the target's digital infrastructure (Verhagen 2016). An attacker can reign over the network it has breached and stay one step ahead of any new security measures that the victimised organisation implements.

The quality and bandwidth of the Dutch IT infrastructure make it highly attractive to outside parties as a transit port for DDoS attacks or cyberespionage against other countries (AIVD 2016).

2.6 Damage caused by cybercrime and cyberespionage

Cybercrime can cause enormous societal and economic damage. According to figures published by Statistics Netherlands, around 11 percent of the Dutch population have at some point been victims of cybercrime (CBS 2016). A study by PwC and VU University Amsterdam revealed that more than 20 percent of Dutch businesses and institutions reported incidents of cybercrime in the previous two years. According to the researchers, the actual figures are 'very likely' to be higher (PwC & VU 2014).

Estimates by Deloitte indicate that cybercrime costs the Dutch economy some 10 billion euros a year (Deloitte 2016). Verhagen cites a figure of around 15 billion but warns that the true scale of the damage remains unknown (Verhagen 2016).

These figures are unverified, however, making it almost impossible to draw definitive conclusions about the actual damage (Overvest & Straathof 2015; Hendriks et al. 2016). According to the Netherlands Bureau for Economic Policy Analysis, it is difficult to quantify either the importance of cybersecurity for the economy or the economic damage arising from cybercrime. The Bureau claims that estimates are generally based on experts' best guesses and on 'impenetrable methodologies' (CPB 2016).

The damage caused by economic cyberespionage is even more difficult to establish because it may only become clear in the longer term (NCSC 2016).

Cybercrime and cyberespionage are serious threats. If Dutch businesses are subject to large-scale cybercrime attacks, and if foreign intelligence services manage to access information about advanced technologies – one of the main pillars of the Dutch economy – then these threats will eventually undermine the innovativeness and competitiveness of the Dutch business sector (Verhagen 2016).

2.7 Manipulating information

State actors can also deploy digital tools to influence public opinion, political stability or decision-making processes in other countries (NCSC 2016). The manipulation of information is thus a threat to the functioning of the democratic system.

Such attacks include the deliberate dissemination of fake news and the above example of an alleged Russian hack and leak of Democratic Party e-mails in the US, presumably to influence the 2016 presidential election. Other Western countries are very concerned about the manipulation of news reporting by foreign powers. That is the case in Germany in the run-up to their general election in 2017. For example, misleading information has been distributed about criminal activity among migrants, potentially boosting the popularity of Eurosceptic parties such as Alternative für Deutschland. The German intelligence and security services regard such manipulation as part of a longstanding Russian cyberattack on Germany (*Deutsche Welle* 2016a; 2016b).

The European Union has sought to counter Russian propaganda by establishing the East StratCom Task Force. According to this body, Russian hackers are exceptionally active and are operating a large-scale, organised disinformation campaign targeting the European Union (Alonso 2017).

2.8 Cybersabotage

Cybersabotage is another serious risk. A deliberate attack on critical sectors, for example power plants, drinking water supplies or payment systems, can cause enormous economic damage and social disruption (Verhagen 2016). The internet itself can be regarded as critical infrastructure. A DDoS attack that disables the internet will have major consequences for the economy and society.

Foreign military intelligence services are increasingly hacking into industrial control systems (or SCADA systems) operated by enterprises in critical sectors, for example. Future conflict situations could involve the manipulation or impairment of such systems (MIVD 2016).

There are no known instances of external actors engaging in successful sabotage in the Netherlands (NCSC 2016), but that cannot be said of other countries. For example, in 2007 Estonia battled a series of serious DDoS attacks, presumably by Russian hackers. The attacks disabled a number of news and government websites and took Estonia’s largest bank offline for more than an hour. The bank suffered more than a million dollars of damage. The culprits are said to have been Russian hackers who were seeking revenge for Estonia's removal of the Bronze Soldier Soviet Second World War memorial in Tallinn (Landler & Markoff 2007; Davis 2007; Traynor 2007).

In 2015, an attack on Ukrainian electricity companies left around a million people without power. The perpetrators, allegedly a Russian hackers’ collective, hacked into the electricity companies’ IT systems, allowing them to stymie operations. It was six hours before the power supply could be restored (NCSC 2016; Trend Micro 2016).

2.9 The Internet of Things & DDoS

A fairly recent development that may well increase the impact of various cyberthreats is the emergence of the Internet of Things. A growing number of devices, including household appliances, wearables, TVs, self-driving cars and medical equipment, are now connected to the internet. Many of these ‘smart devices’ are not properly secured, for example because their users employ standard passwords, the software is difficult to update, or the supplier no longer supports them after a certain period.

The growing number of smart devices is opening the door to cybercriminals wider every day. That is true not only for individual users’ home networks but also for business and government networks. A single weak link in a network, in the shape of an inadequately secured device, gives hackers access not only to the network itself but also to other devices connected to it. That makes it easy for cybercriminals to steal, misuse or manipulate personal data or other important information.

Hacked devices can also be used as part of a large-scale network for carrying out DDoS attacks. Recent incidents involved hundreds of thousands or even millions of connected devices, adding considerably to the ferociousness of the attacks. If a DDoS attack is severe enough, it will ultimately disable any connected IT system.

One recent example of a major DDoS attack took place in October 2016. The target was the cloud and network infrastructure firm Dyn (Hilton 2016). The first wave of attacks targeted Dyn data centres in Chicago, Washington DC and New York mainly affecting users on the US East Coast and disabling Twitter, Netflix, Spotify, GitHub and other popular websites for two hours. The second and third waves hit Dyn data centres worldwide and lasted for several hours. The attackers gained access by hacking into digital video recorders, printers and other connected devices. The attacks may have infected some 100,000 devices (Hendrikman 2016). Two hackers’ groups, Anonymous and New World Hackers, both claimed responsibility, but their claims have not been substantiated. A security firm suspects script kiddies because some of the attack infrastructure was used to infect a gaming company (Security.nl 2016).

Like ransomware, DDoS attacks can be used for other purposes, such as extortion. The attackers first carry out a small DDoS attack and let the targeted organisation know that they plan to stage a much larger attack later unless it pays. Managed service providers claim that they deal with extortion attempts every week. So far, a refusal to pay ransom has not led to a larger attack (NCSC 2016).

An international expert meeting organised by the Netherlands Cyber Security Council (CSR) concluded that the rise of the Internet of Things constitutes one of the most disruptive present-day developments and a major cybersecurity challenge (CSR 2016).

3 Cyber-resilience

3.1 User-friendliness more important than security

The cyberthreats described in Chapter 2 lead us to question how resilient Dutch society actually is. The short answer is that the public, businesses and government are not resilient enough in many cases. Too often, cybersecurity is not a priority in everyday life. We tend to assess IT applications mainly on their functionality; user-friendliness is more important than security.

That is not to say that Dutch society is unaware of the potential risks posed by the increasingly widespread use of IT. Such awareness has been raised by headlines concerning data breaches in the health care sector, Russians hacking US Democratic Party emails, and Edward Snowden's revelations about the US National Security Agency. At the same time, however, the public, businesses and the authorities have insufficient knowledge or understanding of the precise risks they are running and what to do about them. Risk is often an impalpable factor, and the need to take action is ignored until something finally goes wrong. For example, the 2011 hack of Diginotar, a firm responsible for securing government websites, was an important wake-up call for the Dutch government.

Not everyone is a likely cyberattack target and the level of risk also differs from one target to the next. The average person or small business owner will generally have little to fear when it comes to cyberespionage or sabotage by foreign intelligence services, and if such an attack were to occur, he or she would be utterly helpless anyway. Conversely, large organisations that have access to the right expertise and tools generally have less to fear from script kiddies or petty criminals.

In the following, we discuss the resilience of various (potential) targets in order of their ability to resist cyberthreats, from the public, consumers and small companies with low-level cyberskills and tools up to large corporations and organisations with extensive security capabilities.

3.2 The public: limited resilience

The Dutch are international trailblazers when it comes to adopting IT in their everyday lives, but their cyberskills have not kept pace, certainly not when it comes to cybersecurity. According to the annual Alert Online survey, the Dutch barely get a passing mark in that respect.

Anti-virus software is by far the most common method used by the Dutch to protect themselves against cyberincidents. A quantitative study by market researcher Gfk of online behaviour shows that 71 percent of the individuals surveyed update their software automatically. Other basic security measures are much less common, however, for example making backups, using strong passwords, or changing settings so that devices do not connect automatically with WiFi networks (Gfk 2015). It is precisely these measures that are most important, given the growing use of ransomware by cybercriminals and the rising number of connected devices consumers are purchasing.

People tend to be more vigilant about the dangers of phishing e-mails. The vast majority claim that they delete suspect e-mails immediately and do not click on suspicious links. Half of those surveyed by Gfk also claim that they recognise phishing e-mails immediately. They are less familiar with relatively new cybercrime techniques, such as ransomware and spear phishing. For example, 65 percent of the respondents did not know the term ransomware (Gfk 2015).

Nevertheless, it cannot be said that the public underestimates the dangers lurking online. For example, only 43 percent of the respondents feel that they have adequate protection against online threats, and half believe that malicious actors will succeed in the end. They therefore assume that they cannot really protect themselves against major threats.

The rise of the Internet of Things is creating new risks for the public. Because many connected devices – including consumer electronics – are inadequately secured, users are not only susceptible to data breaches and ransomware but also to device manipulation or impairment. There are known instances in which hackers gained remote access to insulin pumps and controlled the dosage, or to automobiles whose brakes they then disabled (Greenberg 2015; Keijzer 2016).

Infected devices can also become part of a botnet used to carry out DDoS attacks, as we saw in Chapter 2. The device's owner may be unaware that their smartphone or tablet is facilitating an attack and causing damage. Unsecured devices therefore not only put individual end-users at risk but are also a potential threat to critical or other IT infrastructure. Hacks of inadequately secured devices can have serious consequences. They can lead to social disruption (attacks on critical sectors) and even end up killing users (hacked insulin pumps or automobile brakes).

Although we may question the ease with which all sorts of consumer products – right down to refrigerators and toasters – are being connected to the internet, it is becoming ever more difficult to reverse this trend. In fact, consumers often have little choice nowadays. The government and energy companies want a smart thermostat in every household, and the standard television today is a smart TV. It is pointless for average citizens to try securing these types of devices on their own, however.

Market failure

One related problem is the absence of economic incentives that might induce IT providers to make devices more secure. Providers compete fiercely on price and cannot afford to offer robust security for such a low price. On top of that, consumers are not insisting on security improvements. Because it would nevertheless be better for society to have secure IT devices, we can regard this as a form of 'market failure' (CPB 2016).

3.3 Support needed for small and medium-sized enterprises

The situation for small and medium-sized enterprises (SMEs) is similar to that of the public. Small businesses generally have only a limited understanding of the risks to which they are exposing themselves and they lack the tools, expertise or access to knowledge needed to take the appropriate steps (Verhagen 2016). IT providers do offer all sorts of security products and services, but many SMEs are unable to weigh up the pros and cons of different solutions and identify the right products and services for them. The Netherlands Bureau for Economic Policy Analysis refers to a ‘knowledge asymmetry’ between IT providers and IT users. And because businesses do not know what they are looking for in a security system, price is often the deciding factor (CPB 2016).

Basic security is often inadequate at SMEs. They fail to use strong passwords, do not update their security software regularly, and neglect to make frequent and proper backups of important files. Another issue is that businesses may be induced to purchase what they consider an innovative IT solution without having enough knowledge to use the software properly or without thinking clearly about the threats to which they are actually exposed. They may feel they are properly protected without actually being so.

In many cases, technology alone is not the answer. The weakest link is in fact the laptop, PC or tablet user on staff. Spear phishing e-mails can easily tempt recipients to click on infected links. One added problem is that work and private life often overlap when it comes to IT. Malware on a home computer or tablet can end up infecting the IT system at work.

SMEs have an urgent need for independent advice and support when deciding on appropriate security measures. Because the SME sector is made up of a large and highly diverse group of businesses, ranging from freelancers to companies with 250 employees, the necessary measures depend on the type of company and the specific sector in which it operates. About 97 percent of Dutch trade and industry consists of SMEs. Their lack of resilience is therefore a serious problem.

3.4 Greater awareness at larger enterprises

Larger enterprises are generally more aware of their cybersecurity risks and can engage cybersecurity experts to help protect their organisation. At times, however, it may be difficult to convince senior executives of the need to invest in security measures; they may be quick to regard cybersecurity as a ‘negative investment’ because it does not produce any direct benefits. An associated problem is that cyber-risks are difficult to quantify.

Another issue is that not all mitigating measures are equally effective. Security measures are often meant to prevent attackers from gaining access to IT networks, but more persistent or more skilled hackers will succeed anyway in the end. Once they are inside, it may be quite a while before anyone notices their presence, but businesses often neglect to implement security measures geared towards detecting hacker activity (AIVD 2016; 2017).

3.5 Concern for critical infrastructure

The failure of critical infrastructure, such as the supply of energy and drinking water and payment transfer systems, can wreak havoc in society and the economy. The National Cyber Security Centre

(NCSC) supports these critical sectors by lowering the risk of failure and by acknowledging and neutralising threats.

Critical sectors are diverse in nature and their level of resilience differs. The energy, telecommunications and financial sectors appear to have a satisfactory level of resilience. In fact, the Dutch banking sector is regarded as innovative in this respect, even by international standards. We have already noted that Dutch banks have been successful at frustrating criminal attacks against private account holders. They have also invested heavily in security against DDoS attacks, for example by contracting specialist firms that provide cybersecurity-as-a-service. Although these safeguards are expensive, they have become ‘business as usual’ (NCSC 2016).

Even here, however, the weakest link is often the person behind the PC, laptop or tablet who neglects to keep basic security up to scratch and favours user-friendliness over security.

According to one of our interlocutors, critical sectors are too sluggish about developing emergency scenarios, for example in the event of a major attack. Backup facilities meant to keep critical processes running in emergencies still leave much to be desired. There is friction here between the cost of an emergency facility with little commercial appeal and the need to serve the public interest by guaranteeing the continuity of critical processes.

Chain dependencies also play a role in critical infrastructures. Vulnerabilities can arise when the organisations in the chain all use the same hardware and software or when multiple organisations contract the same service or service provider and create a ‘single point of failure’. If problems arise with that shared service or service provider and multiple organisations in the chain experience the same failure, it becomes more difficult to cope with the fallout. Voster and De Bruijn recommend a review of dependencies within certain services and prioritisation in those areas that face the greatest risks (Voster & De Bruijn 2016).

3.6 Limited resilience against cyberespionage

Cyberespionage by state actors is a vital concern for both critical sectors and the national government. The AIVD is capable of tracking espionage attacks by detecting unusual patterns in data traffic within IT networks. If the AIVD detects espionage, it informs the target where possible and advises on an appropriate response. This might involve disconnecting and cleaning the infected system. If the infection has already infiltrated deep into the system, all physical hardware may need replacing. That was the case after a major attack on the German parliament in 2015 (*Die Welt* 2015).

The AIVD focuses on detecting and protecting against cyberespionage targeting the national government and part of the Netherlands’ critical infrastructure. Owing to its limited capacity, the AIVD cannot oversee the entire field and detect all espionage attacks, nor can it resolve all incidents that have been detected. The attacks that it does detect are merely ‘the tip of the iceberg’ (NCSC 2016). Under current legislation, the AIVD also has only limited authority to monitor internet traffic.

3.7 Too little coordination by government

Generally speaking, the national government seems reasonably aware of the cybersecurity risks that it faces. Like the critical sectors, it has the assistance of the NCSC and the AIVD. Data security at national level is provided by the Information Security Baseline for National Government (BIR). Issued in 2012, the BIR consists of a list of mandatory standards and non-mandatory best practices. It is meant to support safe cooperation and data-sharing among national government agencies (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2012).

That does not mean that security is always as it should be. The government does not always have enough expertise at its disposal leading to the ‘fragmented’ procurement of cybersecurity services, for example (Hendriks et al. 2016). There are also problems phasing out obsolete software. The Netherlands Court of Audit claims that, while government ministries now have a clearer notion of security risks and have drafted plans to lower those risks to an ‘acceptable level’, data security within national government still requires a lot of work in the years ahead (Algemene Rekenkamer 2016a).

In 2015, for example, the Court found – for the third year in a row – that the DigiD authentication system meant to enable communication between Dutch citizens, the government and care institutions did not comply with the NCSC’s security standards for web applications (Algemene Rekenkamer 2015a). A year later, the Court once again warned that the DigiD system failed to satisfy the data security requirements, even after various improvements, and that further action was required (Algemene Rekenkamer 2016b).

The Court of Audit also found security risks associated with physical infrastructure, for example bridges, roads and locks, which is the responsibility of RWS (Rijkswaterstaat, the national public works agency). The biggest risk factor, the country’s dykes and dams, appeared to be properly secured, however (Algemene Rekenkamer 2015c). By 2016, RWS’s security risks had been reduced to a ‘point of concern’ (Algemene Rekenkamer 2016c).

The most common problems in health care are a lack of awareness and deficient security measures. When Deloitte conducted a phishing study among 65,000 employees at 28 hospitals, an average of 17 percent of staff clicked on the link in the e-mail, and a majority of those who did (12 percent) entered personal data on the website to which they had been directed (Van Beurden 2016). The health care sector also struggles with massive breaches of privacy-sensitive information (Van Lonkhuyzen 2016).

In general, it appears that the importance of cybersecurity is often underappreciated in national government, with security in last place on the list of priorities. Price is often the deciding factor in public procurement procedures. A further aspect is that government responsibility for cybersecurity is shared among different ministries, resulting in fragmented policy coordination and governance (Verhagen 2016). Various interlocutors also pointed out that the various ministries have differing interests, and that government-wide assessment and oversight is therefore lacking.

The issue of data security is even pressing within the lower tiers of government. For example, in 2016 almost a third of municipal authorities reported breaches of citizens' personal data, and 15 percent had faced a data breach after a cybercrime attack (Van Lonkhuyzen 2017).

3.8 Chain dependencies

More and more IT applications are interconnected. Businesses, government and quasi-government organisations, and those who operate critical infrastructure often procure network-based products or services (hardware, software, cloud services, data storage) externally. No single organisation is capable of carrying out all the relevant tasks on its own anymore. Organisations often misjudge how vulnerable their dependence on external companies and service providers makes them. The weakest link can cause disruptions farther down in the chain, and in critical sectors that could very well lead to widespread system failure and social disruption.

Chain dependencies and the associated vulnerabilities also apply in the case of digital services procured by smaller users, such as web shops or SMEs. They often depend on multiple parties to provide these services (data centres, cloud services, internet service providers) but are incapable of ascertaining just how secure they actually are. And when something goes wrong, it is often unclear who is responsible. At the moment, that responsibility is too often borne by the end-user.

3.9 Existing measures protecting critical sectors and government

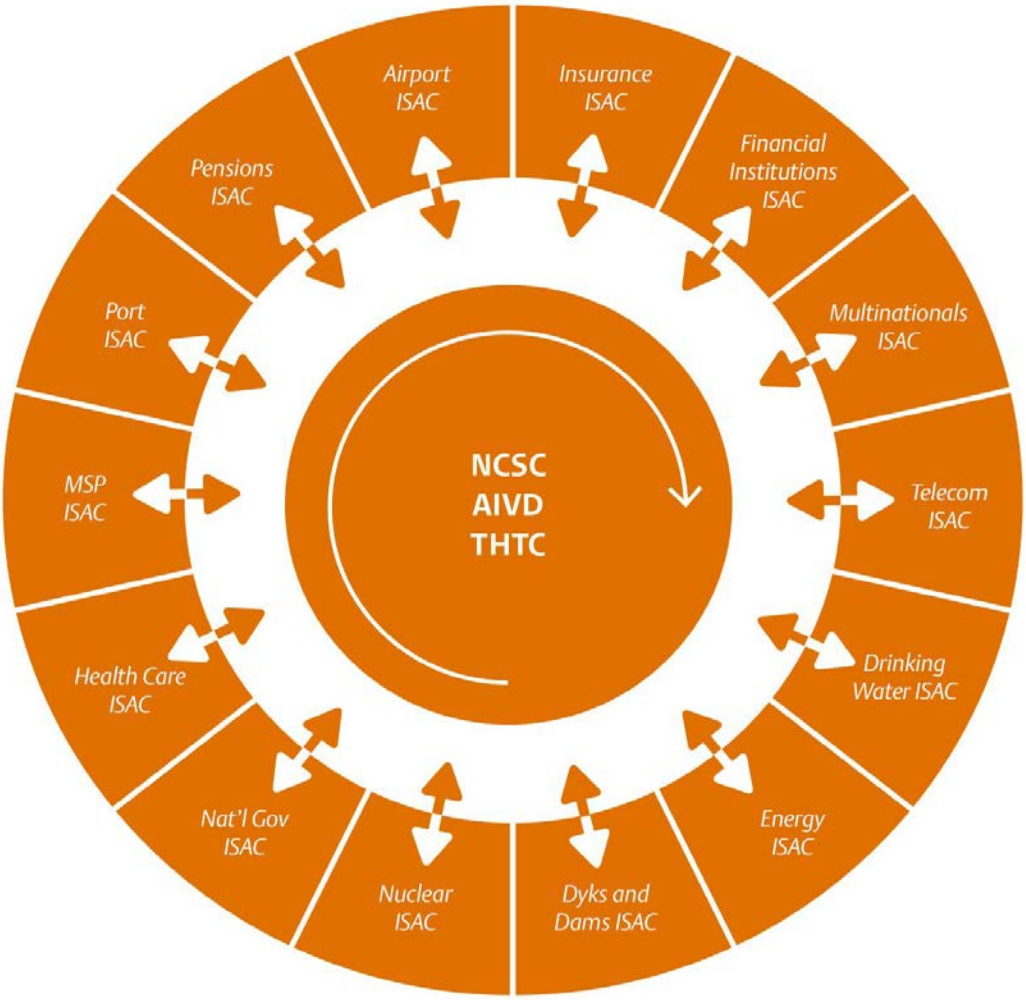
ISACs

To strengthen critical sectors' resilience against cyberthreats, the Dutch government has established seventeen Information Sharing and Analysis Centres (ISACs). The NCSC supports these centres. They can be found in the following sectors: financial, multinationals, telecoms, water supply, energy supply, dykes and dams, nuclear installations, national government, health care, managed service providers, ports, pensions, airports and insurance (see Figure 2).

ISACs are public-private partnerships in which businesses share cybersecurity information and lessons learned. The aim is to provide a comfortable environment in which they can learn from and assist one another in the event of problems. The partnerships make it possible to fight off complex attacks, something that is often impossible for individual businesses to do on their own (Verhagen 2016). Crucially, the partners must be willing to share confidential information (ENISA 2015). The Netherlands' ISAC system puts it at the forefront of international developments in this arena.

The NCSC informs ISAC member organisations about vulnerabilities and offers them advice. It does not regard it as its task to monitor whether organisations actually follow its advice and introduce patches; that is up to the organisations themselves. The NCSC considers that monitoring would not be conducive to building a trust relationship because organisations might be less inclined to share information. The organisations share the NCSC's views in this regard (Inspectie Veiligheid en Justitie 2015).

Figure 2: Information Sharing and Analysis Centres (ISACs).



Source: https://www.ncsc.nl/samenwerking/isacs.html

The NCSC's security recommendations are considered authoritative, making it easier for members to persuade their senior executives of the need to introduce measures. The NCSC's autonomy is another important factor, given the individual commercial interests of IT product suppliers and service providers (Inspectie Veiligheid en Justitie 2015).

There are also risks involved in making the relevant organisations responsible for repairing vulnerabilities that have come to light. As will have become clear, security is not always ideal in critical sectors. According to various interlocutors, that is why government should in fact take a more prominent, active role.

Network separation

To protect critical sectors and the national government, the National Cyber Security Strategy 2 notes that organisations could consider separating their IT networks. There are various ways to do this. User separation involves authorising a select group of users to access specific IT facilities. In addition, terminal separation is also possible, with access to IT facilities being restricted to authorised computers and mobile devices. Organisations can also introduce access network separation, for example by creating their own wireless network. The safest option by far is to take the organisation's network offline while simultaneously designing and building the IT infrastructure from its individual components.

In real life, many organisations apply partial forms of network separation. Choosing one option or another depends on the organisation’s security priorities and the resources that this requires. The deeper down in the network security needs to be guaranteed, the less feasible chain separation becomes in a financial and practical sense (PwC 2014).

The government-wide DigiNetwerk is an example of a partially separated network. It allows government authorities to share data securely with other authorities. DigiNetwerk links existing government networks, including The Hague Ring, which in turn runs on the fibreoptic Netherlands Armed Forces Integrated Network (NAFIN) as a separate virtual network (PwC 2014).

TenneT, the company that manages the Dutch and part of the German high-voltage grid, has introduced a far-reaching form of network separation. For its primary process – the reliable and uninterrupted supply of electricity to about 41 million end-users – TenneT uses its own offline IT network. That means that, in the event of a major DDoS attack in the Netherlands, its primary process will not be at risk. TenneT’s network can only be accessed from the inside. TenneT does use the internet to optimise its primary process, which requires continuous contact with producers of electricity. That is also true of its other operational management activities. These processes are therefore vulnerable to internet crashes, for example. To protect itself against hacks, TenneT prohibits employees from receiving private e-mails on their work laptops – one of the few companies to do so.

3.10 Security is never entirely fool proof

Nature of attacks continues to change

Chapter 2 showed that the nature of cyberthreats is changing continually. Cybercriminals are constantly seeking new revenue models and trying a variety of different attack tools; state actors continue to develop sophisticated methods to circumvent security measures. What is regarded as secure today may be obsolete tomorrow.

The rapid advances in technology, the many mutual dependencies between organisations and between them and their IT suppliers, and the inherent insecurity of IT itself all make it difficult to predict what new forms cyberthreats will take. Ransomware and spear phishing are relatively new methods, for example. Many IT users are less wary of them than they should be, and less resilient as a result. And although efforts to fend off DDoS attacks have been more successful in recent years, recent DDoS infections with botnets consisting of hundreds of thousands of connected devices have thrown up a significant new challenge.

Race between attacker and target

Threats and resilience are interrelated. The level of threat posed by a certain method of attack depends on the extent to which the target can resist that attack. This power struggle can be seen as a sort of rat race between attacker and target. On the one hand, there is the inventiveness of the attacker, who seeks out new vulnerabilities and uses new methods; on the other, there is the ability of the target to respond swiftly to the attack. Both parties must carry out a cost-benefit analysis: how much time, money and expertise are they willing to commit to attain certain benefits (financial profits, valuable information) or to avoid damage?

What is secure and resilient?

Maximum security is usually not – or in fact never – feasible because the benefits simply do not outweigh the costs. Both businesses and public authorities base their cybersecurity investment decisions on cost-benefit analyses (CPB 2016). It is beyond the financial capacity of most organisations to introduce comprehensive security measures such as TenneT's separate IT network. But even that network is not one hundred percent secure. The Stuxnet virus – allegedly used by the US and Israeli secret services to sabotage centrifuges at Iranian uranium enrichment facilities – shows that it is possible to bridge an 'air gap' with an infected USB stick, in this case (Zetter 2014).

One of our interlocutors hence questions what the attributes 'secure' and 'resilient' actually mean. Cybersecurity risks are often regarded as unacceptable. But like risks in the physical world, risks in the digital domain cannot be expunged entirely. Achieving a certain level of cyber-resilience involves accepting certain risks. The question then is: which risks and ensuing damage are we, as a society, prepared to accept?

4 Measures

During the two workshops organised within the context of this study, we discussed at length potential measures to strengthen the resilience of Dutch society against cyberthreats. This chapter reviews those measures. We differentiate between measures meant to improve media literacy; measures meant to protect ordinary people, businesses, critical sectors and government; statutory measures; and measures related to expertise, capacity and budgets. All these measures require an investment on the part of government, financial and otherwise, and this chapter also looks at how that investment can create opportunities for the Dutch economy. It further describes the Netherlands' standing in the international cybersecurity arena and relevant international agreements on combatting cyberattacks.

4.1 Improve digital literacy

As the previous chapter made clear, people often have only a vague idea of the risks posed by new cybercrime methods, such as ransomware and spear phishing. They also fail to make adequate use of basic security measures, for example strong passwords and backups.

To improve public 'digital literacy' – i.e. to increase public awareness of cyber-risks and what can be done about them – the most sensible approach might be to spend more time teaching cybersecurity and cyberskills in schools. Verhagen argues that digital literacy, including instruction in cybersecurity, should be added to the core primary and secondary school curriculum as soon as possible (Verhagen 2016). Others acknowledge the need to improve digital literacy among young people (above all), but are wary of saddling the education sector with this task.

The second option for improving the public's digital literacy is to launch a series of public information campaigns, whether government-sponsored, industry-driven or run by the Dutch Consumers' Association or a similar organisation. For example, the Dutch Payments Association (NVP) made customers more aware of the risk of online banking fraud and how to cope with its 'Hang up! Click close! Call your bank!' campaign (NVB 2016).

But we cannot expect too much of the public's cyberskills. Many users already have trouble making sure that their computer and smartphone are adequately secured. Most people will not be capable of protecting all the insecure or poorly secured connected devices that the emergence of the Internet of Things is unleashing on the market.

Of course, we might wonder whether we really need to equip our homes with all sorts of connected household appliances and other devices, and whether it is even clever to do so from the viewpoint of security.

4.2 Security precautions

4.2.1 Arrange basic security

The first step towards strengthening resilience against cyberattacks is to ensure that basic security is as it should be. That is not only something that the public must do, it is also a requirement for businesses, government and critical infrastructure. Besides the precautions already noted, for example timely installation of software updates, strong passwords and backups of important files, other options include two-factor authentication or encryption of important data.

SMEs can take security precautions by contracting cloud services from IT providers that offer a comprehensive service package, thus relieving them of their security worries. Cloud services can provide innovative and easy-to-access security solutions covering computing power, security applications and expertise about cyberthreats (PwC 2016), exemplifying ‘security-as-a-service’.

The relevant small businesses will, however, have to perform a cost-benefit analysis before contracting such services. That means understanding their own operational processes, the data essential to those processes, the risks that they run in the event of a hack, and whether the service package suits their specific situation. They must also have enough confidence in the provider to entrust it with the job of securing their critical business data (PwC 2016).

Cybersecurity goes beyond technical precautions; it also involves organisational matters. For example, it is important for businesses and organisations to have an open reporting culture in which employees can report security incidents without fearing reprisals (KPMG 2013).

4.2.2 Detection and response

Merely fending off attackers is not enough in many cases. Persistent or skilled hackers will eventually find their way in. That is why businesses need to know which information and processes are critical to operations and introduce fit-for-purpose measures.

To be able to detect unusual patterns and intervene where necessary, businesses must monitor their critical processes. For example, banks have successfully battled online fraud by focusing on the rapid detection of suspect transactions.

Businesses also need to know how to respond when facing a ransomware infection or DDoS attack, and how to return to ‘business as usual’ as quickly as possible.

4.2.3 Set up a Digital Trust Centre

One key question is which security measures are appropriate for which business or type of business. The corner bakery works with different data and runs different risks than high-tech firms or companies operating entirely online, such as web shops. But as we saw earlier, many businesses possess neither the expertise nor the skills necessary to determine which security precautions they require or which cloud or other services are the best fit for them. What they really need, in other words, is independent advice.

Many of our interlocutors advocate more public-private partnerships and information-sharing. Several of them referred to the support and advice offered by the NCSC to ISAC member businesses and organisations that operate critical infrastructure. The question is whether the ISAC approach would work for SMEs. The system of regular consultation in a confidential setting seems more suited to sectors made up of a small number of large businesses, for example the financial or energy sector, than to those consisting of large numbers of smaller firms.

SMEs therefore prefer to see the establishment of a Digital Trust Centre, a centre of expertise that could offer them the necessary advice and support. The centre should be able to draw on the expertise of the NCSC. Because SMEs are so numerous, their industry associations could function as a link, ensuring that information specific to each sector is passed on to industry members. Because industry associations tend to be small in size, they should have the encouragement and support of government. Larger businesses outside the critical sectors would also benefit from a Digital Trust Centre.

4.2.4 Strengthen the resilience of critical infrastructure

Various interlocutors feel that government should play a more active role in strengthening the resilience of critical infrastructure against cyberthreats. After all, the level of resilience is not what it should be and critical sectors do serve a broader, public interest. Attacks on critical infrastructure could result in severe societal and economic disruption.

The question is how government should interpret that more active role. According to some of our interlocutors, there is no point in prescribing and enforcing specific security standards; sectors are too diverse and standards are never specific enough. Less stringent measures might be preferable, for example agreeing on annual hack tests that also cover the latest cyberthreats.

4.2.5 Have government set an example

Government must also do more to optimise its basic security. As a purchaser of security products and services, it plays an important role in the field. About thirty percent of all security products and services sold in the Netherlands go to government organisations, illustrating the need for government, as a key market party, to set a good example with its procurement practices (CPB 2016; Ministerie van Economische Zaken 2016).

Unfortunately, it does not always do so. Basic government security is not always as it should be and too often, cybersecurity is in last place on the list of budget priorities. Several of our interlocutors argue that government should be more ambitious and showcase itself as an innovator and launching customer. Government could, for example, improve shared procurement of cybersecurity products and services. Not only would this allow it to build its own knowledge base, but it might also ‘challenge’ commercial parties to innovate more (Hendriks et al. 2016). Government could also identify a clearer overall strategy and do more to coordinate implementation of effective security precautions. This assumes, however, that it has a sufficient level of internal expertise.

Our interlocutors made several suggestions for improving coordination and efficiency in government. They range from appointing a senior official or separate minister for cybersecurity to facilitating closer cooperation between ministries and establishing a top ministerial team under the prime minister's leadership. Participants in the second workshop noted that the first steps towards interministerial cooperation had recently been taken, partly in response to the Verhagen report (2016).

4.3 Statutory measures

4.3.1 Expand powers of intelligence and investigative agencies

To improve its defences against cyberespionage and the manipulation of information by state actors, the AIVD has argued for broader powers to intercept internet traffic. This would allow it to detect suspect patterns more quickly. The Dutch House of Representatives discussed a bill updating the Intelligence and Security Services Act [*Wet op de inlichtingen- en veiligheidsdiensten*, Wiv] in December 2016. It passed the bill and the Memorandum of Amendments in February 2017 (*Kamerstukken II 2016-2017a*). The bill has yet to be reviewed by the Senate.

According to Ronald Prins, director of security firm Fox-IT, the proposed expansion of the intelligence and investigative services' powers is a 'dire necessity' (NOS 2015). The AIVD plays an important role in the Netherlands' defences against cyberespionage by state actors. Updating the Wiv would make the defences against cybercrime and cyberespionage much more effective, according to Prins (Prins 2016). Verhagen agrees that the existing statutory powers of the intelligence and security services are too weak to offer the Netherlands the appropriate level of cybersecurity, and that those powers should be expanded (Verhagen 2016).

Others – including the Council of State and the Review Committee on the Intelligence and Security Services (CTIVD) – have criticised the bill, however. Although both acknowledge the need to expand the powers of the intelligence services, they are critical about the bill's method for overseeing the exercise of those powers. The Council of State has 'serious doubts' about the effectiveness of that oversight (RVS 2016). The CTIVD considers that, although the bill offers more assurances than the existing act – including prior approval – those assurances are inadequate given the scope of the new powers. The Memorandum of Amendment offers various improvements in this regard, but they do not go far enough in the CTIVD's view. The bill does not offer enough verifiable standards, making effective oversight difficult (CTIVD 2016; 2017).

The CTIVD is also worried about the legal position of citizens in the event of information-sharing with foreign intelligence services. It sees this as a 'serious gap' in their legal protection (CTVID 2017). The same point was raised during a Senate expert meeting on cyberintelligence in 2014. It is not always clear how well personal data is protected when Dutch intelligence services cooperate with their foreign counterparts. It is furthermore difficult for people to defend themselves against unjust suspicions of wrongdoing by intelligence services (Rathenau Instituut 2014; *Kamerstukken I 2013-2014*).

The House passed the bill in February 2017 with an amendment and a number of motions. The motions ask the Government to have the CTIVD investigate the risks of data-sharing with foreign intelligence agencies and report on how the three-year data retention period will affect the protection of personal privacy (*Kamerstukken II 2016-2017d; Kamerstukken II 2016-2017e*). They also ask the Government to exercise the expanded powers as specifically and narrowly as possible (*Kamerstukken II 2016- 2017f*).

Like intelligence agencies, investigative services would like to have greater access to online communication, but they are thwarted by the proliferating encryption of internet traffic. The services would therefore like to exploit ‘zero-days’, a software or hardware vulnerability that has been detected but not yet fixed. Zero-days would allow the investigative services to break into suspected hackers’ computers (‘hacking back’).

The Computer Crime III bill is meant allow hacking back. The House discussed this bill in December 2016 and adopted it, with a few amendments (*Kamerstukken II 2015-2016*). This bill too is controversial. Critics have pointed out that until a software manufacturer is told about a zero-day vulnerability, other parties – such as cybercriminals – can also exploit it. In response, the House adopted an amendment proposed by MPs Recourt and Tellegen stipulating that the public prosecutor must report the exploitation of zero-days by investigative services to the software manufacturer, and may only postpone that report if doing so serves a ‘critical investigative interest’ (*Kamerstukken II 2016-2017c*). Another motion proposed by MP Recourt was also adopted, asking the Government to exploit zero-days only ‘as a last resort’ (*Kamerstukken II 2016-2017b*).

4.3.2 Enforcement and oversight

Chapter 2 described how the emergence of the Internet of Things has given rise to a steady stream of new, connected devices, from routers to baby phones and ‘smart dolls’. Many of these devices are not secure; they may use a standard password to prevent unauthorised access, or no password at all.

In practical terms, that means that consumers bear the responsibility for securing these devices. They are expected, for example, to alter the standard password immediately after purchase and to update software and change passwords regularly. In reality, however, many people do not. And the more ‘smart’ devices they purchase, the bigger the problem will become (Eskens et al. 2016).

A frequently cited option meant to bridge this security gap is to introduce a quality mark for secure devices that would wipe insecure devices from the market. A quality mark imposed by law will probably fail, however. The legislative process is lengthy and technology is advancing too rapidly for the law to keep up. Before pertinent legislation even enters into force, the security requirements it prescribes will be obsolete. The huge numbers of new IT products flooding the market every week would also make a quality mark hard to implement.

Potentially more successful is to provide for a minimum level of security in the law in the form of an ‘open standard’, combined with active oversight of actual specifications and enforcement down on the ground. Dutch legislation makes frequent use of such open standards. For example, the Personal Data Protection Act [*Wet bescherming persoonsgegevens*] provides for an open standard for protecting personal data. Organisations that work with personal data must take ‘appropriate technical and organisational measures’ to secure that data against loss or unauthorised use. The Data Protection Authority of the Netherlands (CBP) also issued guidelines for personal data protection and oversaw compliance with them (CBP 2013). The CBP’s successor, the Dutch Data Protection Authority (Dutch DPA), recently warned hospitals that their patient data portals were insufficiently secure (AP 2016). Because medical data demands the very highest standard of reliability, hospitals are required to use two-factor authentication. The Dutch DPA has let it be known that hospitals are expected to comply with this requirement. If they do not, the Dutch DPA will enforce compliance.

The US Federal Trade Commission (FTC) offers a good example of active oversight in the field of IT. In 2015, the FTC decided to prioritise the privacy and security of connected devices and published guidelines for securing them (FTC 2015). Under a statutory prohibition on misleading and unfair trade practices, the FTC took legal action against three companies. It was able to show that these companies had marketed their products as secure even though they had failed to take reasonable steps or make use of generally known security precautions. The FTC slapped one of the companies, computer hardware manufacturer ASUSTeK, with a twenty-year audit (FTC 2016).

The example of the FTC raises the question of whether Dutch regulatory agencies can take similar action against inadequately secured IT devices. Can the Netherlands Authority for Consumers and Markets (ACM) or the Radiocommunications Agency Netherlands take steps against insecure products based on their current mandates? Like the United States, the Netherlands has legislated against ‘unfair trade practices', with the ACM as the relevant regulatory agency. The legislation covers such matters as misleading advertising, failure to report all additional costs, or aggressive pursuit of new customers. The ACM can impose a fine, a penalty or both.

In late 2016, the Dutch Consumers’ Association informed the ACM, the Dutch DPA and the Netherlands Food and Consumer Product Safety Authority (NVWA) about the sale of insecure smart dolls (Consumentenbond 2016d). The dolls are connected to the internet and will reply when children talk to them. An investigation by the Norwegian consumers’ association had shown that anyone in the vicinity of such a doll could use Bluetooth on their mobile phone to listen in on these conversations and put words in the doll’s mouth. As yet, the regulatory agencies have not responded to the Dutch Consumers’ Association’s campaign. Blokker Holding (which owns the toy store chains Bart Smit and Intertoys) has taken the dolls off the shelves, however.

4.3.3 Duty of care and liability legislation

Another option to promote the sale of more secure products is through duties of care and liability legislation. Existing legislation imposes several duties of care related to proper security. The relevant provisions can be found in the Personal Data Protection Act, the Dutch Criminal Code and the Dutch Civil Code. However, businesses are often unaware of their duties of care and what they mean in actual practice. The Netherlands Cyber Security Council recently published a manual on cybersecurity and duties of care. For example, IT product vendors or service providers must ensure that their products and services comply with relevant security standards, and that their software can be updated (CSR, 2017).

One important duty of care for IT device vendors is to ensure that products are ‘fit’ (i.e. safe enough) for the purposes for which they would normally be used. In real life, however, it is not always clear what this means. The product must not have any known security issues at the time of sale. But whether customers can expect vendors to patch vulnerabilities that arise thereafter within a reasonable time frame depends on the circumstances (CSR, publication pending).

The Dutch Consumers’ Association has started legal proceedings against Samsung because it does not update the software of many of its Android smartphones, or only for a short period of time. The Association claims that Samsung is acting unlawfully. It is demanding that the company issue updates for a minimum of four years following the introduction of, or two years after the purchase of, a smartphone to ensure that the software meets the latest security requirements (Consumentenbond 2015; 2016a; 2016b).

The European Commission is currently preparing a Directive on the ‘supply of digital content’. The proposal is meant to provide uniform rules with consumer rights related to digital products and services. The proposal makes explicit that security, accessibility and continuity, including updates and security patches, must ensure that digital content is ‘fit for the purposes for which digital content of the same description would normally be used’ (European Commission 2015).

Combining statutory oversight of IT product and service security with liability legislation could very well give rise to forms of certification or quality marks in the marketplace. After all, businesses will want to avoid regulatory or judicial intervention. Verhagen (2016) and Hendriks et al. (2016) have also pointed out the possibility of certification based on self-regulation.

4.3.4 Report cybercrime and increase likelihood of apprehension

Although the Dutch national police service has a High-Tech Crime Unit (THTC) that specialises in fighting cybercrime, the battle at regional level is receiving less attention. Cybercrime is a matter of small concern for regional police services, and individuals and businesses encounter great difficulty when they try to report it. Regional police services seemingly lack the relevant knowledge – for example about ransomware – and thus tend not to prioritise cybercrime.

Several of our interlocutors pointed out the need to improve the odds of apprehending and prosecuting cybercriminals. It must be made clear that cybercrime does not pay. Increasing the likelihood of apprehension and prosecution would certainly help scare off script kiddies and petty criminals.

If law enforcement were to take cybercrime reports more seriously, the authorities would also have a better idea of the actual problems, allowing them to bring more focus to the fight against cybercrime.

4.4 Expertise, capacity and budget

4.4.1 Develop expertise and build capacity

The Netherlands has a deep well of knowledge about cybersecurity distributed across different organisations: businesses such as Deloitte and KPN; knowledge-driven institutions such as TNO and Radboud University; and government organisations such as the NCSC or the national police service's High-Tech Crime Unit.

In addition, the Dutch government encourages research and innovation in data security. For example, the Netherlands Organisation for Scientific Research (NWO) has announced plans to launch three different cybersecurity research programmes in 2017, including within the context of the National Cyber Security Research Agenda (NCSRA) (NWO 2017). The programmes will coordinate with the second National Cyber Security Strategy (NCSS) and the Netherlands' top sectors policy, which targets economic innovation.

But the demand for cybersecurity experts far outstrips the supply. That is true not only of employees with tertiary-level degrees but also of trained workers with vocational qualifications (Verhagen 2016; Hendriks et al. 2016). The labour market is tight and the parties that require the expertise are all fishing in the same pond. Qualified specialists tend to gravitate towards well-paying jobs in the private sector, at the expense of employee quality in government.

The police also lack the necessary expertise. They are losing cybersecurity specialists to large companies because they cannot offer them the same attractive career prospects. As a result, law enforcement agencies have a shortage of data specialists capable of producing more comprehensive analyses of cybercrime and the forces that drive it. That is not conducive to effective policing of cybercrime.

The demand for expertise will only rise in the years ahead, in part owing to the scale of the cyberthreat and the rapid pace of technological progress. That pace makes it difficult to predict the form cyberthreats will take in the future and what we must do to protect ourselves against them. Our ability to adapt is therefore crucial.

Several of our interlocutors pointed out the urgent need to invest in cybersecurity training and capacity-building in both the private and public sectors. If that fails to happen, our resilience against cyberthreats will be even weaker than is presently the case.

One of the interlocutors noted that the Netherlands could also make better use of the expertise of the Dutch hacker community, a resource that is still too often ignored.

4.4.2 Increase the budget for cybersecurity

To boost investment in cybersecurity training and capacity-building, government and businesses must spend more of their budgets on cybersecurity. Several of our interlocutors pointed out that the Netherlands invests very little in cybersecurity compared with other western countries. Verhagen has also advocated a sharp increase in the cybersecurity budget (Verhagen 2016).

Others would rather not place all the emphasis on more spending. Resilience against cyberthreats can be considerably improved by expanding public-private partnerships, either within the context of the ISACs or in the form of a Digital Trust Centre. Such initiatives may only require limited human and financial resources.

4.5 Economic opportunities

Several interlocutors argued that cybersecurity trends should also be viewed as opportunities for the Dutch economy. As host of the largest internet exchange in the world, the Netherlands has high-speed broadband telecommunications networks and is therefore a key location for IT-related activity. By maintaining the quality and security of its IT infrastructure, it can become even more attractive as a business location for IT-related activity (Ministerie van Economische Zaken 2016; PwC 2016).

The Dutch cybersecurity sector can also capitalise on the demand for new security products and services. The Netherlands is already well placed to showcase itself in this field. It has the necessary specialist know-how, present in such firms as Fox-IT and Deloitte Nederland and in knowledge-driven organisations such as TNO, Radboud University and the University of Amsterdam.

The Netherlands underutilises this know-how at the moment, ignoring the economic opportunities it creates. To take advantage of those opportunities, businesses must do more to promote data security as one of their ‘unique selling points’ (PwC & VU 2014).

It should be noted that the Dutch cybersecurity sector is growing faster than the IT sector as a whole. In 2014, about 10 percent of revenue generated in the IT sector was related to cybersecurity activities (Hendriks et al. 2016).

4.6 International context

Cybersecurity is not only a Dutch problem. The internet transcends national borders; cybercriminals are active all over the world; and insecure devices are produced by manufacturers worldwide. Cyberattacks are often international in scope. Countries can be a target, a transit port (by hosting botnets) or a source of attack (for example if Dutch cybercriminals are the culprits). Tackling cyberattacks effectively therefore requires not only national measures but also international agreements. This section describes the Netherlands’ standing in the international arena and relevant international agreements on fighting cyberattacks.

4.6.1 The Netherlands' standing

In terms of threat levels, the Netherlands is reasonably similar to countries like Germany, the United Kingdom, France and the United States. Notable points are that it hosts a relatively large number of fraudulent websites and that Dutch internet users are increasingly plagued by phishing and malware hosting sites. The Netherlands leads the way in cybersecurity in several respects for example its public-private partnerships in the ISACs and the Dutch banking sector's innovative strike against cybercrime.

In other respects, however, the Netherlands could stand to learn from other countries, for instance when it comes to applying and updating security standards. The UN's International Telecommunication Union has identified the United States' cybersecurity standards as an example of good practice (ITU 2015). One of the key components of its approach is a national framework, made up of a set of recommended security standards for industry and a collection of best practices (NIST 2014). The framework offers organisations guidelines for detecting and responding to cybersecurity risks. The National Institute of Standards and Technology (NIST) ensures that the framework is implemented and kept up to date. In Europe, the Network and Information Systems (NIS) platform facilitates such standards.

The Netherlands has no organisation focusing exclusively on cybersecurity standards. The Standardisation Forum does maintain the mandatory open standards for the public sector, as formulated in the Data Security Baseline for National Government. In addition, the NCSC advises the national government and operators of critical infrastructure on security standards. In 2015, the Ministry of Security and Justice asked research firm InnoValor to survey and produce an overview and classification of standards (Hulsebosch & Van Velzen 2015). The classification can help organisations deal with risks, but unlike the US framework it does not offer any specific guidance. Another point of concern is that the classification and underlying standards need to be updated if they are to remain relevant.

The United States is also explicitly concerned about threats associated with the Internet of Things. The Department of Homeland Security has published a document setting out *Strategic Principles for Securing the Internet of Things*. It identifies six 'non-binding strategic principles' designed for 'developers, manufacturers, service providers, and the users who purchase and deploy the devices, services, and systems', for example incorporating security at the digital product/service design phase, promoting security updates, and connecting carefully and deliberately to the internet (US Department of Homeland Security 2016). As mentioned earlier, the FTC has also made the Internet of Things one of its priorities.

The Netherlands could also learn from other countries with regard to certification. Unlike Estonia, Germany and the United Kingdom, the Netherlands has no policy on certifying professional qualifications. Germany's Federal Office for Information Security has drawn up guidelines for certifying cybersecurity firms and professionals (*IT-Grundschutz*) (BSI 2017). Certification provides clients and customers with information about a firm's cybersecurity efforts. Estonia has followed Germany's example and made its certification guidelines mandatory for public-sector organisations that work with databases or registers (ISE 2016). The EU is exploring the possibility of harmonising certification programmes for IT security products (European Commission 2016). At the moment, an IT firm that wishes to sell its products and services in the EU must go through several national certification processes in different EU member states. Companies in the United Kingdom bidding for certain government contracts involving sensitive and personal information handling are obliged to gain Cyber Essential badges. The procedure has been laid down in the Cyber Essentials Scheme (Gov.uk 2014).

4.6.2 International agreements

Once one country takes steps to defend itself, for example against ransomware, cybercriminals will defect to another that has yet to introduce relevant protections. The never-ending race between attackers and defenders is also an international affair. Given the ‘waterbed’ effect of these cyberthreats, international harmonisation of agreements is important. The European Union Agency for Network and Information Security (ENISA) therefore advocates harmonised measures (ENISA 2015).

The EU itself has recently taken several steps to strengthen its resilience against cyberthreats. For example, in 2016 it passed the Directive on Security of Network and Information Systems (NIS Directive). The aim of the Directive is to ensure a high common level of network and information security across the Union. This involves closer cooperation between Cyber Security Incident Response Teams in the various member states (such as the Netherlands’ NCSC). The Directive also requires businesses that operate ‘essential services’ (i.e. critical infrastructure) to report ‘serious incidents’ to the relevant authorities. The Directive entered into force in August 2016 but has yet to be incorporated into national legislation. The member states have 21 months to do so (European Parliament 2016).

The EU has also adopted the General Data Protection Regulation in 2016, enforceable in 2018. Its purpose is to harmonise the personal data protection rules throughout the Union. Among other things, it makes the reporting of data breaches mandatory. In addition, the Regulation imposes a duty of documentation on organisations: they must be able to demonstrate that they have taken the appropriate technical and organisational measures to safeguard personal data.

Alongside international regulation, international knowledge generation and cybersecurity innovation are important tools for surmounting cyberthreats. The European Commission announced an action plan for this purpose in July 2016. It will invest 450 million euros in a public-private partnership on cybersecurity innovation to encourage cooperation in this area (European Commission 2016). By 2020, total investment is expected to reach around 1.8 billion euros, with funding coming from the EU’s Horizon 2020 research and innovation programme.

5 Conclusions and recommendations

5.1 The Digital Dutch

The Netherlands is one of the most digitalised countries in the world. Almost everyone here owns a computer, and more than 90 percent of all households and businesses use the internet. Digitalisation has made inroads into virtually every aspect of our lives. As a result, the physical and digital domains are becoming more intertwined all the time.

Dutch society and the Dutch economy are thus becoming increasingly dependent on a properly functioning IT infrastructure and IT services. Data theft, data manipulation or the failure of IT structures can all have major consequences for society and the economy. Our growing dependence on IT makes Dutch society vulnerable.

The question is what Dutch society and the economy can do to resist cyberthreats. Does the level of cyber-resilience need to be strengthened, and if so, what steps should we be taking to do so? To answer this question, Chapter 2 surveyed the most serious cyberthreats. Chapter 3 described how resilient various sectors are to these threats, and Chapter 4 identified potential measures that we can take against them.

This chapter lists the main conclusions and offers a set of recommendations at varying levels, specifically for government and businesses.

5.2 Conclusions

5.2.1 Rising cyberthreats

In theory, everything that contains IT can be hacked. Our growing dependence on IT makes digital products and processes an attractive target for cybercriminals, cyberspies and other malicious hackers. Software consists of many lines of code, sometimes running into the millions, and errors and imperfections are unavoidable. These vulnerabilities can be abused by malicious actors. Their motives range from politically motivated espionage by state actors to ransomware attacks by cybercriminals for monetary gain and hacks by mischievous teenaged script kiddies.

The biggest threat is posed by foreign intelligence agencies and their allied hacker groups. Russian and Chinese intelligence services in particular collect vast amounts of political, military and technological information. Their work is highly professional and their operational effectiveness is enormous. The Dutch government and Dutch high-tech businesses are regular targets of cyberespionage attacks. State actors also increasingly focus on manipulating information, for example to sway public opinion or influence the political climate in another country.

In addition, cybercrime is increasingly turning into a form of organised crime. Cybercriminals are becoming more professional, they employ increasingly sophisticated methods, and their revenue model is proving more profitable all the time. Botnets are becoming harder to detect and criminals are making growing use of spear phishing. Ransomware has become a popular form of attack in recent years affecting not only individuals and businesses but also hospitals. Cybercrime and economic espionage could eventually undermine the innovativeness and competitiveness of Dutch trade and industry.

Petty criminals or script kiddies are also a problem. With the dark web lowering the threshold to digital attack tools ('cybercrime-as-a-service'), even less proficient hackers can launch a DDoS attack and cause severe damage.

5.2.2 Inadequate resilience

The public, businesses and government do too little to ward off cyberthreats. They frequently fail to take even the most basic security precautions, e.g. updating software, using strong passwords or making backups of important files. They also have insufficient knowledge or understanding of the precise risks they are running and what to do about them. Risk thus remains an impalpable factor, and the importance of cybersecurity is largely ignored until something finally goes wrong. Private citizens, SMEs and lower tiers of government are especially guilty of inadequate basic security.

Businesses that operate critical infrastructure and the national government are often more aware of the risks they are running and how to protect themselves. The critical sectors and the national government are supported in this regard by the NCSC and the AIVD. The NCSC, for example, cooperates with companies in Information Sharing and Analysis Centres (ISACs). ISACs are public-private partnerships in which businesses share cybersecurity information and lessons learned. The ISAC system puts the Netherlands at the forefront of international developments in this arena.

Critical sectors differ in terms of their level of resilience. The energy, telecommunications and financial sectors appear to be reasonably resilient, but that is not true of all critical sectors.

The national government also comes up lacking at times. For example, it has problems phasing out obsolete software, and its DigiD authentication system has failed to meet the NCSC's security standards for several years. All too often, cybersecurity is at the bottom of the priority list in procurement procedures. Government is a key purchaser of security products and services and should set an example, but it does not always have enough expertise itself to do so.

The Internet of Things increases vulnerability

The rise of the Internet of Things is leading to a growing number of connected devices. Many of these 'smart devices' are not properly secured, making them vulnerable to cyberattack. And because smart devices are flooding the market, cybercriminals now have a much larger field to target.

The hack of a connected device not only poses a risk to the individual end-user, for example the theft or manipulation of personal data. When cybercriminals use hacked devices to carry out major DDoS attacks, they can also disable government services or critical infrastructure. Recent incidents involved hundreds of thousands or even millions of connected devices. If an attack is severe enough, it will ultimately knock out any connected IT system.

Market failure

IT providers have no economic incentive to make substantial improvements to device security. Providers compete fiercely on price and cannot afford to offer robust security for a low price. Because hacked devices can be used to carry out major DDoS attacks, however, this situation can ultimately be very harmful to society and the economy. The lack of device security can therefore be regarded as a serious form of 'market failure'.

Existing measures inadequate

It is worrying that individuals, businesses and government are all insufficiently resilient against cyberthreats. The situation is even worse in view of the rapid pace of technological progress and the increasingly sophisticated methods employed by cybercriminals and state actors. Existing cybersecurity measures are thus inadequate.

5.3 Recommendations for strengthening resilience

It is very important that we take steps to strengthen our resilience against cyberthreats. This section describes what those measures are and makes recommendations for the relevant parties, in particular government.

5.3.1 Recommendations to improve security

We cannot expect the same level of expertise and cyberskill from all individuals, businesses and public authorities. In addition, not everyone is an equally likely target of a certain type of cyberattack. The average person or small business owner will generally have little to fear when it comes to cyberespionage by foreign intelligence services, and if such an attack were to occur, he or she would be utterly helpless anyway. Conversely, large organisations that have access to the right expertise and tools generally have less to fear from script kiddies or petty criminals, but they can become the target of advanced attacks by state actors.

The first step towards strengthening resilience against cyberattacks is to ensure that basic security is as it should be, for example by installing software updates without delay, using strong passwords and making backups. That is not only a requirement for the public but also for businesses, critical sectors and government. As long as basic security is inadequate, there is little point in introducing other, more far-reaching security measures.

Promote cyberskills, but don’t expect too much of ordinary people

The most sensible approach might be to promote basic cyberskills among consumers and the general public by focusing more on cybersecurity in education and in public awareness campaigns. But we must not expect too much of such measures. Many users already have trouble making sure that their computer and smartphone are adequately secured. Most people will not be capable of protecting all the insecure or poorly secured connected devices that the emergence of the Internet of Things is unleashing on the market. The responsibility for this needs to be assumed by other parties.

Recommendation for government, businesses and other parties, e.g. the Dutch Consumers’ Association:
Pay more attention in education and in public information campaigns to cybersecurity and the cyberskills that consumers and the public should possess.

Establish an independent expertise and advisory centre for businesses

SMEs have an urgent need for independent advice and support when it comes to security measures. They have only a limited understanding of the risks that they are running, and they lack the expertise to take appropriate precautions. When they do take steps to fend off attackers, they are often inadequate. Sooner or later, hackers find their way in anyway. That is why businesses need to know which processes and data are critical to their operations, so that they can introduce targeted measures.

IT specialists supply all sorts of security solutions, but SMEs are often incapable of determining whether these products and services are right for them. After all, the corner bakery runs different risks than high-tech firms or web shops.

SMEs therefore prefer to see the establishment of a Digital Trust Centre, a centre of expertise that can offer them the necessary advice and support. This organisation must have access to the expertise of the NCSC. Because SMEs are so numerous, their industry associations could function as a link. Larger businesses outside the critical sectors would also benefit from an independent centre of expertise and advice.

Recommendation for government and businesses:
Invest in an independent expertise and advisory centre for SMEs and larger businesses operating outside the critical sectors.

Protect critical sectors by introducing a hack test

The businesses that operate critical infrastructure are diverse in nature and their level of resilience differs. Whereas the banks or companies such as TenneT have taken extreme measures to secure their primary process – the supply of electricity, financial transactions – other businesses have not done enough. There is friction here between their commercial interests, which make investing in security unappealing, and the public interest, which benefits from the continuity of critical processes.

To strengthen the resilience of those critical sectors that lag behind, government may need to play a more active role. This does not necessarily mean prescribing specific security measures from the top down. The sectors differ too much for that. What government can do is hold sectors accountable for running secure operations, for example by agreeing with them on an annual 'hack test'. If such agreements fail, government can make the hack test a statutory requirement.

Recommendation for government:
Do more to hold critical sectors accountable for running secure operations, for example by agreeing on an annual hack test.

Ensure that government sets a good example

Government must also improve its own resilience. About thirty percent of all security products and services sold in the Netherlands go to government organisations, making it a key player in this market. Government should therefore play a more ambitious role. It ought to set an example by positioning itself more prominently as an innovator and 'launching customer'. That requires government to have enough cybersecurity expertise in its own organisation. It also means tighter internal coordination. The responsibility for cybersecurity is much too fragmented at the moment. Tighter coordination would make it possible to improve the level of security within the various government organisations. The Dutch could also learn from other countries, for example the US or UK, when it comes to security standards and certification of IT businesses.

Recommendation for government:
Set a good example as a 'launching customer' and do more to coordinate sound security measures internally.

5.3.2 Recommendations for statutory measures

Government has various statutory options at its disposal for tackling cybercrime and cyberespionage and preventing insecure IT products from entering the market. However, it is not always clear how far it can go. Some of these options are also controversial.

Improve reporting and prosecution of cybercrime

Reporting and investigation of cybercrime is one area in which government can make improvements. It can be difficult for individuals and businesses to report cybercrime. Regional law enforcement agencies lack the necessary level of expertise and often fail to prioritise such reports. Making it easier to report cybercrime would increase the likelihood of apprehension and prosecution, and may help scare off script kiddies and petty criminals.

Recommendation for government:
Do more to support reporting of cybercrime at regional level and its prosecution.

Monitor ‘checks and balances’ related to the expanded powers of intelligence agencies and investigative services

To increase the likelihood of apprehension and prosecution, the Government has submitted the Computer Crime III bill to Parliament. If passed, the bill will make it possible for the investigative services to break into the computers of suspected hackers (‘hacking back’) by exploiting zero-day vulnerabilities, a point that has generated considerable debate. After all, cybercriminals can also exploit zero-days to gain access to IT systems. The debate concerns the conditions under which the investigative services are permitted to exploit zero-days. The future will show whether the bill’s ‘checks and balances’ are adequate.

Recommendation for government:
Monitor whether the Computer Crime III bill imposes adequate conditions on the investigative services for exploiting zero-day vulnerabilities.

The need to strengthen the resilience of critical sectors and the national government against cyberespionage and the manipulation of information by state actors makes it necessary to expand the capacity and powers of the AIVD. Broader powers will allow the AIVD to monitor online traffic on a vaster scale and to detect suspicious patterns. The bill updating the Intelligence and Security Services Act should provide for such broader powers.

This bill too is controversial. Critics claim that it does not provide for adequate independent oversight of how the services will use their broader powers. Another criticism concerns the legal position of citizens. The bill would not offer them sufficient legal protection against unjust suspicions of wrongdoing. Once again, the future will show whether the bill’s ‘checks and balances’ are adequate.

Recommendations for government:
Build capacity in the AIVD so that the agency is better able to detect cyberespionage and the manipulation of information by state actors and to take (or encourage others to take) appropriate measures.

Monitor whether the ‘checks and balances’ in the bill updating the Intelligence and Security Services Act are in fact adequate in practice.

Legislate a set of ‘open standards’ for product security

Growing numbers of poorly secured smart devices are appearing on the market. The security risks that they pose have led to frequent calls for legislation that would impede their sale, for example by introducing a quality mark. However, rapid advances in IT mean that any prescribed security specifications will be obsolete almost as soon as they are introduced.

A better strategy might be to set a minimum level of security in legislation in the form of an ‘open standard’. Such standards allow regulatory agencies to elaborate the details and actively monitor compliance. Open standards are common and have been used by the Dutch Data Protection Authority (Dutch DPA) and the US Federal Trade Commission (FTC). For example, the Dutch

Personal Data Protection Act stipulates that businesses and organisations that work with personal data must take ‘appropriate technical and organisational measures’ to secure that data against loss or unauthorised use. It was pursuant to this standard that the Dutch DPA recently warned hospitals that their patient data portals were insufficiently secure. The question in this case is whether the Netherlands Authority for Consumers and Markets (ACM), the Radiocommunications Agency Netherlands and other regulatory agencies have the mandate and capacity to take steps against the marketing of insecure digital products.

Another option that would impede the sale of insecure smart products involves compliance with duties of care and liability legislation. At the moment, the law imposes several duties of care on businesses to ensure proper security. However, businesses are often insufficiently aware of the duties to which they are subject and what they mean in practice. If regulatory agencies were to emphasise statutory oversight and compliance with duties of care, they could encourage market parties to organise a form self-regulation that would potentially give rise to certification or quality marks.

Right now, it is mainly the Dutch Consumers’ Association that is taking action against insecure products. For example, it has made various regulatory agencies aware of the sale of insecure smart dolls, causing shop owners to remove them from their shelves. The Association has also started legal proceedings against Samsung for not updating the software of many of its Android smartphones, or doing so only for a short period of time. It is important for regulatory agencies to exercise more active oversight in this respect.

Recommendation for businesses:
Learn about existing duties of care and comply with them.

Recommendations for government:
Legislate ‘open standards’ to permit oversight of smart device security. Allow regulatory agencies to take action against insecure IT products on that basis.

Ascertain whether regulatory agencies (Dutch DPA, ACM, Radiocommunications Agency Netherlands) have a mandate to take action against insecure IT products, or whether their mandate needs to be amended. Equip regulatory agencies with enough expertise and capacity.

See that IT manufacturers and suppliers comply with duties of care for secure products and check whether duties of care and liability legislation require amendment.

5.3.3 Recommendations related to expertise and capacity

Develop expertise and build capacity

The rapid advances in technology, the many mutual chain dependencies and the inherent insecurity of IT itself make it difficult to predict what new forms cyberthreats will take in the years ahead. Many IT users are less wary of the relatively new methods of ransomware and spear phishing, for example, and less resilient against them as a result. And although efforts to fend off DDoS attacks have been more successful in recent years, recent DDoS infections with botnets consisting of hundreds of thousands of connected devices have thrown up a significant new challenge. The increasingly sophisticated methods used by cybercriminals and state actors are especially worrisome.

Because cyberattack methods are constantly changing and growing ever more advanced, the rat race between attacker and target is never-ending. Resilience against cyberthreats is never finished, but requires continuous monitoring and investment.

It is worrying that individuals, businesses and government are all insufficiently resilient against cyberthreats. They lack the necessary expertise and capacity to deal effectively with such threats. As indicated in the foregoing sections, government and businesses should invest more in developing expertise and in capacity-building. That applies across the board: from expanding cybersecurity training and supporting SMEs with an independent expertise and advisory centre to ensuring that government, the relevant regulatory agencies and the AIVD have enough internal expertise and capacity. Investment in expertise- and capacity-building is even more necessary to strengthen resilience against the new, unpredictable cyberthreats that Dutch society and the Dutch economy will face in the years ahead.

Recommendations for government and businesses:
Invest in cybersecurity training.

Invest in capacity-building: establish an independent expertise and advisory centre for SMEs and other businesses (non-critical sectors); see that expertise and capacity are sufficient in government, the relevant regulatory agencies and the AIVD.

5.4 Economic opportunities

The measures required to strengthen resilience against cyberthreats will require the necessary investment. At the same time, that investment can create opportunities for the Dutch economy. A more secure IT infrastructure will increase the Netherlands' appeal as a business location for IT-related activity. Security measures can also create new opportunities for the Dutch cybersecurity sector. To capitalise on those opportunities, however, we must do more to harness the expertise of businesses and institutions specialising in cybersecurity.

5.5 Learning to live with insecurity

Security is never entirely fool proof. Technology is advancing much too rapidly for that, and the race between attacker and target is never-ending. The level of threat posed by a certain attack depends on the extent to which the target can resist it. On the one hand, there is the inventiveness of the attacker, who seeks out new vulnerabilities and uses new methods; on the other, there is the ability of the target to respond swiftly to the attack.

Both attackers and defenders must perform a cost-benefit analysis: how much time, money and expertise are they willing to commit to attain certain benefits (financial profits, valuable information) or to avoid damage? Financial and human resources will always be limiting factors. As in the physical world, then, it is impossible to expunge risk entirely in the digital domain. Achieving a certain level of cyber-resilience involves accepting certain risks. And as in the physical world, this means that we will have to learn to live with a certain level of insecurity in the digital domain.

As this study has shown, knowing this does not obviate the need to take measures to strengthen the resilience of Dutch society and the Dutch economy against cyberthreats.

5.6 Summary of recommendations

This final section provides a concise summary of the recommendations of this report.

Strengthening the resilience of the public, businesses and government
Recommendation for government, businesses and other parties, e.g. the Dutch Consumers' Association:

1. Pay more attention in education and in public information campaigns to cybersecurity and the cyberskills that consumers and the public should possess.

Recommendation for government and businesses:

2. Invest in an independent expertise and advisory centre for SMEs and larger businesses that operate outside the critical sectors.

Recommendations for government:

3. Set a good example as a 'launching customer' and do more to coordinate sound security measures internally.
4. Do more to hold critical sectors accountable for running secure operations, for example by agreeing on an annual hack test.

Statutory measures
Recommendation for businesses:

5. Learn about existing duties of care and comply with them.

Recommendations for government:

6. Do more to support reporting of cybercrime at regional level and its prosecution.
7. Monitor whether the Computer Crime III bill imposes adequate conditions on the investigative services for exploiting zero-day vulnerabilities.
8. Build capacity in the AIVD so that the agency is better able to detect cyberespionage and the manipulation of information by state actors and to take (or encourage others to take) appropriate measures.
9. Monitor whether the 'checks and balances' in the bill updating the Intelligence and Security Services Act are in fact adequate in practice.
10. Legislate 'open standards' to permit oversight of smart device security. Allow regulatory agencies to take action against insecure IT products on that basis.

11. Ascertain whether regulatory agencies (Dutch DPA, ACM, Radiocommunications Agency Netherlands) have a mandate to take action against insecure IT products, or whether their mandate needs to be amended. Equip regulatory agencies with enough expertise and capacity.
12. See that IT manufacturers and suppliers comply with duties of care for secure products and check whether duties of care and liability legislation require amendment.

Expertise and capacity

Recommendations for government and businesses:

13. Invest in cybersecurity training.
14. Invest in capacity-building: establish an independent expertise and advisory centre for SMEs and other businesses (non-critical sectors); see that expertise and capacity are sufficient in government, the relevant regulatory agencies and the AIVD.

Bibliography

AIVD (2016). *Jaarverslag 2015*. Den Haag: Algemene Inlichtingen- en Veiligheidsdienst.

AIVD (2017). 'Economische Cyberspionage'. https://www.aivd.nl/onderwerpen/cyberdreiging/inhoud/economische-cyberspionage

Algemene Rekenkamer (2015a). *Resultaten verantwoordings-onderzoek 2014 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2015b). *Resultaten verantwoordings-onderzoek 2014 Ministerie van Infrastructuur en Milieu (XII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016a). *Staat van de rijksverantwoording 2015: Rijksbrede resultaten verantwoordingsonderzoek*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016b). *Resultaten verantwoordingsonderzoek 2015 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016c). *Resultaten verantwoordingsonderzoek 2015 Ministerie van Infrastructuur en Milieu (XII)*. Den Haag: Algemene Rekenkamer.

Alonso, S., 'Brussel voert strijd op tegen Russische desinformatie'. In: *NRC Handelsblad* 24 januari 2017.

Autoriteit Persoonsgegevens (2016). 'Brief aan NVZ over patiëntenportalen'. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief-nvz-patientenportalen.pdf

Beek, M. van, 'Rebelleren tegen foute knuffels'. In: *Het Financieele Dagblad* 1 oktober 2016.

Beurden, P. van, (2016). 'Informatieveiligheid is een issue voor de zorg'. https://www.zorgvisie.nl/personeel/nieuws/2016/10/informatieveiligheid-is-een-issue-voor-de-zorg/

BSI (2017). 'IT-Grundschutz Certification process'. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/itgrundschutzcertification_node.html

CBS (2016). *Veiligheidsmonitor 2015*. Den Haag: Centraal Bureau voor de Statistiek.

College Bescherming Persoonsgegevens (2013). *CPB Richtsnoeren. Beveiliging van persoonsgegevens*. Den Haag: College Bescherming Persoonsgegevens.

Consumentenbond (2016a). ‘Dagvaarding bodemprocedure Consumentenbond / Samsung over Android updates’. https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf

Consumentenbond (2016b). ‘Kort geding Consumentenbond versus Samsung’. https://www.consumentenbond.nl/nieuws/2016/kort-geding-consumentenbond-versus-samsung/

Consumentenbond (2016c). ‘Bodemprocedure tegen Samsung van start’. https://www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start

Consumentenbond (2016d). ‘Pratende pop Cayla slecht beveiligd - update 8 december 2016’. https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd

CPB (2016). *Risicorapportage cyberveiligheid economie*. Den Haag: Centraal Planbureau.

CTIVD (2016). ‘Zienswijze van de CTIVD Op het wetsvoorstel Wiv 20..’. https://www.ctivd.nl/binaries/ctivd/documenten/publicaties/2016/11/09/zienswijze/Zienswijze+van+de+CTIVD_november+2016.pdf

CTIVD (2017). ‘Standpunt CTIVD wetsvoorstel wiv 20.. - vervolg op de zienswijze’. https://www.ctivd.nl/binaries/ctivd/documenten/publicaties/2017/01/31/index/Standpunt+CTIVD+Wiv+20..+-+februari+2017.pdf

Cyber Security Raad (2016). *European Foresight Cyber Security Meeting 2016: Public Private Academic Recommendations to the European Commission about Internet of Things and Harmonization of Duties of Care*. Den Haag: Cyber Security Raad.

Cyber Security Raad (2017). *Ieder bedrijf heeft digitale zorgplichten. Een handreiking voor bedrijven op het gebied van cybersecurity*. Den Haag: Cyber Security Raad.

Davis, J. (2007). ‘Hackers Take Down the Most Wired Country in Europe’. https://www.wired.com/2007/08/ff-estonia/

Deloitte (2016). ‘Cyber Value at Risk in the Netherlands’. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf

Deutsche Welle (2016a). ‘Merkel warns of Russian cyber attacks in German elections’. http://www.dw.com/en/merkel-warns-of-russian-cyber-attacks-in-german-elections/a-36314197

Deutsche Welle (2016b). ‘Germany's domestic intelligence chief accuses Russia of cyberwarfare’. http://www.dw.com/en/germanys-domestic-intelligence-chief-accuses-russia-of-cyberwarfare/a-19256911

Dialogic (2014). *De impact van ICT op de Nederlandse economie*. Utrecht: Dialogic.

Die Welt (2015). ‘Bundestag muss IT-Netzwerk wohl komplett austauschen’. https://www.welt.de/politik/deutschland/article142298394/Bundestag-muss-IT-Netzwerk-wohl-komplett-austauschen.html

ENISA (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*. Heraklion: ENISA.

Eskens, S., J. Timmer, L. Kool & R. van Est (2016). *Beyond Control. Exploratory Study on the Discourse in Silicon Valley About Consumer Privacy in the Internet of Things*. Den Haag: Rathenau Instituut.

European Commission (2015). *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*. Brussels: European Commission.

European Commission (2016). ‘Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’. https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

European Parliament (2016). ‘Cybersecurity: MEPs Back Rules to Help Vital Services Resist Online Threats’. http://www.europarl.europa.eu/news/en/news-room/20160701IPR34481/cybersecurity-meps-back-rules-to-help-vital-services-resist-online-threats

FTC (2015). ‘FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks’. https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

FTC (2016). ‘ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk’. https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

GfK (2015). *Cybersecurity 2015: Awareness, gedrag & digitaal verantwoord ondernemen*. Hilversum: GfK.

Gov.uk (2014). ‘Guidance: Procurement Policy Note 09/14: Cyber Essentials Scheme Certification’. https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification

Greenberg, A. (2015). ‘Hackers Remotely Kill a Jeep on the Highway—With Me in It’. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hendrikman, M. (2016). ‘Ddos-aanval op dns-provider Dyn werd uitgevoerd met Mirai-botnet’. https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dyn-werd-uitgevoerd-met-mirai-botnet.html

Hendriks, A., D. Brandt, K. Turk, V. Kocsis, D. in ’t Veld & T. Smits (2016). *Economische kansen Nederlandse cybersecurity-sector: Een verkenning*. Zoetermeer en Amsterdam: Verdonck, Klooster & Associates B.V. en SEO Economisch Onderzoek.

Hilton, S. (2016). ‘Dyn Analysis Summary of Friday October 21 Attack’. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Hulsebosch, B. & A. van Velzen (2015). ‘Inventarisatie en classificatie van standaarden voor cybersecurity’. https://www.wodc.nl/binaries/2552-volledige-tekst_tcm28-73951.pdf

Inspectie Veiligheid en Justitie (2015). *Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum. Thematisch inspectieonderzoek*. Den Haag: Inspectie Veiligheid en Justitie.

ISE (2016). ‘Three-level IT baseline security system ISKE’. https://www.ria.ee/en/iske-introduction.html

ITU (2015). ‘Global Cybersecurity Index & Cyberwellness Profiles’. http://www.itu.int/pub/D-STR-SECU-2015

Kamerstukken I 2013-2014, CVIII, C. Technische aspecten van (bedrijfs)spionage, juridische normering en privacy. Verslag van een expertmeeting, vastgesteld 5 juni 2014.

Kamerstukken II 2015-2016, 34 372, nr. 2. Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).

Kamerstukken II 2016-2017a, 34 588, nr. 2. Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..).

Kamerstukken II 2016-2017b, 34 372, nr. 23. Motie van het lid Recourt, 13 december 2016.

Kamerstukken II 2016-2017c, 34 372, nr. 14. Motie van het lid Recourt en Tellegen, 13 december 2016.

Kamerstukken II 2016-2017d, 34 588, nr. 58. Motie van het lid Schouten, 8 februari 2017.

Kamerstukken II 2016-2017e, 34 588, nr. 56. Motie van het lid Recourt, 8 februari 2017.

Kamerstukken II 2016-2017f, 34 588, nr. 66. Motie van het lid Recourt, 8 februari 2017.

Keijzer, R. (2016). ‘Insulinepomp uit VS kan gehackt worden’. http://agconnect.nl/artikel/insulinepomp-uit-vs-kan-gehackt-worden

KPMG (2013). *Vijf denkfouten over cybersecurity: Een bestuurdersperspectief op cybersecurity*. Amstelveen: KPMG.

Landler, M. & J. Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’. In: *The New York Times* 29 mei 2007.

Lonkhuyzen, L. van, ‘Meeste melding van datalekken uit zorgsector’. In: *NRC Handelsblad* 28 december 2016.

Lonkhuyzen, L. van, ‘Datalekken bij gemeenten; ‘het is een beetje een zooitje’’. In: *NRC Handelsblad* 27 januari 2017.

Ministerie Binnenlandse Zaken en Koninkrijksrelaties (2012). ‘Baseline Informatiebeveiliging Rijksdienst: Tactisch Normenkader (TNK)’. http://www.earonline.nl/images/ear/6/6f/BIR_TNK_1_0_definitief.pdf

Ministerie van Economische Zaken (2016). *Digitale Agenda: Vernieuwen, vertrouwen, versnellen*. Den Haag: Ministerie van Economische Zaken.

MIVD (2016). *MIVD Jaarverslag 2015*. Den Haag: Militaire Inlichtingen- en Veiligheidsdienst.

Nakashima, E., ‘Powerful NSA hacking tools have been revealed online’. In: *The Washington Post* 16 augustus 2016. https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.a7b20034bd7e

NCSC (2014). *Cybersecuritybeeld Nederland CSBN-4*. Den Haag: Nationaal Cyber Security Centrum.

NCSC (2015). *Cybersecuritybeeld Nederland CSBN 2015*. Den Haag: Nationaal Cyber Security Centrum.

NCSC (2016). *Cybersecuritybeeld Nederland CSBN 2016*. Den Haag: Nationaal Cyber Security Centrum.

Nederlandse Vereniging van Banken (2016). ‘Factsheet veiligheid en fraude’. https://www.nvb.nl/media/document/000254_od15799-nvb-factsheet-veiligheid-en-fraude-06-06.pdf

NIST (2014). ‘Framework for Improving Critical Infrastructure Cybersecurity’. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NOS (2015). ‘Nieuwe wet veiligheidsdiensten: hard nodig of gevaarlijk?’. http://nos.nl/nieuwsuur/artikel/2070103-nieuwe-wet-veiligheidsdiensten-hard-nodig-of-gevaarlijk.html

Overvest, B. & B. Straathof (2015). *What Drives Cybercrime? Empirical Evidence from DDoS Attacks*. Den Haag: Centraal Planbureau.

Prins, R., ‘AIVD moet helpen digitale ophaalbrug snel te openen’. In: *Het Financieele Dagblad* 10 mei 2016.

PwC & VU (2014). *Cybercriminaliteit tegen Nederlandse organisaties: een digitale dreiging*. Amsterdam: PwC & Vrije Universiteit Amsterdam.

PwC (2014). *Verkenning naar gescheiden ICT-netwerken en -diensten in Nederland*. Amsterdam: PwC.

PwC (2016). *Moving Forward with Cybersecurity and Privacy: How Organizations are Adopting Innovative Safeguards to Manage Threats and Achieve Competitive Advantages in a Digital Era*. New York, NY: PwC.

Rathenau Instituut (2014). ‘Notitie cyberintelligence en publiek belang: Expertmeeting Eerste Kamer 6 mei 2014’. https://www.rathenau.nl/nl/publicatie/notitie-cyberintelligence-en-publiek-belang

RVS (2016). ‘Samenvatting advies voorstel nieuwe Wet op de inlichtingen- en veiligheidsdiensten’. https://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=421

Security.nl (2016). ‘Beveiligingsbedrijf verdenkt scriptkiddies van aanval op Dyn’. https://www.security.nl/posting/490384/Beveiligingsbedrijf+verdenkt+scriptkiddies+van+aanval+op+Dyn

Scott, J. & D. Spaniel (2016). ‘Rise of the Machines: The Dyn Attack Was Just a Practice Run’. http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf

Traynor, I. (2007). ‘Russia Accused of Unleashing Cyberwar to Disable Estonia’. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Trend Micro (2016). ‘Frequently Asked Questions: BlackEnergy’. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

US Department of Homeland Security (2016). ‘Strategic Principles for Securing the Internet of Things (IoT)’. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten*. Den Haag: PostNL.

Voster, W. & J. de Bruijn (2016). *Cyber security supply chain risicoanalyse 2015*. Den Haag & Utrecht: Royal Dutch Shell & Power of 4.

Zetter, K. (2014). 'Hacker Lexicon: What Is an Air Gap?' https://www.wired.com/2014/12/hacker-lexicon-air-gap/

Annex 1: Interviewees

Ioannis Agrafiotis, Oxford University

Philipp Amann, Europol

Axel Arnbak, De Brauw Blackstone Westbroek N.V.

Kraesten Arnold, Dutch Ministry of Defence

Jaya Baloo, KPN

Arie van Bellen, ECP

Bibi van den Berg, Leiden University

Herbert Bos, VU University Amsterdam

Aad van Boven, SecureMe2

Lotte de Bruijn, Nederland ICT

Marjolijn Durinck, ECP

Jos de Groot, Dutch Ministry of Economic Affairs

Wim Hafkamp, Rabobank

Raymond van den Hoek, Bol.com

Erik Huizer, Surfnet

Demosthenes Ikonomou, ENISA

Gerrie de Jonge, PostNL

Elena Kvochko, Barclays

Steven Luitjens, Dutch Ministry of the Interior and Kingdom Relations

Dave Maasland, ESET

Nicole Mallens, VNO-NCW/MKB-Nederland

Ron de Mos, Nederland ICT

Jason Nurse, Oxford University

Wouter Oosterbaan, Netherlands' National Coordinator for Security and Counterterrorism (NCTV)

Bastiaan Overvest, Netherlands Bureau for Economic Policy Analysis (CPB)

Erik Poll, Radboud University

Ronald Prins, Fox-IT

Melanie Rieback, Radically Open Security

Marijn Schuurbiers, Dutch National Police Force

Ton Siedsma, Bits of Freedom

Robert Spronk, General Intelligence and Security Service (AIVD)

Eelco Vriezekolk, Radiocommunications Agency Netherlands

Maurice Wessling, Dutch Consumers' Association

Jos Weyers, TenneT

Patricia Zorko, Netherlands' National Coordinator for Security and Counterterrorism (NCTV)

Large multinational corporation

Annex 2: Workshop participants

Kraesten Arnold, Dutch Ministry of Defence

Herbert Bos, VU University Amsterdam

Aad van Boven, SecureMe2

Jeremy Butcher, Fox-IT

René Corbijn, Nederland ICT

Michel van Eeten, Delft University of Technology

Nico van Eijk, Institute for Information Law

Jos de Groot, Dutch Ministry of Economic Affairs

Raymond van den Hoek, Bol.com

Floor Jas, Surfnet

Eric Kaasenbrood, Rabobank

Linda Kool, Rathenau Institute

Matthijs Kouw, Rathenau Institute

Gino Laan, Dutch Ministry of the Interior and Kingdom Relations

Jos Leenheer, National Cyber Security Centre (NCSC)

Dave Maasland, ESET

Nicole Mallens, VNO-NCW/MKB-Nederland

Geert Munnichs, Rathenau Institute

Erik Poll, Radboud University

Els Prins, VNO-NCW/MKB-Nederland

Melanie Rieback, Radically Open Security

Hessel Schut, Dutch National Politie Force

Ton Siedsma, Bits of Freedom

Jelte Timmer, Rathenau Institute

Maurice Wessling, Dutch Consumers' Association

General Intelligence and Security Service (AIVD)