CPB Netherlands Bureau for
Economic Policy Analysis

Cyber Security Risk Assessment for the Economy 2019

The risk of **damage to society** by cyber incidents seems to increase with **further digitalization**.

It is often unclear what the financial and societal consequences are of a digital attack or digital espionage.

This is because companies:

1) do not notice every attack;

2) do not publicize every attack;

3) cannot always know what the long term consequences of a hack or theft are.

This incomplete image of the costs and benefits of investing in cybersecurity means the level of investment could be both too high or too low.

This lack of insight also hampers the development of a cyberinsurance market.

CPB Communication
Bastiaan Overvest, Marielle Non, Milena Dinkova,
Ramy El-Dardiry and Rinske Windig

October 2019

Better information is crucial

Cyber-attacks occur are **known** to occur in businesses, households and government bodies

It is **unknown** how often disruptions occur, by who and what the consequences are

Users might therefore **overinvest or underinvest** in cybersecurity

Cyber Security Risk Assessment for the Economy 2019

Risks of disruption

Threats are complex and constantly evolving

Critical processes have become more vulnerable to ICT-disruptions. This could lead to disruptions of society

Non-critical processes are entwined with critical processes which makes the chain more vulnerable

New risks

Artificial intelligence makes personalized attacks possible and can find system vulnerabilities more easily

5G facilitates new Internet-of-Things applications. This makes cybercrimes more visible outside of the digital world

Challenges for businesses and citizens

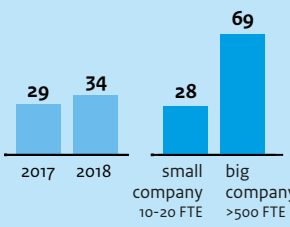
- How much do we invest in cybersecurity? Effects of investments are hard to quantify
- How can we keep up to date if threats and security measures develop so fast?
- How to guarantee security in a chain of ICT-applications?

Challenges for government

- How to inform millions of users and hunderds of thousands of businesses?
- Leave measures against disinformation to social media or regulate?
- How effective is stimulating cooperation between organizations?

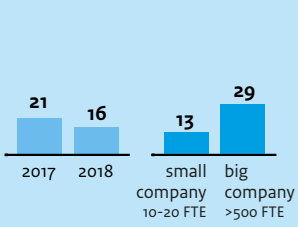
Small companies take less measures compared to big companies

% of companies that encrypt their data



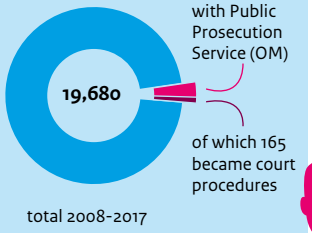
Companies report **fewer ICT-incidents**

% of companies that deal with outside attacks



Most cybercrimes **never reach a judge**

amount of registered hacking crimes



source: CBS

1 Introduction

1.1.1 Persistent risks, new risks and uncertainty

The risks of disruptive cyber incidents have not decreased. Critical processes are dependent on ICT, and technological developments, such as 5G, will only increase this dependence, both within and outside the critical infrastructure. With the ongoing international political unrest, there is a continued risk of nation-state actors deliberately disrupting critical infrastructure. Digital disruptions pose a real risk to society, particularly because of the combination of persistent geopolitical threats and increasing digitalisation.

Rapid developments in the field of artificial intelligence are creating new risks, but also offer new opportunities for cyber security. Research into artificial intelligence (AI) is flourishing; for example, algorithms are becoming increasingly effective in recognising patterns and making decisions in complex situations. Some AI applications may also lead to new or greater risks for cyber security. An example of such a risk is the *deep fake* technique, in which AI is used in the production of fake photographs and videos. The technique could be exploited by nation-state actors to spread disinformation. Cyber criminals can also use deep fake in identity fraud and *spear phishiakeng* (i.e. sending targeted and personalised e-mails in order to unlawfully obtain or hack into information). Artificial intelligence can also be used in rapid and systematic searches for software vulnerabilities, with the aim of subsequently exploiting those vulnerabilities. On the other hand, AI also offers opportunities for cyber security. It can be used to help detect deep fake products and other forms of disinformation, DDoS attacks and rogue websites. The possibilities for detecting software vulnerabilities can be used by software developers, thus preventing vulnerable software from entering the market.

Uncertainty and incomplete information are hampering cyber security policy. Various opinions and guidelines are circulating on the optimal investment level for cyber security and on what measures should be taken. Nevertheless, or precisely because of that, it is difficult for individual users and organisations to make informed decisions about which measures to take. This is partly due to the fact that existing opinions and guidelines are never an exact match for the situations of specific users and organisations, and partly due to a lack of information about the extent of cyber risks and their financial consequences. And finally, some of the consequences of inadequate cyber security may have an impact on third parties. This lack of information prevents users from determining the benefits of their investment in security. It also forms an obstacle for government policy: to what extent would it be desirable to stimulate private and public investment in cyber security? For cyber insurers, the lack of information means that premiums cannot be properly risk-based.

The fragmented landscape of initiatives on collaboration and education may hamper the provision of information. The government uses multiple channels to informs various target groups about cyber risks. In addition, it seeks to stimulate various public–private partnerships to encourage participants to share knowledge and experiences. In certain cases, these initiatives on collaboration and education may overlap. The risks of this type of fragmentation include those of target groups being less aware of where relevant information can be found, of initiatives duplicating each other's work, and of important themes being left unaddressed.

1.1.2 Businesses have increased their resilience, households are lagging behind

Over the past year, Dutch companies have taken more measures to increase their resilience. In 2018, they implemented more measures to enhance their resilience to digital disruption. For example, the percentage of companies using two-factor authentication increased by 9 percentage points (34% in 2017) and more companies created log files for the purpose of analysing incidents (from 55% in 2017 to 60% in 2018). Fewer

companies suffered costs following an ICT incident involving an external attack (1.3% in 2018 compared to 2.3% in 2017). It should be noted that, particularly in the case of smaller businesses, the adoption of measures appears to be lagging behind, causing these businesses to run more of the avoidable risks.

Households remain vulnerable. Households have only limited knowledge of cybercrimes, particularly with respect to the latest cyber risks. In 2018, 8.5% of households fell victim to digital crime. People who are less alert could be more at risk if AI is used in phishing/spear phishing or when disinformation is generated.

1.2 Aims, definitions and scope

Similar to the previous risk assessment reports, the purpose of this edition is also to provide insight into the trends, causes and economic consequences of various cyber risks. The focus of this report lies primarily, but not exclusively, on the Netherlands and the past year (from the time of the publication of the previous risk assessment, which was on 15 October 2018). Opinions and definitions of cyber risks differ. The NCSC's definition of cyber security is 'striving for the prevention of damage caused by the disruption, failure or improper use of ICT and restoring any damage that has nevertheless occurred'. Based on this definition, cyber risks can be defined as threats that may cause damage, system failure or lead to various forms of exploitation of ICT. DDoS attacks and ransomware (hostage software) clearly fall under this definition and are therefore discussed in this report.

Here, we consider cyber security from a broader perspective than only traditional ICT-focused security. This report focuses on the threats and related phenomena that have a digital impact on both the economy and society. This broader perspective, thus, also includes cybercrime and the fight against it. Cybercrimes are crimes committed using digital methods. Although phishing and purchasing fraud can also be committed without digital means, the scale at which the fraud occurs can be much larger through the use of e-mail, online trading platforms and social media, which also increases the societal impact of such crimes. In addition to cybercrime, disinformation and economic espionage, often by nation-state actors, are important threats that can affect public confidence in the digital arena. Although disinformation and economic espionage can also occur outside digital channels, the scale at which it occurs can be much larger through the use of social media and the exploitation of software vulnerabilities and digitally stored information. The physical security of the Dutch digital infrastructure falls outside the scope of this report.

Our study was co-funded by the Dutch Ministry of Justice and Security. We made use of a sounding board group and gained insights from discussions with various experts and stakeholders. We hereby would like to thank all these people and organisations for their help and for sharing their thoughts and opinions in relation to this subject. The responsibility for the risk assessment itself rests entirely with CPB.

Since 2016, CPB has published an annual Cyber Security Risk Assessment (CSRA) for the Economy. The current publication will be the last one in this format, for the foreseeable future. These risk assessment reports have provided an overview of a large number of risks and 'bottlenecks' (e.g. employment in the ICT sector, and the market for cyber security services and DDoS mitigation) and have identified the underlying causes ('market failure') from an economic perspective. Where possible, the assessments have provided insight into the quantitative scope of trends and the economic impact of risks. In the future, insights into the economic causes and impacts of cyber security disruptions will remain important for policymakers, but will have to be obtained from other sources. This could be achieved through targeted empirical studies or by conducting these types of risk assessments less frequently.

1.3 Reader

This Cyber Security Risk Assessment for the Economy 2019 (CSRA2019) contains a discussion of the main risks to the economy and ultimately to society, as they relate to the cyber domain. Chapter 2 describes the developments of specific events and threats of the past year — for example, addressing how often a particular event occurred, both in the Netherlands and abroad. It also provides an indication of future risks, based on policy and technological developments. Chapter 2 is mainly descriptive; for information about the economic perspective of market failure and its possible economic impact, we refer to the previous editions of this series of risk assessment reports. Chapter 3 focuses on the impact of the mostly digital threats to the economy and society, rather than on the means.

This report is the translation of the original Dutch report. The original report was published on October 17 2019 and can be found here: link. Incidents, policy changes or other notable events that occurred after this date are not included in the translated version.

2 Assessment of cyber risks

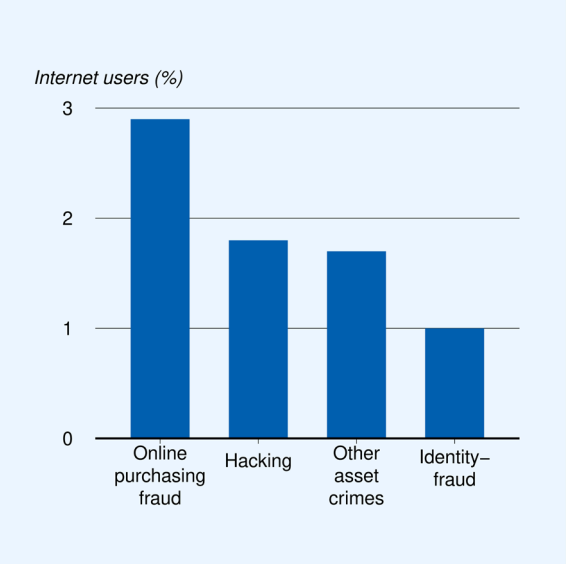
2.1 Introduction

For a few hours on 24 June of this year, the 112 emergency telephone number could not be reached. Although, according to provider KPN, the system had not been hacked and the investigation into the cause is still ongoing, it does illustrate how our society depends on digital systems. As far as we know, apart from the 112 failure, the Netherlands has not experienced any major cyber incidents, such as large-scale malware infections or very large DDoS attacks, over the past year. The situation was different in 2017, with the WannaCry and NotPetya malware infections. In addition, in early 2018, there were a number of DDoS attacks on the websites of Dutch banks, the Tax Department and the DigiD identity management platform. In addition, in April 2018, Russian spies attempted to hack into the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague.

The risks of disruptive cyber incidents have probably not decreased over the past years. The disruption to the 112 emergency number on 24 June 2019 showed that critical processes depend on digital resources. As a result of the increasing digitalisation, society has become increasingly dependent on digital assets. Disruptions to cyber security, such as those caused by an attack from a malicious hacker or a foreign espionage service, can therefore have major consequences. For example, in a recent study, the Netherlands Court of Audit warned that digital security has not been properly organised at a number of critical waterworks and that the degree to which Rijkswaterstaat is able to deal with a cyber attack could be improved. The future implementation of 5G will further increase the dependence on digital processes. There is no reason to assume that the threat from either nation-state actors or cybercriminals has diminished, over the past year (AIVD, 2018; NCTV, 2019)

Businesses and households are regularly adversely affected and, in some cases, financially harmed by cybercrime and cyber insecurity. For example, 4.6% of internet users say they were the victim of a digital asset crime, such as fraud in online purchases[1], in 2018. In addition, 1.8% of them were hacked, see Figure 2.1. The consequences may be financial, as in the case of fraud, but also non-financial, such as the loss of documents. In addition, there are also indirect effects; almost 4 out of 10 victims had less confidence in digital security after having been hacked, and more than a quarter of internet users sometimes refrain from internet banking because of concerns about security. Almost half of the Dutch companies (48%) experienced an ICT security incident in 2018, and, for 1 in 5 cases, these incidents had financial consequences.[2]

Figure 2.1 Fraud in online purchasing is the most common form of cybercrime



Source: CBS (2019)

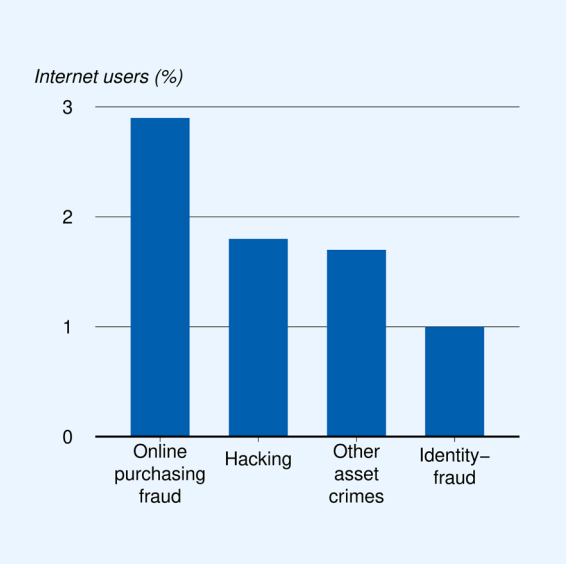
The impact of the various cyber risks differs per type of threat. The following sections, therefore, discuss the most important developments for various threats and vulnerabilities and provide a qualitative risk assessment.

2.2 Hardware and software vulnerabilities

A vulnerability is a weakness in hardware or software that cyber criminals are able to exploit. Weaknesses can be caused by errors or holes in both the design and implementation of hardware or software. Cybercriminals and nation-state actors tap into these vulnerabilities and carry out cyber attacks, using specific software, so-called exploits. These attacks range from ransomware to the mining of crypto coins.

[1] Online purchasing fraud is one of the forms of digital asset crime. Other forms include advance fee scams, Microsoft scams and fake fines. (CBS, 2018).
[2] Source: CBS Statline.

Figure 2.2 Development of vulnerabilities, per risk profile



Source: United States National Vulnerability Database (link).

Hardware and software vulnerabilities continue to pose a major cyber security risk. In 2017, the number of known vulnerabilities in the National Vulnerability Database (NVD)[3] increased, considerably, but subsequently remained on a comparable level in 2018 (see Figure 2.2). An alternative database of the private company *Risk Based Security* shows the same trend, but with a higher baseline level (for 2018, 22,000 vulnerabilities versus 16,500 in the NVD) (Risk Based Security, 2018). The difference in absolute numbers illustrates that keeping an accurate record of vulnerabilities is a challenge. Part of the increase in the number of known vulnerabilities can probably be attributed to an increase in digital crime reporting by organisations.

The Internet of Things increases the likelihood of the presence and exploitation of vulnerabilities. The Internet of Things (IoT) has the potential to drastically increase the number of Internet-connected devices. IoT devices are relatively poorly secured and security updates are rarely carried out.[4] Vulnerabilities in these devices therefore offer opportunities for cybercriminals. Most of the criminal activities via IoT devices have so far been aimed at launching large-scale DDoS attacks.[5] However, the development of the VPN filter malware shows that the potential threats via IoT are greater than that.[6] This malware, which lodges itself in routers, can be used to intercept communications and erase data from infected devices.

Dependencies in the software supply sector affect the likelihood of vulnerabilities being exploited. Organisations are increasingly outsourcing parts of their digital infrastructure or services. This may increase security, if the chosen supplier has invested more in cyber security than their client. However, such outsourcing can also increase risks, if suppliers have not taken sufficient security measures (Skybox Security, 2019). For example, the exploitation of a vulnerability in the software supply chain occurs when

[3] This database is maintained by the US National Institute of Standards and Technology.
[4] See, for example, the WODC report (Verkeerd) verbonden in een slimme samenleving (2017) [Wrong connections in a smart society].
[5] According to Symantec, by 2018, almost 80% of IoT attacks were related to DDoS threats via LightAidra, Kaiten and Mirai exploits. See Symantec (2019).
[6] See news messages about VPNfilter here and here.

updates have been infected with malicious code. For 2018, Symantec reports a 78% increase in this type of attack (Symantec, 2019).

The knowledge about vulnerabilities and code (i.e. exploits) with which these vulnerabilities can be exploited by criminals or nation-state actors is being traded in various ways. For example, technology companies often maintain 'bug bounty' programs through which researchers receive financial compensation for finding and reporting vulnerabilities.[7] At the other end of the spectrum, there is a black market on which cybercriminals buy and sell exploits and vulnerabilities. Most of these exchanges take place on the dark web and are therefore difficult to trace. In addition, there is a 'grey' market through which governments often buy knowledge about vulnerabilities — for example, as part of their cyber defence programme. The desirability of the use of zero-day vulnerabilities by the Dutch Government is the subject of political debate.[8] The price of exploits or knowledge about vulnerabilities varies from hundreds to hundreds of thousands of US dollars and depends on how easy they were to detect, how many other vulnerabilities have already been detected in the product in question and their possible impact (Ablon and Bogart, 2017).

The use of artificial intelligence may both increase and decrease the risk of exploitation of vulnerabilities. The search for vulnerabilities and the development of exploits are rather labour-intensive activities, which may cause supply to be limited.[9] Vulnerabilities may be detected sooner through the use of machine-learning techniques. If these techniques are applied by malicious parties, this increases the risk of exploitation,[10] but if used by software developers, it reduces the chances of such vulnerable software reaching the market, at all.[11]

2.3 DDoS attacks

A distributed denial of service (DDoS) attack, is an attack in which a web service is inaccessible because it is being flooded by incoming network traffic from various sources[12].Roughly speaking, there are two types of DDoS attacks: volume attacks (the largest possible amount of network traffic sent to a single target) and application layer attacks (attacks on underlying computer systems)[13]. Serious DDoS attacks on the websites of banks and the Dutch Tax and Customs Administration took place at the beginning of 2018, making them temporarily inaccessible[14]. Since then, no successful DDoS attacks on critical infrastructure have been reported. However, incidents involving smaller websites have occurred; for example, there were several successful attacks on *Magister*, a Dutch online school platform.[15]

[7] See, for example, this article about the bug bounty programme by Facebook.
[8] See, for example, this NOS news item (in Dutch).
[9] Ibid.
[10] See, for example, this article of the World Economic Forum and this CSO article.
[11] See, for example, this blog by Bruce Schneier.
[12] See p.48 in NCTV (2019), for their definition.
[13] The previous Cyber Security Risk Assessment (CSRA) for the Economy (CPB, 2018) contains more details about DDoS attacks (types and trends) and related risks and policy options.
[14] See this NOS news item (in Dutch).
[15] See this and this news message (in Dutch).

DDoS attacks continue to be prevalent and increasingly vary in duration and size. The number of DDoS attacks that were observed and thwarted by NBIP, a Dutch provider of DDoS mitigation services, increased by nearly 15%, between 2017 and 2018.[16] This increase continued over the first half of 2019.[17] In both 2017 and 2018, most attacks amounted to fewer than 10 gigabits per second. However, the largest attack in 2018 was almost twice as large as the largest of 2017 (68 and 36 gigabits per second, respectively), and the proportion of very small attacks increased in 2018. The average duration of an attack remained roughly the same, between 2017 and 2018. Also, on a worldwide level, there are no clear indications of the number of DDoS attacks diminishing.[18]

Booter websites remain a persistent problem. These are websites that facilitate low-threshold DDoS attacks, so that virtually anyone (also those without any expertise) is able to buy and carry out a DDoS attack.[19] In December 2018, the US Federal Bureau of Investigation (FBI), in cooperation with the Dutch police, took 15 booter websites offline.[20] Whether this will lead to a temporary or longer-term effect on the risk of DDoS attacks is still uncertain. There are indications of new booter websites having been set up,[21] and, after a temporary decline, the number of DDoS attacks appear to have increased again in the first months of 2019.[22]

The increasing number of IoT devices in combination with a growing digital infrastructure may potentially lead to stronger and longer DDoS attacks. The roll-out of 5G, the fifth-generation mobile network, has the capacity to facilitate larger DDoS attacks, as it enables more data traffic and allows for mobile devices with stronger processors to be connected to the mobile network. This may particularly affect the impact of volume attacks, because more and more IoT devices can be connected. Devices such as smart refrigerators and toasters, Wi-Fi sockets and plugs are generally not very secure.[23] These devices form weak links as they can be integrated into a botnet by malicious parties to be used in more powerful DDoS attacks.[24]

DDoS attacks remain a risk for the Netherlands and their potential financial impact can be significant. Although DDoS attacks currently tend towards vandalism and are often targeted at educational institutions and small web shops, it cannot be ruled out that nation-state actors may use DDoS attacks aimed at the national critical infrastructure.[25] Even when the target is one of non-critical infrastructure, the consequences of a successful DDoS attack can still be significant. A joint report by NBIP and SIDN (2018) makes a first attempt to assess the damage caused by DDoS attacks and estimates the financial impact per attack at hundreds of thousands of euros, depending on the sector and the season.

Taking down booter websites, educating potential cyber criminals and the use of DDoS mitigation services all remain necessary. Although a number of booter websites have been shut down, attacks can still be purchased online. In addition, with the increasing number of poorly protected IoT devices, it is relatively easy for cybercriminals to launch a new booter service. Continued efforts are therefore needed to shut down these websites. Over the past year, the police have launched a campaign to make schoolchildren aware that a

[16] See this link for a news message about the DDoS data reports by the Dutch supporting services for Internet providers (NBIP) (2017, 2018) summarised.
[17] See NBIP (2019).
[18] See this message by Kaspersky.
[19] The issue of buying DDoS attacks online was also discussed in the Dutch House of Representatives in the spring of 2019 (Parliamentary documents II, 2018/2019, 1853).
[20] See tweakers.net for this news message by the U.S. Department of Justice. Earlier in 2018, a major provider of DDoS services, webstresser.org, was taken down (see this NOS news item and this message on politie.nl). Around 135,000 customers were registered on this platform, enabling them to carry out any DDoS attack of their choice, at a rate starting from EUR 15 per month.
[21] See, for example, this news message and this report by Nexusguard.
[22] According to this message by Kaspersky and NBIP (2019).
[23] This survey, conducted at the request of the Dutch Ministry of EZK, for example, shows that most respondents are aware of the security risks, but nevertheless, less than half of them take actual steps to protect IoT devices.
[24] See, for example, Cisco (2018). These risks are also mentioned in the ENISA Threat Landscape report (ENISA, 2018).
[25] The NCTV (2019) discusses in detail the risks posed by government bodies.

DDoS attack is a criminal offence rather than a misdemeanour. Initial figures suggest that these campaigns are successful.[26] DDoS attacks can be effectively thwarted by using a DDoS mitigation service, such as the NaWas by NBIP. In 2019, however, there were several successful attacks. This suggests that not all websites or hosting providers use DDoS mitigation. More awareness and use of mitigation services could prevent financial damage and would make it less attractive for criminals to buy these attacks.

2.4 Financially motivated malware

Malware is malicious software that allows a cybercriminal to take control of a computer. The most common form of malware is ransomware — software that blocks computers or access to the information they contain. Victims have to pay a ransom in order to regain access. In recent years, also other variants of malware have emerged. Examples are *cryptojacking*, criminals using the power of the infected computer's processor to extract crypto currency (e.g. bitcoin) (CPB, 2018), and *formjacking*, where criminals try to steal payment data or other confidential information by infecting payment forms on web shops with malware that can read them.

Ransomware regularly causes casualties and may have a substantial financial impact. Over the past year, several organisations came into contact with ransomware. According to security company Fox-IT, dozens of Dutch companies have fallen victim to a ransomware known as *SamSam*.[27] It is unknown how many and exactly which Dutch companies were affected or what the financial damage was. In some international cases, however, the direct financial impact is known. Over the past year, several US cities were attacked by ransomware and reportedly made ransom payments totalling over one million US dollars.[28] Norwegian aluminium producer Hydro fell victim to the *LockerGoga* ransomware, last March, and reported a financial damage of EUR 31–36 million.[29] In addition to the direct financial impact (i.e. the ransom), there are also indirect costs in the form of data, time and production losses — these costs are probably higher than the direct financial impact.

Despite the fact that cases of ransomware are still in the news on a regular basis, the threat of ransomware seems to have lessened. The NCTV reported this year that the number of ransomware infections in the Netherlands appears to have decreased. Symantec (2019) and Microsoft (2019) also saw a decrease in the number of infections. Several explanations can be given for these decreases. Security companies, such as Symantec, state that they are better able to detect ransomware before it reaches the end user. It is also possible that users have become more aware of the risks and, as a result, for example, update software more frequently, make more backups, or handle suspicious e-mails with more caution. A third explanation could be that the profitability of ransomware has come under pressure. For example, via the 'No More Ransom' platform, victims of ransomware can often recover the encrypted data without having to pay the ransom. This undermines this particular revenue model of cyber criminals.

In 2018, formjacking increased in popularity, while cryptojacking activities seem to be strongly related to the value of cryptocurrencies. Symantec (2019) reports a global increase in formjacking over the course of 2018, with a total of 3.7 million thwarted formjacking attempts, of which 1 million occurred in the months of November and December. According to the same Symantec report, cryptojacking activities decreased by 52% in 2018. This was probably due to the sharp decrease in the value of crypto currencies. Cryptojacking nevertheless will remain an interesting option for cybercriminals because of the anonymity of the perpetrators and the low barriers to committing this type of crime.

[26] See this message by the Dutch police.
[27] See this Fox-IT message (link).
[28] Source: https://nos.nl/l/2290780 and here.
[29] Source: Hydro news item (link).

The risk of malware is permanent, as cybercriminals work on innovating their methods. In part, because of the global infections of the WannaCry and NotPetya viruses in 2017, organisations have become more aware of the risks and have taken precautions, such as updating software and making backups on time. For malware creators, this means that they need to modify their product if their activities are to remain profitable. There are indications that this is happening. For example, the SamSam ransomware deletes or sabotages backups before blocking files. As a result, the owner of an infected computer system may not be able to rely on any previous backups and is, thus, more likely to pay the ransom. Cybercriminals can also deploy ransomware in smarter ways and targeted at specific organisations.[30] Instead of untargeted mass distribution, cybercriminals are able to up their illegal earnings by targeting the organisations that are highly dependent on IT systems and that suffer rapid production losses when systems are down. This is similar to the distinction between regular phishing and spear phishing, or between untargeted and targeted advertising.

2.5 Social engineering

Social engineering refers to techniques that mislead users into disclosing certain information or taking specific actions to their own detriment.[31] This broad definition includes, for example, *phishing* e-mails or purchasing and sales fraud, but also fake fines/invoices and advance fee scams (or Nigerian fraud).[32] In the case of *phishing*, cybercriminals use certain techniques to gain the trust of their victims. For example, by replicating reliable domains or persons, or by leading the victims to fake login pages.[33] If *phishing* is aimed at specific individuals or institutions, it is referred to as *spearphishing*. In the case of purchasing and sales fraud, the victims do not receive either money or the product or service they paid for. *Phishing* and purchasing and sales fraud are cybercrimes often encountered by individual users and are therefore discussed in this report.

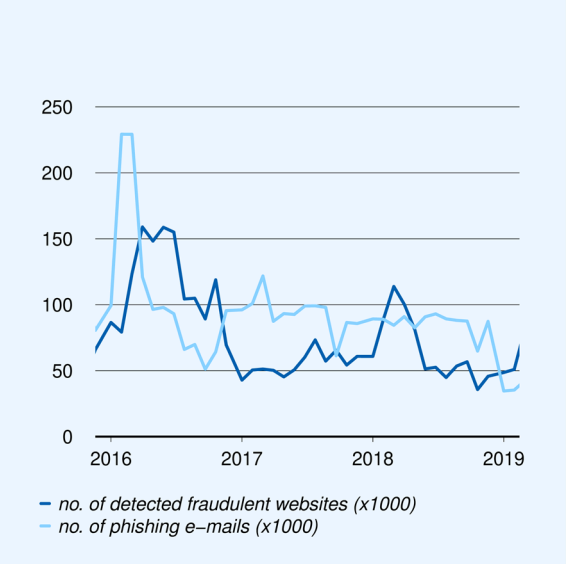
2.5.1 Phishing

Phishing remains a method often used by cybercriminals. Statistics Netherlands (CBS, 2018) estimates phishing to be the cause of approximately 30% of the type of digital fraud where victims have money removed from their bank accounts. Figure 2.3 shows that the number of detected rogue websites and phishing e-mail campaigns, worldwide, has fluctuated considerably over time, but since 2017 has remained at a comparable level. The Dutch Payments Association (Betaalvereniging Nederland) finds that the total damage caused by fraud within the payment system is declining, but that fraud due to phishing has actually increased from EUR 1.05 million in 2017 to EUR 3.81 million in 2018. In their annual Security Intelligence Report, Microsoft shows that the share of phishing e-mails in total e-mail traffic increased in 2018.[34] The number of fake e-mails reported via the Fraud Help Desk (de Fraude helpdesk) peaked in the first months of 2019, see Figure 2.4. This peak may be due to an increase in phishing activity or a greater awareness of the existence of the help desk itself.

[30] This is in line with the finding that cybercriminals appear to focus ransomware attacks more on businesses. Symantec (2019), for example, reports a 12% increase in corporate ransomware infections, while the total number of infections is decreasing.
[31] See the Glossary of ENISA, for their definition of social engineering.
[32] See here the explanation of Nigerian fraud.
[33] For example, see Microsoft (2019).

[34] Press release by Betaalvereniging Nederland, see here. (in Dutch)

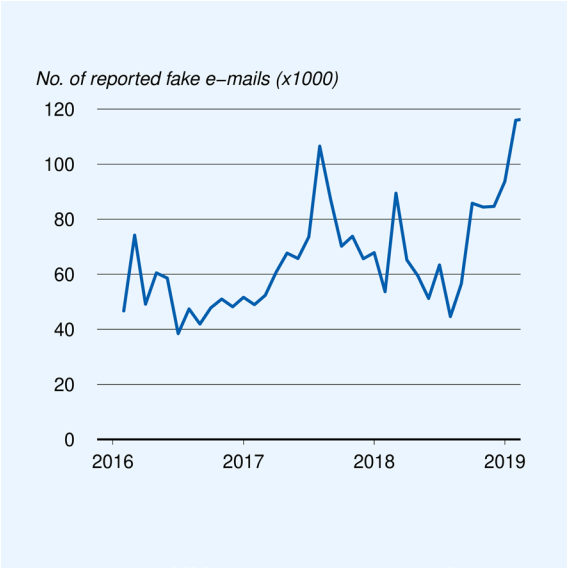
Figure 2.3 Detection of malicious websites and phishing e-mails, worldwide, 2016–2019



Source: Anti Phishing Working Group Phishing Attack Trends Reports, link.

Spear phishing is also a risk in the Netherlands. This can be concluded from several incidents that have occurred over the past year. Attackers, for example, have posed as employees of specific care institutions in order to obtain confidential data.[35] The Dutch branch of Pathé Cinemas lost EUR 19 million through spear phishing.[36] In its cyber security assessment for the Netherlands (NCTV, 2019), NCTV warns that spear phishing has a high chance of success because attacks are difficult for victims to recognise.

Figure 2.4 Reported number of fake e-mails in the Netherlands, 2016–2019



Source: Fraudehelpdesk.

[35] See, for example, here and this message by the Elkerliek hospital.
[36] See, for example, this NOS news item (in Dutch).

Both phishing attacks and phishing detection methods are becoming increasingly sophisticated. It is now possible to successfully conduct phishing attacks even in the case of two-factor authentication.[37] In addition to e-mails, cybercriminals also use other digital means of communication, such as WhatsApp and social media, to increase the credibility of phishing attempts and circumvent spam filters.[38] A recent development is the use of software that mimics the voice of, for example, a company's executive with the malicious intent to obtain money.[39] These forms of phishing are personalised and therefore more time-consuming for perpetrators to implement. In theory, however, Artificial Intelligence could automate the time-consuming aspects of spear phishing.[40] This could increase the magnitude and frequency of spear phishing attacks, while lower costs for criminals could mean that a larger group of people may become interesting targets for spear phishing attacks (Herley, 2010). Artificial Intelligence is also used by both established companies and start-ups to protect consumers and businesses against phishing.[41] Machine Learning, for example, is used in the early identification of suspicious messages. The use of physical keys in two-factor authentication also appears to be a good way to combat phishing.[42]

2.5.2 Online purchasing fraud

Purchasing fraud is a common type of cybercrime. In the case of purchasing fraud, consumers pay for products or services they will never actually receive. In 2018, 2.7% of Dutch households reported to have been the victim of purchasing fraud (CBS, 2019). For a large proportion of those victims, the fraud took place via a second-hand sales platform (e.g. Marktplaats.nl, Tweakers.nl and Speurders.nl). In a quarter of cases, victims were defrauded via a fake web shop. Sales fraud, where the victim delivers the product but the recipient does not pay, is far less common. In 2018, 0.2% of Dutch households were affected by this type of fraud.

The chances of getting caught while committing purchasing fraud are relatively small, which makes it attractive to criminals. Of the victims of purchasing fraud, 39% reported the incident to either the police, the bank or the website involved (e.g. *Marktplaats.nl*). In the end, 23% of those victims filed an official complaint with the police. According to participants in a survey on the matter, among the main reasons for not officially reporting the incident were the fact that it concerned only a small amount of money, or that filing a police report would not help them to get their money back (23.5% and 16.9%, respectively). However, as cybercriminals can relatively easily defraud large numbers of people via digital means, all these relatively small amounts add up and provide them with a substantial total profit.

There are several initiatives to combat purchasing fraud. In order to simplify and stimulate reporting, victims can report fraud online.[43] All reports are collected at the national hotline for internet fraud (*Landelijk Meldpunt Internet Oplichting*), a special division of the police. This unit works together with banks, certification organisations, hosting companies and consumer information television shows, such as *Opgelicht* and *Kassa* to combat online fraud. If, for example, multiple incidents of fraud are reported against particular entities, the bank accounts of those perpetrators could be blocked or fake web shops be taken offline. The police also regularly speak out to warn consumers and to emphasise the importance of reporting fraud to the police, even if not every report leads to prosecution.

[37] See, for example, this news message.
[38] See here for an SMS example and here for an example of a WhatsApp message. The police speak of hundreds of reportings of *phishing* by SMS.
[39] See this FD news item.
[40] See, for example, Brundage et al. (2018) and this message by the World Economic Forum.
[41] See, for example, here (Microsoft) and here (INKY).
[42] In 2018, Google claimed that, since the introduction of physical keys, phishing attacks on its employees have not been successful. See this message.
[43] This can be done via the police website.

Purchasing fraud can be combatted more intensively through more frequent preventive action. The initiatives discussed above, generally, all focus on intervention after these crimes have been committed. In order to strengthen the fight against purchasing fraud, more can be done in the way of preventive measures. For example, SIDN is working on methods for automatically detecting unreliable websites and taking them offline at an early stage, instead of the current methods of not intervening until after the crimes have been committed and reports have been filed.[44] Second-hand sales platforms may also be able to apply such preventive techniques, so that fraudulent advertisements and providers can be traced before they cause any damage.

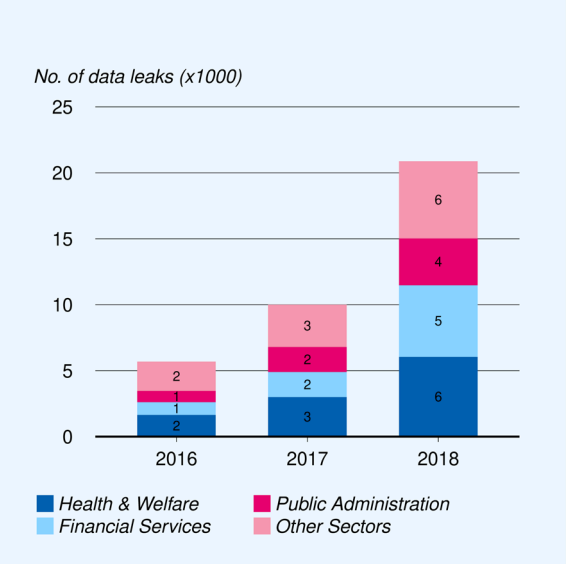
2.6 Data breaches

Since 2016, the number of reported data breaches has more than tripled. A data breach gives someone unauthorised or unintentional access to personal data, or personal data are unwittingly destroyed, lost, altered or provided.[45] Losing a USB flash drive, accidentally sending an e-mail with confidential information to the wrong person, as well as being deliberately hacked, are all examples of data breaches. Figure 2.5 shows the number of reported data breaches, per sector, between 2016 and 2018. The three sectors with the most reports are Health & Welfare, Financial Services and Public Administration. In 2016, almost 6,000 data breaches were reported, whereas in 2018 there were over 20,000 reports. Between 1 January and 1 May 2019, almost 8,000 reports were received by the Dutch Data Protection Authority (DPA). It is therefore expected that the total number of reported data breaches will be higher this year than 2018. Two incidents related to child welfare services led to parliamentary questions in the first half of 2019 (*Bureau Jeugdzorg Utrecht* and *Stichting Kwaliteitszorg Jeugd*).[46]

The Netherlands has the highest number of reported data breaches compared to other European countries.[47] In the Netherlands, 15,400 data breaches were reported between 25 May 2018 and 28 January 2019. Germany and the United Kingdom are in second and third place, with 12,600 and 10,600 reports, respectively. A possible explanation for the higher number of reports could be that the reporting obligation had already been introduced in the Netherlands in 2016, which means that organisations here are more familiar with the obligation. In most other European countries, the reporting obligation was not introduced until the General Data Protection Regulation (GDPR) came into force, in May 2018.

[44] See, for example, this message by SIDN.
[45] See here for a definition of a data breach.
[46] In April 2019, it became known that 3278 files on 2702 children had been leaked due to an error at the youth welfare organisation *Bureau Jeugdzorg Utrecht* (article security.nl). At another youth registry organisation, *Stichting Kwaliteitsregister Jeugd*, a data breach also came to light; the test environment of a knowledge base was accidentally published online. As a result, non-anonymised decisions in the institute's disciplinary cases became publicly accessible. (article security.nl). Also see the Parliamentary documents II 2018/19, 31839, no. 686, on both incidents.
[47] Source: DLA Piper (2019). See here the link to the survey and here the related news message. International companies with offices in several countries file reports via their Head Office country. This can distort the ranking for countries such as the Netherlands and Ireland, where a number of multinationals have their headquarters.

Figure 2.5 Increase in the number of reported data leaks



Source: Dutch Data Protection Authority (DPA).

Almost two thirds of the reports filed in 2018 concern personal data sent to the wrong recipient. In its 2018 annual report, the Dutch DPA writes that 63% of the reported data breaches were due to personal data sent or delivered to the wrong recipient. In 4% of data breaches, the breach was the result of 'hacking, malware and/or phishing'. This percentage may seem small, but particularly digital data breaches involving personal information can affect large numbers of people. Leaked data can sometimes be used directly, for example if it concerns credit card information, or indirectly via phishing or identity fraud, if a password was leaked.

Protection of personal data can also go too far. Over the past year, the Dutch DPA imposed a penalty payment on the UWV[48], a fine on Uber[49] and a fine on the Haga Hospital in The Hague.[50] The fear of penalties and fines, possibly in combination with the desire to fully comply with the GDPR, seem to have led to greater caution at various organisations.[51] This development may unnecessarily increase the compliance costs for organisations or deter others from using new and socially desirable applications. This consideration could be included in the upcoming evaluation of the GDPR in 2020. Specific issues, in this respect, would be whether supervision and regulations are sufficiently in line with organisation sizes and whether the right balance has been struck between protecting personal data and facilitating socially desirable data applications.

[48] The Dutch DPA forced the UWV to pay a penalty of 150,000 euros per month, starting in November 2019, if they would not improve data protection. See the DPA Press Release and NOS news item. And another related news item on Dutch Business News Radio (BNR) about CVs being leaked from werk.nl.
[49] In November 2018, the Dutch DPA imposed a fine of EUR 600,000 on Uber for late reporting of a data breach involving 57 million Uber users (174,000 of them Dutch). See the news message by DPA and that by nu.nl.
[50] See this DPA news message and this article in the *Volkskrant* newspaper.
[51] In July 2019, for example, the Fraud Help Desk discontinued registering reports (of e.g. fake e-mails) by private citizens and entrepreneurs. See this blog by Arnoud Engelfriet, for more examples (link).

3 Cyber risks and public interests

3.1 Introduction

This chapter focuses on the risks in relation to public interest. Disruptions to cyber security, such as cybercrime and ICT failure, may have serious consequences for the companies and people affected. In many cases, however, the impact remains limited to those directly affected and any suppliers or customers involved, without much discomfort for society as a whole. The situation becomes different if the affected company is part of the critical infrastructure. Disruptions to critical processes, such as the power supply or electronic payment transactions, affect society as a whole. Digital resources may also be exploited by criminals in other, less immediately visible ways to undermine the public interest, such as by economic cyber espionage and spreading disinformation.

Section 3.2 discusses cyber risks in relation to critical infrastructure, in greater detail. Almost all critical processes and services depend on ICT, which means that cyber incidents may have serious consequences. In addition, critical processes are relatively vulnerable to cyber incidents; many systems are outdated and replacing them is a complex operation. In some cases, there are also concerns about the reliability of foreign suppliers. Cyber threats to critical processes evolve continually and are difficult to predict. However, it is clear that, as time goes by, society will only become more dependent on ICT, and that technological developments, such as 5G and Artificial Intelligence, will have to be closely monitored.

Section 3.3 analyses the risks related to economic cyber espionage. This digital espionage, which leads to the exploitation of company information, is considered a major threat to the Netherlands, as is emphasised by both the AIVD and NCTV. At the same time, there is a lack of public information to substantiate this claim, as only a handful of incidents are known and details about them are not available. Section 3.3 introduces a conceptual framework that indicates the steps that a spying criminal would need to take in order to profit from the use of stolen company information. This framework shows that economic cyber espionage is not automatically profitable and does not always cause damage to Dutch businesses.

Section 3.4 discusses the digital influence on public opinion. Disinformation can undermine the functioning of a democracy, and technological developments, such as Artificial Intelligence, increasingly simplify the generation and distribution of misleading messages. In recent years, online platform companies seem to have become more aware of their social responsibility and, partly through pressure from the European Commission and public outcries, have taken steps to combat disinformation. However, current self-regulation can mean that online platform companies, in certain circumstances, unjustly restrict people's freedom of expression. Co-regulation, in which the government draws up guidelines for such online platform companies on the basis of public debate, is a more promising policy option.

3.2 Critical processes

3.2.1 Critical processes increasingly dependent on ICT

Critical processes are services considered essential to society. Processes are identified by the NCTV as critical if their failure would lead to serious social disruption, such as accidents with many fatalities or serious injuries, billions of euros in damage, or to survival problems for large groups of people.[52] Examples of critical processes are the distribution of natural gas and electricity, the supply of drinking water, flood defences, the facilitation of internet and data services and payment transactions. Disruptions can cause a domino effect in a number of critical processes. The National Security Profile 2016 (National Security Analyst Network, 2016) states that these effects are mainly a risk in the energy and telecom sectors. If, for example, there is a prolonged power outage, electronic payment transactions, public transport and communication services may break down, depending on the availability of fallback options.

Almost all critical processes and services depend on ICT. This is stated by the NCTV in its 2019 CSBN report. The NCTV also emphasises that analogue fallback options often no longer exist. An example of this, although of a non-critical process, is that of container company Maersk, which was attacked by the ransomware NotPetya in 2018. As a result, its digital systems failed and the digitally controlled gate for trucks would not open. As it turned out, it was no longer possible to open this gate manually.[53] Another example is that of emergency generators in hospitals, which are intended to take over in case of power outage. However, far from all hospitals have the recommended amount of fuel available to cope with prolonged power outages of up to 72 hours. And, because fuel pumps run on electricity, it may be difficult to fill those fuel tanks during a power outage.[54]

Protecting critical processes is relatively complex. Digital systems that control critical processes often have evolved and grown organically and end up being very complex, which makes it more difficult to make a complete inventory of all the related risks. In addition, some systems are decades old and not equipped to deal with current cyber threats, but, over time, they were nevertheless connected to larger networks and sometimes even to the Internet.[55] Replacing or updating these obsolete systems is, however, extremely expensive. A study by the Netherlands Court of Audit concludes that digital security is not properly organised for a number of critical waterworks and that Rijkswaterstaat's ability to deal with a cyber attack could be improved.[56]

Over the past year, there have been various cyber incidents related to critical processes, both in and outside the Netherlands. The failure of the 112 emergency telephone number, in June 2019, shows that ICT-dependent critical processes can become disrupted.[57] In September 2018, two international ports, in Barcelona and San Diego, experienced a cyber attack.[58] There were also reports of a new group of hackers calling themselves GreyEnergy who carried out digital attacks on the energy sectors of Ukraine and Poland. These attacks, incidentally, did not result in system failure and were possibly conducted as a try-out in preparation of future cyber attacks.[59]

---

[52] This NCTV website provides a definition of critical processes.
[53] Based on the interview with Professor Bibi van den Berg in the Dutch newspaper, *Leids Dagblad*, titled 'Digital war at least as destructive' (in Dutch), 12 February 2019.
[54] See this news message by the NOS.
[55] More details are provided in NCTV (2019).
[56] See here the report by the Netherlands Court of Audit.
[57] Incidentally, the 112 service disruption did not seem to have been caused by a deliberate attack. See, for example, the reports by the NOS.
[58] See this news message.
[59] For more details, see this website.

Dependence on ICT and vulnerability to cyber attacks are expected to increase in the years to come. The NCSC regularly issues security advisories to warn companies in critical sectors of known vulnerabilities. A recent CPB study (2019) shows that the amount of advisories has increased in recent years. In addition, it is expected that the 5G network will lead to further digitalisation, as a result of which the number of ICT-dependent processes will continue to increase. Moreover, new applications may emerge that will eventually also become part of the critical infrastructure. The text box on '5G and ICT dependence' discusses this in more detail.

5G and ICT dependence

5G is a new core technology that will improve the current 4G network, in several areas. It builds on existing networks, but offers more capacity. Data transfer is faster and response times are shorter. In addition, more users and/or devices can use the network simultaneously.

5G is expected to lead to many new applications. Due to the short response times, 5G enables real-time interaction between, for example, machines or cars. This is an important building block in the development of autonomous vehicles. Applications in the medical world are also widely discussed. Examples, such as remote surgery, appeal to the imagination. Existing applications, currently still used on a limited scale, will probably be used more often if the network can operate thousands of devices in close proximity to each other. These include smart homes full of interconnected IoT devices and industry using a multitude of sensors.

A number of new applications may become essential to the functioning of society. As a result of 5G, society is expected to become more dependent on all types of digital processes than it is today. These digital processes may therefore also become part of the critical infrastructure. An example of such an area is that of road traffic. At the moment, this area is not regarded as a critical process. But once a large proportion of road traffic consists of autonomous vehicles that communicate with each other as well as with road sensors, smart traffic lights and traffic signs, system failures may have major consequences for road safety. In addition, the failure or disruption of medical applications could also potentially endanger people on a large scale.

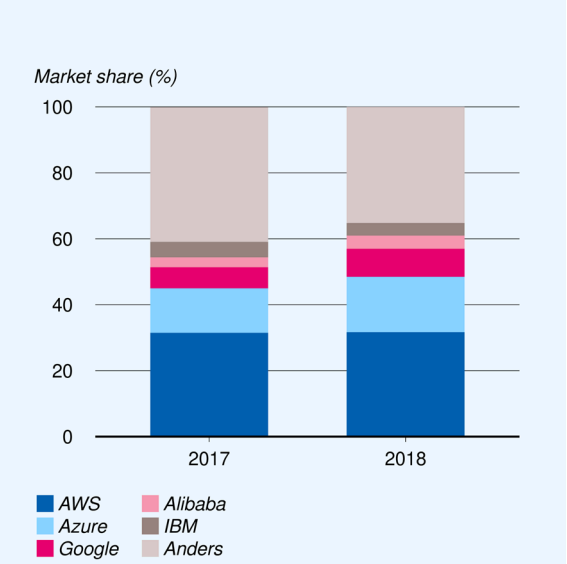
3.2.2 Dependence on one or more foreign suppliers

The Netherlands is highly dependent on foreign suppliers and has few fallback options. For some digital services, one or more providers have such a large market share that social cyber security is highly dependent on a handful of parties. Figure 3.1 illustrates this for cloud services. The five largest providers, together, have a global market share of around 60%, and this market share is growing. Because of their large market share, these providers probably have more opportunities to arm themselves against cyber attacks, but should things go wrong, a very large number of systems will be affected at the same time. Examples of such providers are DDoS mitigation services. Due to a recent software failure at DDoS mitigation service Cloudflare, part of the Internet temporarily shut down.[60] Some hardware and software markets are also highly concentrated and can therefore indirectly pose risks to social cyber security. However, these large providers can be attractive to

[60] See this news message.

individual customers because their size allows them to offer a better price–performance ratio. Large providers can generally invest more in innovation and security and, therefore, offer more attractive products. Data collection also plays a role, here. For example, large DDoS mitigation services have more information on DDoS attacks and can therefore offer better protection.

Figure 3.1 Half of the cloud market for the top 3 providers



Source: Canalys.

If a large supplier is based abroad, there may be concerns about its reliability. Several nations have a 'cyber offensive programme' aimed against the Netherlands (AIVD, 2019). The Russian cyber programme, in combination with legislation that requires Russian companies to support the intelligence services when asked to do so, has prompted the Dutch Government to phase out the use of Kaspersky antivirus software.[61] Concerns have recently emerged about the reliability of some foreign suppliers of 5G technology.[62] The storage of personal data abroad is also a sensitive issue.[63]

There are also concerns about the possible consequences of foreign parties taking over companies that are critical to the Netherlands. In September 2013, América Móvil attempted to acquire KPN, which raised the question of what impact this could have on national security. América Móvil's takeover attempt seemed to be motivated by commercial interests, but other foreign players could act for geopolitical or ideological reasons and exploit their access to Dutch communication networks. At the time of writing, there is a bill before the Dutch House of Representatives that gives the Minister of Economic Affairs and Climate the power to prohibit takeovers in the telecom sector if those pose a threat to the public interest.[64] In addition, there is concern about China's increasing role on the world stage. This relates to unfair trading practices, whereby Chinese companies operate abroad with the support of their government, while the Chinese market is shielded from foreign companies. Other concerns refer to developments in security and the realm of political influence. In its China strategy, the Dutch Government states that, among other things, it does not want to become dependent on China for certain key technologies.[65]

[61] For more information, see Parliamentary documents II 2017/18, 30821, no. 46.
[62] See Parliamentary documents II, 2019.
[63] This article elaborates on the consequences of the GDPR for data storage outside the EU.
[64] See this news message.
[65] Link to the Dutch Government's China strategy.

3.2.3 Cyber threats rife with uncertainty

The cyber threat to critical processes is constantly evolving and is difficult to predict. The greatest threat seems to emanate from nation-state actors. The NCTV (2019) states that carrying out cyber espionage or a cyber attack is not very risky. Hacking into electronic systems is not always immediately detected and the means of attack are easy to obtain at relatively low cost. Attributing them to nation-state actors, on the other hand, is very complex, and even when successful often remains without consequences. The threat posed by nation-state actors is closely linked to current geopolitical developments and is therefore difficult to predict.

The critical infrastructure has become interwoven with other processes that have not been identified as critical. The NCSC makes a 'binary' distinction between critical and non-critical processes. In practice, however, this distinction is not always very clear. Critical processes have increasingly become part of a network, which is why incidents involving a non-critical provider can also have an impact on a critical process. Focusing on the current list of critical processes carries the risk of important supporting processes being excluded. Examples of such supporting processes include suppliers of crucial software, digital systems for the supply of solar energy, hosting companies, and the providers of DDoS mitigation products or services who are protecting the Dutch banks. In addition, these support processes can be in the hands of private, sometimes foreign providers, some of whom are very large and powerful. Against this background, the Netherlands Scientific Council for Government Policy (WRR, 2019) argues in favour of an assessment of cyber dependence to provide insight into the parties, digital processes and services on which the functioning of critical processes depends.

Technological developments are changing the cybersecurity landscape and need to be closely monitored. One of the most important future developments will be the construction of a 5G network and its associated new applications. The security of the 5G network is currently surrounded by uncertainty and is being critically monitored by the government. Economic considerations also play a part, here. Excluding suppliers of 5G technology, or postponing the construction of the network until more information on its security can be obtained, could potentially lead to economic damage. When new applications take shape, such as autonomous vehicles and remote care, research is needed to determine whether these processes should be regarded as critical. Other developments, such as in the field of Artificial Intelligence (AI), can also lead to new security issues. If AI is to be used to control critical processes, criminals or nation-state actors could, for example, influence these systems by manipulating the training data. At the same time, AI could also be helpful in making critical processes more secure.

Various policy measures are aimed at increasing the resilience of critical infrastructure. The Dutch Network and Information Systems Security Act (Wbni), which came into force on 9 November 2018, obliges providers of essential services and digital service providers to take measures to secure their ICT systems and imposes a reporting obligation for serious incidents.[66] A remarkable aspect, in this respect, is that not all processes that are identified by the NCTV as critical fall under the security obligation.[67] The Wbni is an implementation of the EU NIS Directive, which excludes, among other things, nuclear energy and waterworks. For these processes, the Wbni only contains a reporting obligation, without obliging the providers to take any security measures. In addition to legislative developments, a large-scale cyber exercise is currently being organised, for the third time, with critical parties from the public and private sector (ISIDOR III).

[66] More information can be found on the NCTV website.
[67] However, companies may have security obligations under other legal regimes.

3.3 Economic cyber espionage

3.3.1 Introduction

Various organisations warn against economic cyber espionage conducted by nation-state actors. In its annual report AIVD (2018), the Dutch general intelligence and security service, writes that several countries, including China, Iran and Russia, are using digital means to achieve their own economic goals, to the detriment of Dutch interests and those of others. The NCTV (2019) also sees economic espionage as a current threat to the Netherlands, and identifies China as the main source of the threat. Economic cyber espionage is the illegal acquisition of knowledge and economically valuable information via digital channels.[68] Foreign intelligence services and other government bodies have access to various digital means to do this. Spies can use malware, place digital 'backdoors' in networks or try to gain access to confidential information via digital service providers, such as software suppliers or cloud services (AIVD, 2019). Manufacturers and service providers in various countries may also be required to cooperate with intelligence services.[69] Intelligence services can also use phishing or spear phishing to penetrate organisations.[70]

Organisations can also be spied on by competitors.[71] Nevertheless, there is an important difference between industrial espionage by competitors and economic espionage by nation-state actors. Such government bodies from countries with an offensive cyber programme have much more capacity and technical possibilities to engage in espionage. Also, attributing such espionage to a particular country is also more complex and there are fewer possibilities to recover damages. This suggests that economic espionage by nation-state actors poses a greater risk than industrial espionage.

Public information is lacking on the extent and impact of the threat. There are no reliable figures on how often Dutch companies are spied on, or on the related financial damage. Despite the great threat of economic cyber espionage, no Dutch companies have issued any profit warnings [72] after having been the victim of hacking. For example, former employees of AMSL did steal technological knowledge and used it to start their own business, but it is unknown whether these people acted on behalf of a government body.[73] More cases seem to be known in other countries. For example, the FBI has charged two Chinese citizens with hacking into more than 45 organisations and steeling sensitive data.[74] Internationally, too, data is currently lacking to quantify the financial losses to the companies affected.[75]

The information needed to properly understand the risk of economic cyber espionage is currently lacking. While the reported threat level of economic cyber espionage is high, only a limited number of incidents are known and information about demonstrable economic damage is lacking. This is a paradoxical situation. This section provides a framework to explain the paradox. The framework also helps to assess in which cases economic espionage would constitute a major risk and in which cases this would be less likely. The subject of economic cyber espionage fits in with the theme of economic security. Economic security is 'the undisturbed functioning of the Netherlands as an effective and efficient economy' (NCTV, 2019b).

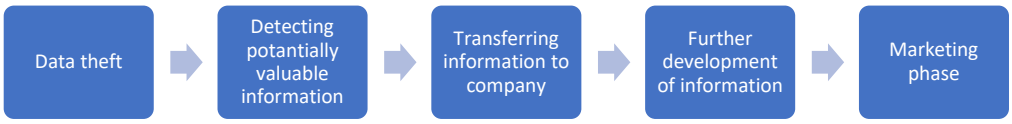
---

[68] This definition is in line with the AIVD's general definition of digital espionage ('the acquisition of sensitive or confidential information from another nation by digital means in order to achieve its own strategic goals').
[69] See, for example, AIVD, 'Cyber offensive programme. An ideal business model for nations' and the letter of 16 July 2019 from the Minister of Justice and Security 'Reaction Kaspersky Lab on the role of the government and IT industry in cyber security'.
[70] As suggested in this article.
[71] For example, the case of Waymo versus Uber (link).
[72] Listed companies are obliged under the Financial Supervision Act to disclose price-sensitive information as soon as possible by means of a press release.
[73] Source: FD (link).
[74] See this FBI news message: link.
[75] For example, see Anderson et al. (2019): 'While we do not dispute the occurrence of IP infringement, we failed to find any case with quantifiable losses'.

3.3.2 The phases in the chain of economic espionage

When is economic cyber espionage profitable for nation-state actors? News reports and research reports on economic cyber espionage often focus on the theft of corporate secrets and seem to assume that this automatically leads to damage for the companies in question and to profits for the perpetrating government body. However, the 'value chain' of economic cyber espionage consists of several phases and the theft of trade secrets is only the first phase. A spying country needs to go through these phases before the espionage can become profitable, see Figure 3.2.

Figure 3.2 The value chain of economic cyber espionage



Data theft: the first phase has become easier under increasing digitalisation. Companies are increasingly storing and sharing information digitally. Spying countries are responding to this by using exploits, access via backdoors into software or cleverly designed phishing e-mails. Insiders can also easily smuggle out digital information.[76] This phase in the value chain is characterised by economies of scale: with a relatively small number of employees, a country can try to spy on a large number of companies.

Detecting potentially valuable information: this is a labour-intensive and costly phase. When a hostile government body has succeeded in obtaining data through espionage, the next phase is to extract potentially valuable information from this data. This phase requires market knowledge and/or technological expertise and is therefore much less scalable than the first phase.

Transferring information to companies: the more intertwined the business community and governments are, the easier this phase will be. Information must end up in the right place in order to be valuable. This can be a difficult allocation issue for nation-state actors, because the organisation that is allowed to receive the information must be both politically reliable and able to utilise the information quickly. There may be an incentive to share the stolen information with large companies that have good political connections, but these are not necessarily the companies with the flexibility to develop new products. In this phase, there is the risk for nation-state actors that the knowledge is shared with large, cumbersome companies that are subsequently unable or unwilling to put the information to good use. The extent to which this phase is a bottleneck also depends on the national context — on the extent to which governments and companies are intertwined.

Further development of information: data or other information are rarely of immediate value. In order to ultimately lead to profitable products or process improvement, privileged companies will have to process the stolen information. This is similar to regular R&D and has largely the same uncertainties. A difference with a regular R&D process is that privileged companies have fewer opportunities for 'open innovation'; because they need to work with stolen information, it is more difficult for them to work with outside experts. For example, it is not wise to share stolen source code externally, and it may be difficult to attract new R&D staff – especially if they come from the company from which the information was stolen.

Marketing phase: depends on the speed of the value chain and protection of intellectual property. The final phase of the value chain involves the economic utilisation of the stolen information. This phase also differs little from a regular R&D and innovation process. The risks of exploitation, for example, are that these

[76] A possible example is the case of a Chinese employee of Apple (link).

companies, despite them having the stolen information, are later than the original owner to market their new products, or that the stolen knowledge is protected by a patent. In some cases, stolen information can be valuable in itself, without little additional costs, such as competitively sensitive takeover information or source code for software applications. Stolen information can also help a company to get closer to the technological forefront.

3.3.3 Conclusion

For the time being, the profitability of economic cyber espionage remains uncertain. The value chain of economic cyber espionage contains several bottlenecks and risks. This suggests that cyber espionage does not automatically lead to financial damage for the affected company. In certain situations, these bottlenecks are much less serious and the risk of damage is greater for Dutch companies. This is the case when stolen information hardly needs to be further developed and can be utilised relatively quickly. This could be the case, for example, in the event of theft of bidding strategies during a tender procedure, stolen contracts with buyers, or theft of source code. The risk of damage also appears to be greater if the transfer of knowledge between intelligence services and companies is easily accessible. Whether or not economic cyber espionage leads to financial damage, the risk of theft is likely to remain high due to the digitalisation of information and products.

3.4 Digital influence

3.4.1 Risks to a well-functioning democracy

Disinformation is about knowingly creating and disseminating false, inaccurate or misleading information.[77] Disinformation in itself is not a new phenomenon. However, digitalisation has changed the generation, distribution and consumption of information within our society, introducing new risks of disinformation. Nowadays, the Dutch population consumes news mostly through online channels.[78] Wardle and Derakhshan (2017) distinguish four dimensions in which digitalisation has changed the information value chain: 1) it has become easier to create and publish information, 2) information consumption takes place partly in public via social media, 3) news is spread faster through mobile communication and online publication, and 4) information is more actively shared between like-minded people who trust each other.

I**ndividual people, organisations or nation-state actors may have different reasons for using disinformation**.[79] Some parties use disinformation for financial gain. So-called clickbait websites, for example, can make a profit through advertisements by attracting consumers with sensational, but untrue, information. Furthermore, disinforming can have the objective of influencing or polarising public opinion. This may include attempts to manipulate elections with disinformation, but it can also involve influencing societal debate or behaviour, as in the case of disinformation about vaccinations.[80] Finally, disinformation may be fuelled by a need for entertainment, which often goes hand in hand with online bullying. This section is confined to disinformation that is aimed at manipulating public opinion. This form of disinformation has the potential to undermine the public interest in a well-functioning democracy.

Concerns about the impact of digital disinformation on public opinion have increased in recent years. For example, the European Commission regards the exposure of its citizens to disinformation as a major challenge.[81] Foreign powers have actively tried to influence elections and public perceptions in other

[77] See Van Keulen, Korthagen, Diederen and Van Boheemen (2018).
[78] Reuters Institute, Digital News Report 2019.
[79] For example, see the white paper by Google (2019).
[80] For example, see Welcome (2018).
[81] See the website of the European Commission.

countries. The best-known example is the recent United States Presidential Election. The use of Russian Internet trolls on Twitter after the shooting down of Malaysia Airlines Flight 17 (MH17), is an example of how disinformation was also used in the Netherlands to manipulate public opinion.[82]

Dutch citizens themselves are less concerned about the impact of disinformation, compared to those in other countries. A Reuters survey shows that 53% of Dutch people trust most of the news and only 31% are worried about what is true and false with regard to online news. By comparison, in France and the United States, 67% of people are worried about this (Reuters Institute, 2019). The relatively high score on media literacy on the index of the Open Society Institute (2018) suggests that Dutch society is more resilient to disinformation. However, the fact that the Dutch are relatively unconcerned may also pose a risk, if this trust turns out to be unfounded.

3.4.2 Digitalisation and market failure enable deception

Artificial intelligence increases risks by making it easier to produce credible disinformation.[83] Artificial intelligence (AI) facilitates simplification and more credible manipulation of sound and video images (also known as *deep fake* news). In addition, AI can be used for the automatic generation of false reporting. This makes the use of human Internet trolls superfluous and can lead to an increase in scale in the production of disinformation (Brundage et al., 2018). The dissemination of disinformation often takes place through the use of so-called bots on social media. A scientific study from 2017 estimates that between 9% and 15% of the accounts on Twitter consist of bots (Varol et al., 2017). It is expected that these bots will be used more intelligently in the future. For example, by targeting specific groups that are susceptible to disinformation. On the other side of the spectrum, AI can also be used to combat disinformation. For example, online platform companies use machine learning to enable more rapid recognition of counterfeit accounts and distribution via bots.

In 2017, CPB identified two market failures that could increase the dissemination of misleading information via online platforms. In the first place, such platforms possess more information than their users have at their disposal and are able to make use of this information asymmetry. This may lead, for example, to news being filtered through those platforms before it reaches consumers in order to make the platforms more attractive to consumers. In addition, platforms are perhaps experiencing too few incentives to counteract undesirable behaviour by their users, such as in the case of the spreading of disinformation through fake accounts.

The Dutch language and the organisation of the electoral system make it relatively unattractive for foreign actors to spread disinformation in the Netherlands. The limited knowledge of the Dutch language outside national borders means that disseminators of disinformation have to make relatively large investments in order to compile credible disinformation. In addition, the proceeds for malicious actors in elections are less high because the system of proportional representation ensures that each vote has an equal influence on the election results. In addition, the multiparty system in the Netherlands creates more variety in the public debate, which makes it more difficult for malicious actors to polarise and 'steer' citizens towards one particular party.

[82] See messages in the *Groene Amsterdammer* (here) and the *NRC Handelsblad* (here).
[83] For example, the Dutch Public Prosecutor's Office has recently expressed concerns to the NOS about the rise of deep fake videos, the digital quality of which is getting better and better.

3.4.3 Measures against disinformation are not yet future-proof

Online platform companies seem to have become more aware of their role in society. Partly because of pressure from the European Commission and public outcries, online platforms have taken steps in recent years to reduce the risks mentioned above. In September 2018, global market leaders (including Google, Facebook and Twitter) committed to an EU-wide code of conduct to prevent disinformation. These market parties are now reporting on a monthly basis on the measures they are taking to prevent the dissemination of disinformation. For example, the platforms provide access to political advertisements (see Facebook's Ad Library Report and Twitters Ads Transparency Center) and, in some cases, the geographical scope of political advertisements has been restricted.[84] In addition, large online platforms actively inform users about the origins of the advertisements and the degree of reliability of the reporting. This reduces the information asymmetry between user and platform. Finally, the distribution of incorrect messages is prevented by removing so-called bot accounts and including the degree of reliability of messages in ranking algorithms.

The current European approach to disinformation — self-regulation under administrative pressure — entails risks to freedom of expression and continuity of policy. Social media companies are considering what types of messages are allowed on their platforms. Whenever messages do not comply with their guidelines, they can be removed. The European Commission encourages online platform companies to do more to prevent disinformation. This has led to a tendency to place responsibility for the removal of misleading messages with the platforms. In Germany, this was even recently enshrined in law through the Netzwerkdurchsetzungsgesetz, which obliges online platforms to delete illegal hate speech within a certain period of time. Human Rights Watch warns that this law leads to unnecessary censorship and thus affects freedom of expression.[85] It is currently unclear to online platform companies what the consequences will be if public pressure is not complied with. Due to the current focus on self-regulation, there is a real risk of self-censorship on the part of platform companies, which can go beyond what is socially desirable.[86] In addition, there is a risk that self-regulation is primarily a reflex to the intensity of the public debate. Online platform companies will be inclined to take measures in times of commotion, which is why the sustainability of those measures is not guaranteed.[87]

Co-regulation is a more promising policy option. On the basis of public debate, governments can issue guidelines to online platform companies about how to deal with disinformation and other socially undesirable forms of influence. It is also desirable that these guidelines do justice to the diversity and dynamics of online platforms. An important question on which such a guideline can provide a definite answer is whether personalised political advertisements are acceptable. In addition, a starting point for directives must be that the market remains accessible to small new parties, so that the entry of new platform companies remains possible.

The importance of education aimed at media literacy is increased by the more extensive role of consumers in the news value chain. Social media ensure that consumers not only take in passive news, but also have a role in its dissemination. As a result, this role has increased. Training media-critical citizens can therefore reduce the impact of disinformation in two ways: the chance of disinformation going viral is reduced because citizens are less likely to share it, and misinformation is less likely to be able to influence people's own opinions. In Finland, media training has been part of the curriculum in primary and secondary schools for some time, and this seems effective.[88]

---

[84] For example, during the Irish referendum on abortion legislation, see reports here.
[85] See this message on the website of Human Rights Watch.
[86] For example, see Van Til (2019).
[87] For example, see Desmaris, Dubreuil and Loutrel (2019).
[88] For example see the messages by the World Economic Forum and CNN.

4 Prevention and mitigation

4.1 Introduction

Preventing and mitigating cyber security disruptions involves several aspects. NIST, the National Institute of Standards and Technology, summarises these aspects in five steps: identifying risks, protecting against these risks, detecting attacks, mitigating attacks and repairing damage.[89] These steps are generally applicable to businesses and citizens as well as to the government.

There is a large amount of attention for the first two steps, identification of cyber risks and protection against them. Awareness campaigns, such as Alert Online and platforms such as the Digital Trust Centre, try to raise risk awareness among citizens and businesses and encourage users to take precautions. The NCSC regularly provides security advice, government organisations are obliged to apply standards for secure data exchange, and technical protection methods are continuously being improved, to name but a few initiatives. Section 4.2 discusses a number of these subjects in more detail, with a special focus on the subjects for which statistical data are available.

Much less is known about the third and fourth steps of detecting and mitigating attacks. It is not impossible for attacks to go unnoticed for a long time or even never to be discovered. Some types of attacks, such as DDoS and ransomware, shut down systems and are therefore quickly detected. But, for example, systems that are hacked, cyber espionage or deployment of devices in a botnet are often only detected at a late stage, if at all. A report by cyber security company FireEye (2019) estimates that, in 2018, it took 78 days, on average, before companies would detect they had been hacked. According to Accenture research, 42% of cyber attacks on companies in the financial sector go unnoticed for at least a week.[90] And reports by RAND Europe & WODC (2015) and the WRR (2019) both conclude that cybersecurity focuses primarily on prevention and that detection and mitigation deserve more attention, precisely because complete prevention is impossible. Due to a lack of further information about detection and mitigation by companies and consumers, this is not discussed further in this report. Section 4.3, however, devotes attention to the investigation and prosecution of cybercriminals. These investigations and prosecutions by police and the Public Prosecution Service are not only mitigating the activities of these criminals, they can also have a deterring effect.

Little is also known about the fifth step of damage repair after a cyber attack. Insight into damage is available for a number of specific incidents, but estimates of the damage caused by cyber attacks in general, vary widely.[91] In recent years, however, there has been a growing focus on cyber insurance that covers the financial consequences of a cyber attack. At the moment, the market for this type of insurance is still very modest, but as the market matures, this may lead to better insights into the damage caused by a cyber attack. In addition, cyber insurance also affects the preventive measures taken by insured companies and the information collected by insurers may help to identify risks and detect and mitigate attacks. Section 4.4 analyses the market for cyber insurance.

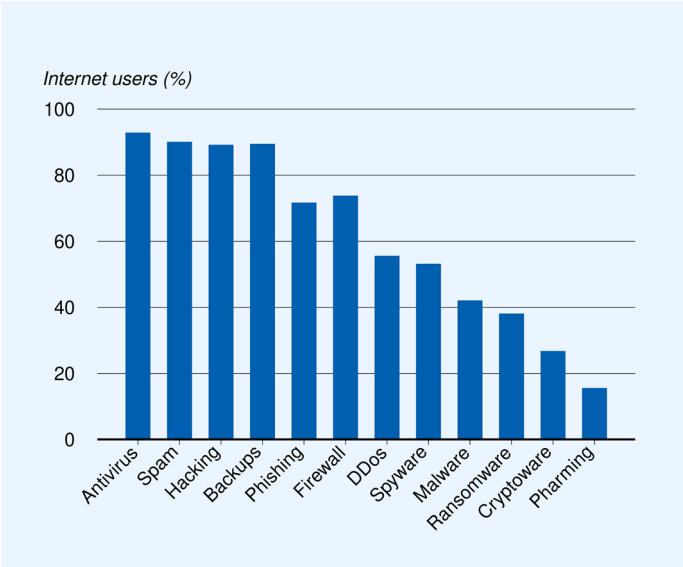
[89] See the NIST cybersecurity framework.
[90] See this message.
[91] For example, Hiscox (2019) reports an average loss of USD 369,000 per incident, while Radware (2018) estimates the average loss per incident at USD 1.1 million, and Accenture (2019) speaks of USD 13 million in losses, per organisation, per year.

The government sees knowledge sharing around these five steps as an important instrument to prevent and combat cybercrime. It therefore is strongly committed to providing information and to public-private partnerships. However, little is still known about the efficiency of this policy. The effects are often difficult to measure, making evaluation difficult. Section 4.5 discusses this in more detail.

4.2 Identification of and protection against cyber risks

Most internet users are aware of common online dangers, but the knowledge about new threats is only limited. Figure 4.1 shows a number of key figures from a CBS survey (CBS, 2018) in which internet users were asked about their knowledge. Many respondents knew what was approximately meant by an antivirus program, making backups, hacking and spam. However, knowledge about less common and/or newer forms of cybercrime was found to be limited. For example, only 27% said they knew what was meant by cryptoware (a form of ransomware) and 16% knew about pharming (the redirecting of internet traffic to a fake website). The same CBS survey shows many internet users as concerned about their online safety, especially in relation to the potential exploitation of their banking information or personal data.

Figure 4.1 Internet users often unfamiliar with new cyber risks



Source: CBS (2019)

In terms of security measures, not all Internet users are proactive, especially when it comes to less well-known measures. Approximately 45% of users regularly update their computer programs (e.g. operating system, virus scanner, internet browser), while 29% indicate that they only do so from time to time. Protecting access to devices with a password or fingerprint is common practice; 64% of Internet users do this often and 17% only sometimes. However, these percentages decline sharply when it comes to less known measures. For example, a password manager is rarely used (only 9% of respondents).

Corporate global spending on cybersecurity is increasing rapidly, with a particular focus on security-as-a-service. Estimates of global cybersecurity spending vary somewhat. Gartner assumes a market the size of USD 114 billion for 2018, with an annual 8.7% increase in spending.[92] IDC estimates the 2018 market at USD 92

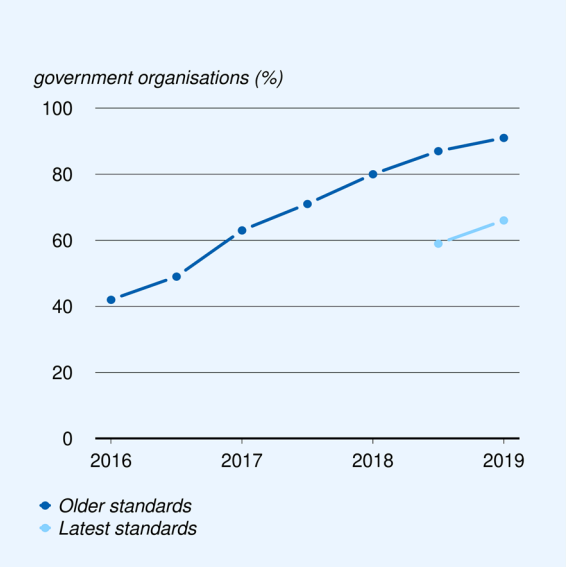
[92] See this news message by Gartner.

billion, with an average annual growth rate of 9.9% up to 2022.[93] Both Gartner and IDC mention security-as-a-service, where some of the security is outsourced, as the largest and strongest growing category of expenditure. No reliable estimates on cybersecurity expenditure are available for the Netherlands. However, a CBS survey from 2018 shows that 44% of surveyed companies have their ICT security carried out mainly by external suppliers. This percentage increases to 69% for companies with 20 to 50 employees, and is lower for very small or very large companies.[94]

As with consumers, not all companies take precautions and more sophisticated measures are mainly taken by large companies. The CBS survey shows that 87% of all companies surveyed use antivirus software, while 68% store a backup in another physical location or in the cloud. These basic measures are also taken regularly by small businesses. More far-reaching measures, such as encryption when storing and sending data, are mainly taken at large companies.

Technical standards for secure online traffic continue to evolve. In April 2019, the NCSC published an updated TLS guideline to secure connections on the Internet.[95] TLS encrypts the data sent between the user and the website; when a website is secured with TLS, 'https' appears in front of the address and a lock pictogram is shown. Outdated DNS applications are also phased out.[96] Outdated DNS protocols can be exploited to redirect internet users to a fraudulent website.

Figure 4.2 Steady adoption of standards within the government domain



Source: Forum Standaardisatie.

The use of technical standards is growing, but is not yet 100%. *Forum Standaardisatie* regularly measures the extent to which government websites and e-mail programs are secure.[97] Older standards for website security (DNSSEC and TLS/HTPPS) and for combating e-mail phishing (DKIM, DMARC and SPF) are widely used by government organisations. The top line in Figure 4.2 shows the adoption rate of these older standards. At the beginning of 2019, this was around 90%, under a steady growth since mid 2015, when the adoption rate was 35%. Newer standards, such as DANE for encryption of e-mail traffic and SPF and DMARC with strict

[93] See this message.
[94] These data can be found at CBS Statline, under ICT use among companies.
[95] See this message by NCSC.
[96] See this news message by SIDN.
[97] See this report by *Forum Standaardisatie*.

application, are used less frequently. The application of these standards is growing, from 59% in mid 2018 to 66% by the beginning of 2019. The adoption rate of standards among all .nl domain names is much lower. In July 2019, for example, 54% of these domain names were secured with DNSSEC.[98]

Authentication shows a shift towards more sophisticated methods that increasingly use physical keys or biometric data. Authentication is the process by which a person or a machine can confirm someone's identity. Well-known authentication methods are the use of a password, or a form of two-factor authentication in which the user, for example, has to enter both a password and an SMS code. Cybercriminals are becoming increasingly adept at bypassing these methods.[99] For this reason, there is a shift towards alternative methods of authentication. Instead of unencrypted SMS authentication, companies are increasingly using apps that send data in encrypted form. In addition, some companies use a physical key.[100] Biometrics is also gaining in popularity. One of the most well-known applications of biometrics is the fingerprint scanner, which has been on the rise for a number of years. By 2018, 60% of the smartphones shipped worldwide were equipped with a fingerprint scanner.[101] Developments in artificial intelligence also enable other forms of authentication based on biometric data, such as voice or facial recognition, a technique that is already offered in the latest generation of smartphones.

The continuous development of new prevention and mitigation methods helps to combat cybercrime, but there is a risk that users will not be able to keep up. New techniques to protect internet users, such as improved standards for secure online data traffic and safer authentication methods, contribute to the fight against cybercrime. However, many of the developments described above show that the adoption of new technologies is lagging behind. The latest technical standards are still far from being applied to all websites, consumers are limiting themselves to basic security, and even here the adoption rate is not 100%. More advanced techniques are also used less frequently in the business world.

It is unclear what level of investment in cybersecurity would be sufficient. The link between investments in security and incidents or operating results is complicated, because cause and effect are intertwined. On the one hand, investments in cyber security can be expected to reduce the likelihood of an incident, although the added value of additional investments is likely to decrease after a certain point. At the same time, companies with a higher risk of an incident, such as large companies or companies that are highly dependent on ICT, will take more measures. Also, companies that take a large number of measures are likely to be more aware of the cyber threat, which means that they will detect and report an incident more quickly.

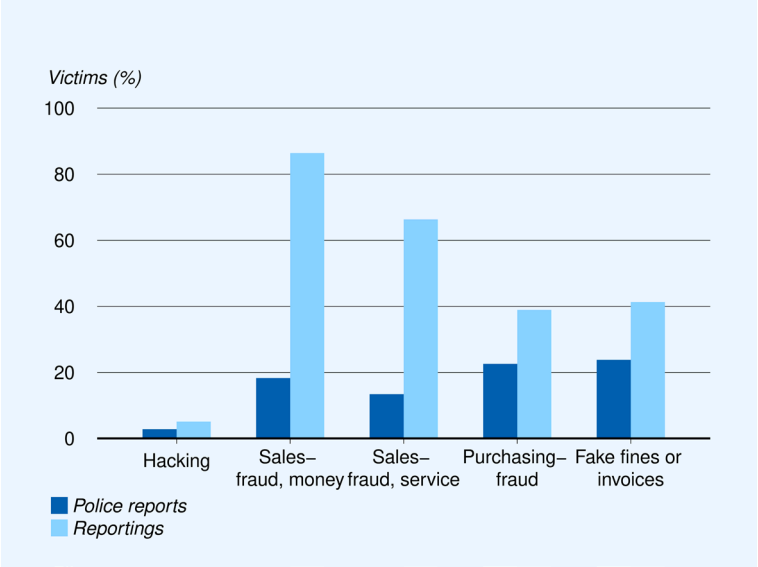
The usefulness of a financial benchmark for investments in cyber security is very limited. Several studies provide a benchmark for the optimal investment in cybersecurity to be made by companies. These benchmarks vary widely, between 3.7% and 10% of the total ICT budget.[102] However, a WODC report (RAND Europe and WODC, 2015) indicates that, based on interviews with experts, it is very difficult to determine how much a company spends on cybersecurity, partly because these costs are often an integral part of ICT projects. This makes it difficult to establish and use a benchmark. In addition, it is not so much the expenditures in a quantitative sense that offer protection, but the measures in a qualitative sense. A financial benchmark is therefore of little use.

[98] See this graph by SIDN.
[99] Among other things, Fox-IT states that SMS authentication is not completely without error.
[100] Google is an example of this.
[101] See these statistics.
[102] This overview article further elaborates this point.

4.3 Investigation and prosecution of cybercriminals

Over the past year, the police have had several successes in taking criminal websites offline. At the end of December 2018, it was announced that the FBI, together with the Dutch police and others, had taken 15 DDoS-as-a-service-websites offline.[103] In collaboration with European partners, the police also took over Wall Street Market, a large marketplace on the dark web, where, among other things, ransomware was traded.[104] It is not yet clear whether these actions will have a lasting effect. Digital security will continue to be a key issue for the Ministry of Justice and Security in 2019.[105] With the Computer Crime Act III, which came into force on 1 March 2019, the police have been given new powers to combat computer crime.[106]

Figure 4.3 The willingness to report is high for financial crime and low for hacking



Source: CBS (2019).

Despite the successes in tackling cross-border cybercrime, the willingness of victims to report it remains low. A recent CBS survey (CBS, 2018) asked victims of digital crime in 2018 whether they had filed a report. Figure 4.3 shows the results for a number of categories of cybercrime. It is striking that fraud via the payment system, where money was withdrawn from the account, was found to be reported often, particularly to the bank or financial institution. This is probably necessary in order to obtain compensation for the financial loss. Other forms of fraud were reported less frequently. The indicated important reasons for not reporting fraud included that it involved only a small amount of money, or that the victim believed that reporting would not help them get compensation nor to catch the perpetrator. Hacking is reported only very sparsely. Reasons given by victims for this included that reporting was not possible, or too much trouble, or that the perpetrator would not be caught anyway. The willingness to file a police report was found to be low in all forms of cybercrime. In addition to the reasons mentioned above, victims also relatively often mentioned that the bank or financial institution would deal with it further. For statistical reasons, the results from this CBS survey cannot be compared directly with previous surveys. Nevertheless, they are reasonably in line with the Netherlands' Safety Monitor 2017, which showed that 3.7% of the victims of hacking and 19.8% of the victims

[103] See, for example, this news message.
[104] See here.
[105] See this news message.
[106] This message further elaborates the new police authorities.

of purchasing and sales fraud had reported those crimes.[107] This suggests that the willingness to file a report with the police has remained fairly constant over time.

Reporting of cybercrimes leads to prosecution and conviction in only a small number of cases. Not all cybercrimes are registered separately. Online fraud, for example, is registered together with non-digital forms of fraud under the category 'fraud'. Only computer hacking, i.e. breaking into a computer system, forms a separate category. The data in Table 4.1 show that, both in 2017 and in previous years, only a very small proportion of the registered cases of computer hacking result in criminal prosecution and that an even smaller proportion will ultimately result in conviction. In the case of fraud, for which only the total number of cases of online fraud and non-digital fraud are known, the proportion of prosecutions and convictions is comparable. Notable fact is that, relatively speaking, physical theft, embezzlement and burglary are much more likely to be prosecuted followed by a conviction — likely because, in those cases, concrete evidence or witness statements are more often available.

A higher percentage of cybercrime prosecutions and convictions may encourage victims to report it. The perception that filing a police report 'won't help, anyway' may change, if the proportion of prosecutions and convictions were to increase. In this context, it is a good idea for successes, such as the arrest of fraudsters on *Marktplaats*, to be shared as much as possible on social media and receive attention in the press. The police are trying to encourage victims to file a report, by facilitating online reporting.[108]

Table 4.1 Overview of cybercrimes versus non-cyber crimes, from a historical perspective and in 2017

Crime	Hacking		Fraud (total)	Theft/Embezzlement and Burglary
Period	2008–2017	2017	2017	2017
Registered crimes	19,680	2,300	39,760	428,280
Registered with the Public Prosecution Service (OM)	715	90	1,925	47,965
Settlement with the Public Prosecution Service (OM)	140	5	95	2,460
Sentence by the Public Prosecution Service (OM)	30	0	145	6,600
Dismissal by the Public Prosecution Service (OM)	95	15	200	2,185
Court Procedure	165	10	820	29,215
Guilty verdict	125	10	670	26,780
Acquittal	35	0	140	2,320

Source: CBS, WODC and the Council of the Judiciary (2017).

[107] Source: CBS Statline.
[108] For example, see this news message.

4.4 Cyber insurance

4.4.1 Dutch market for cyber insurance is small but growing

Cyber insurance covers the financial damage caused by a cyber incident. Most types of cyber insurance are aimed at companies.[109] The first entrants to the market were large international insurers, who mainly focused on large companies. There are now also several Dutch providers that focus more on SMEs.[110] The term cyber incident covers attacks from outside, such as hacking in which company data are harvested, and internal incidents, such as a data breaches caused by a lost laptop. The degree of cover varies per insurance, but roughly includes the costs related to business interruption, crisis management, repair and liability.

The Dutch market for cyber insurance is growing rapidly, but is still modest compared to other types of insurance. According to a survey by the Dutch Association of Insurers, the maximum premium income in 2015 was EUR 10 million, and in 2017 it was at least EUR 20 million.[111] This increase was due to both the entry of new providers and the increase in the number of existing providers. In relative terms, however, this premium income is still modest. In 2017, the premium income for corporate liability insurance was EUR 800 million and for corporate non-life insurance it was EUR 1.4 billion.[112]

Worldwide, the market is most developed in the United States. The total premium income for cyber insurance worldwide was estimated at between USD 2.5 and 3.5 billion in 2016.[113] Between 85% and 90% of this market was in the United States and 5% to 9% in Europe. One year later, in 2017, premium income in the United States was estimated at around USD 3 billion (EU-US Insurance Dialogue Project, 2018). To put this into perspective, this premium income is a factor of 150 higher than in the Netherlands, while the US economy is over 23 times larger than that of the Netherlands.[114] Therefore, if also adjusted for the size of the economy, the US market for cyber insurance is clearly larger. Some of this is likely to be due to the fact that the United States has a stronger insurance culture.[115] In addition, the United States already had an obligation to report data breaches before Europe, which may have stimulated the market (RAND Europe and WODC, 2015).

4.4.2 Many uncertainties remain in the cyber insurance market

Insurers find it difficult to estimate the risks and to formulate a cover with a realistic risk premium to match. There is only a small amount of hard data available on how often cyber attacks occur and what the direct and indirect financial consequences may be.[116] Cyber risks are also dynamic, with threats constantly evolving. This makes it difficult for insurers to determine a specific cover with a realistic price to match. This is reflected in the current insurance on offer. There is a considerable variation in terms and conditions and damage covered, and the wording is not always clear from a legal point of view. This lack of clarity is exacerbated by a lack of jurisprudence. An illustration of this is a major lawsuit currently under way in the United States. Food producer Mondelez suffered millions of dollars in damage from the NotPetya ransomware

[109] Cyber insurance for private citizens is more or less unavailable in the Netherlands. One reason for this may be that the damage experienced by citizens in the event of a cyber incident is often limited in financial terms, and is often already covered by other insurances. At the same time, there is increasing attention for the possible consequences of identity fraud. This could lead to the creation of a private insurance market, in the future.
[110] For example, the insurance policies of *Centraal Beheer* and the *Goudse* are explicitly intended for SMEs with a maximum turnover of 10 million euros.
[111] See this press release.
[112] Based on these data from the Centre of Insurance Statistics.
[113] See OECD (2017) p. 60.
[114] See for example, these data from CBS.
[115] The market for corporate liability insurance, adjusted for GDP, is clearly larger in the United States than it is in Europe. For example, see Swiss Re Group (2014).
[116] EIOPA (2018), among others, further elaborates on this.

and is trying to recover this amount from its cyber insurance. However, insurer Zurich refuses to pay out on the grounds that NotPetya is an act of war, something that is excluded from the insurance policy.[117]

It is difficult for potential customers to determine whether taking out cyber insurance would be wise. Many companies have difficulty estimating the cyber risks they run and the possible consequences of a cyber incident. In addition, the aforementioned lack of clarity about the coverage of cyber insurance can be a barrier for potential customers.[118] It is also not always clear to what extent other business insurances, such as business interruption insurance or legal assistance insurance, already cover part of the consequences of a cyber attack. These insurances often do not explicitly exclude cyber incidents from their coverage.

Some cyber attacks can quickly claim many victims and are therefore complex to insure. The basic principle behind indemnity insurance, such as fire and vehicle insurance, is that the risks are not or hardly correlated. Damage for one policyholder does not affect the risk of damage to another. As a result, the average cost of claims, across all insured parties, is manageable. In the case of damage caused by natural phenomena, such as storms or hail, many people are affected at the same time, but the damage is usually limited to a certain country or region. Reinsurance through an international party allows this risk to be spread to a limited extent. This is more complicated in the case of cyber threats. Ransomware, for example, may cause many casualties more rapidly and worldwide. Experts do not agree on the extent to which such extreme events can be insured. Some see it as an unsolvable problem, because, at first sight, reinsurance and risk diversification, for example across industries or geographical regions, do not offer a solution. Others think there is a way out of this problem and draw an analogy with terrorism insurance. In the case of terrorism, the potential burden of claims is also extremely high and in a number of countries the government therefore acts as a backstop should insurance companies run into problems as a result.[119]

There is no consensus yet as to how moral hazard can be reduced with cyber insurance. In general, non-cyber insurance limits the incentive to invest in preventive measures and can lead to reckless behaviour. In the economic literature, this phenomenon is known as 'moral hazard'. Non-cyber insurance overcomes this by imposing conditions on the policyholder and not paying out when there is evidence of recklessness. When taking out a building insurance policy, the policyholder can, for example, demand that sufficient smoke detectors and fire extinguishers are present, and if a motorist deliberately drives recklessly and causes an accident as a result, the insurer can refuse to pay out. In the case of cyber insurance, this is currently even less developed. It is not always easy to determine the appropriate precautions in the area of cyber security, and preventive measures also require regular maintenance. There is also no case law yet on what 'recklessness' means in the context of cyber security. In today's market, there are therefore major differences between insurance companies. There are insurance packages on the market that combine a cybersecurity subscription from a specific security company with an insurance policy for the residual risk. Other insurance companies recommend a certain brand of security software and offer a cybersecurity subscription at a discount, without making this insurance compulsory. Other insurers leave cybersecurity entirely up to the insured company and merely require an up-to-date virus scanner, firewall and external backup.

4.4.3 Cyber insurance may contribute to cyber resilience

A well-developed market for cyber insurance helps to gain insight into the cyber threat. A good overview of the consequences of cyber incidents is currently lacking. Combined data from insurers and other parties involved may provide a great deal of insight into the frequency of incidents, the types of companies involved,

[117] For example, see this article in the New York Times.
[118] Chapter 4 of OECD (2018) further elaborates on this.
[119] Both EIOPA (2018) and OECD (2018) discuss the problem of correlated risk in more detail.

the attack methods used most often and the consequences.[120] In the United States, where the market for cyber insurance is more developed, these data are already being collected and reported, albeit on a limited scale.[121] These data are not only useful for insurers to make risk assessments and determine premium levels, but are also of wider value. For example, they can raise awareness of the risks and help cyber security specialists focus on the largest threats.

Setting basic conditions for the policyholder to comply with, contributes to cyber resilience, provided that this does not absolve the policyholder of all responsibility. Virtually all providers of cyber insurance place certain conditions on the cybersecurity of the companies insured, which increases general cyber resilience within the business community. However, cyber insurance that completely absolves policyholders of their responsibilities with respect to cyber security carries the risk that policyholders no longer feel accountable for any security errors. A packaged solution is particularly attractive for SMEs, as they no longer need to study the quality of the various cyber security companies and can be assured of complying with the conditions of the insurance company. However, this carries the risk that these SMEs have no insight into what the cyber security company does or does not do and they are entirely dependent on the insurer's assessment of the quality of the cyber security company. If, despite this, there is a data breach with reporting obligation under the GDPR, it is very doubtful whether the responsibility for having applied the appropriate data protection measures can be transposed onto the insurance company. In addition, it is legally unclear to what extent GDPR fines are insurable.[122] In this respect, cyber insurances can give a false sense of security.

4.4.4 Government policy useful for moving the market into the desired direction

Cyber security standards can help further develop cyber insurance. At the moment, insurance companies differ considerably in the conditions they impose on policyholders. This makes it difficult for potential customers to make a choice and can make it particularly attractive for less cybersecurity-aware companies to choose a package that takes the security off their hands. A certification for cyber security companies combined with a risk model for entrepreneurs will help standardise the insurance offering while leaving the policyholder responsible for security. Entrepreneurs can use the risk model to determine the current level of cybersecurity and insurance companies can demand a cybersecurity solution with mandatory quality certificate, without explicitly recommending a particular cyber security company. There are already a number of initiatives in this area. The ISO27k series provides an international standard for information security and, among other things, develops guidelines for cyber insurance. However, the international insurance sector has expressed a critical opinion on this development, partly because it has not been consulted and there are no ISO guidelines for other insurance products.[123] The European Cyber Security Act provides a framework for the certification of ICT products, services and processes in a broad sense. In addition, the Centre for Crime Prevention and Security is working together with the business community and the government on a risk model and a cyber security certificate.[124]

More clarity about the method by which the amounts in GDPR fines are determined and their insurability helps companies to make a proper assessment of the usefulness of having cyber insurance. Violation of the GDPR is one of the most visible possible consequences of a cyber incident. There seems to be both anxiety and a lack of clarity about this among SMEs. The maximum fines are very high and because, so far, few fines have been handed out, it is difficult to predict how the Dutch Data Protection Authority (DPA)

[120] At the moment, cyberinsurance companies in the Netherlands hardly exchange any data. This seems to be related to the fact that the market is still small, the number of claims is very limited and the data are therefore sensitive to competition. The Centre for Insurance Statistics, part of the Dutch Association of Insurers, reports and analyses data from large insurance markets, such as car insurance.
[121] See Insurance Industry Cybercrime Task Force (2010) and NetDiligence (2018).
[122] This article by Aon further elaborates on the insurability of GDPR fines.
[123] For example, see this letter by the Global Federation of Insurance Associations (GFIA) to ISO.
[124] See this message.

will deal with specific circumstances.[125] For some companies, coverage of GDPR fines is therefore an important reason to consider cyber insurance.[126] At the same time, it is legally unclear to what extent insurance against GDPR fines is allowed. And if this were allowed, it would be undesirable if companies were able to take out insurance that would cover the consequences of non-compliance with the GDPR. In view of these uncertainties, more information is needed about the sizes of the GDPR fines and whether insurability of such fines would be desirable.

Because cyber risks are correlated and partly unknown, more attention from regulators may be required. At present, the size of the market for cyber insurance is still limited, which means that a wrong risk assessment will have little impact on the entire financial system. However, as the market grows, the uncertainties surrounding cyber risks may play a role in the financial stability of insurers. At which time, it would be important for DNB to monitor the risk profile of cyber insurance companies and to gain insight into the correlation between cyber risks. It may be useful to take action on a European level. Various cyber insurances are offered by internationally operating insurers. There is also more data available on cyber risks, at European level, which can help with a timely and adequate risk assessment. The EIOPA, the European regulator of insurance companies, has recently proposed to include cyber insurance as a separate category in the reports that companies must submit to the national regulator under Solvency II.[127]

4.5 Information and collaboration within the cyber domain

4.5.1 Diverse mix of information and collaboration

Government policy focuses on information provision and public–private partnerships to prevent and combat cybercrime. This is evident from the Dutch Cyber Security Agenda (Dutch Government, 2018), which mentions public–private partnerships as an important route to guarantee security in the digital domain: 'this can only happen in collaboration with and partly also by the business community'. In addition, 'the public and private sharing of available knowledge and promoting the sharing of information are necessary to strengthen cyber security across the board' (p. 7). In practice, various initiatives are shaping this aim. The Cyber Security Alliance (CSA) and the Digital Trust Centre (DTC) were set up to promote such collaborations. There are also several information websites, such as the information provided by the DTC, which focuses primarily on SMEs, and the websites of Alert Online and Secure Internet (*Veilig Internetten*).

Measured in numbers of initiatives, the commitment to public–private partnerships seems to be bearing fruit. According to a survey by the CSA, 38 different partnerships are currently active in the Netherlands. Table 4.2 shows a number of initiatives by way of illustration and, together with the CSA overview, a picture emerges of collaborations between organisations on various levels and with various objectives. Some of which are focused on a single sector and/or a single goal, while others cover the entire cyber security domain and do not seem to distinguish between types of organisations. In addition to these initiatives, many organisations work together in Information Sharing and Analysis Centres (ISACs) or via a joint Computer Emergency Response Team (CERT).

Little is known about the effectiveness of the various initiatives around collaborations and the provision of information. It is difficult to measure the effects of such collaborations. As Table 4.2 shows, collaborations regularly pursue multiple goals, which makes it unclear which aspects of a project should be assessed. The goals are often formulated qualitatively — for example, 'sharing relevant knowledge' — which means that a

[125] In March 2019, the DPA did publish new policy regulations for fines.
[126] This is also indicated by EIOPA (2018).
[127] The EIOPA proposal.

suitable quantitative measure is lacking. Moreover, organisations that seek voluntary cooperation probably differ from those that do not, with respect to certain important elements, such as awareness. Comparisons between participants and non-participants, therefore, do not provide any insight into the *effect* of collaboration. The same applies to measuring the effect of information campaigns. The numbers of visitors to an information website are often monitored, but the extent to which the information has led to lasting behavioural changes is usually unknown. Alert Online's annually conducted National Cyber Security Awareness Survey provides some insight into cyber security awareness over time, but does not link the results to information campaigns.

Table 4.2 Large amount of diversity in types of collaboration

Name	Level	Identification	Prevention	Detection	Response	Restoration
Cyberweerbaarheid Brainport Eindhoven	Regional	x	x	x	x	x
Connect2Trust	Cross-sectoral	x	x	x	x	x
Secure Software Alliance	Cross-sectoral		x	x		
Cyberweerbaarheid Noord Nederland	Regional		x		x	
TIBER (financial sector)	Sectoral				x	
Veilige E-Mail Coalitie	Cross-sectoral		x			
Dutch Continuity Board	Cross-sectoral		x	x	x	
FERM (Port of Rotterdam)	Regional	x	x	x	x	x

NB The table lists various collaboration initiatives according to the five components of the NIST model for cyber security (link). The examples were obtained from the Cyber Security Alliance (link).

4.5.2 Reasons for government intervention

Some collaborations and information campaigns serve a public purpose and would be difficult or impossible to set up without government intervention. In critical processes, for example, there is a public interest in ensuring that information about threats is exchanged quickly and that organisations respond to an attack as rapidly as possible. To facilitate this, the government encourages ISACs for companies that are part of the critical infrastructure and critical organisations are encouraged to practice dealing with incidents. Government intervention may also be necessary in the fight against cybercrime. In a project such as *No More Ransom*, for example, the government supports a platform that provides free recovery software to counter ransomware, as a result of which its dissemination becomes financially less attractive.[128] Increasing the general awareness of cyber risks can also be seen as a public interest. Finally, government intervention may solve a coordination problem. An example of this is the application of standards for secure e-mail. These standards are effective if they are used throughout the entire chain of senders and recipients. The government therefore participates in the Standardisation Forum and the Secure Email Coalition.

It is important to always consider whether government intervention would be justified. Is there a public interest to be served or can the initiative also be left to the market? In some collaborations, the rationale for government support is unclear, but there may be a private reason for collaboration. Organisations within a supply chain, for example, may be dependent on each other and therefore enter into collaboration to prevent

[128] Link to the No More Ransom website.

a cyber attack on either one of them, as financial damage to one also would lead to financial damage to the other. The reasons for government intervention in such a case would be unclear if the supply chain does not produce a critical process and there are no domino effects that can lead to social disruption. Another example of an initiative that might also be possible without government support is that of collaboration around a cyber security training course, in which students can gain practical experience at companies in the region. The provision of information could also partly be left to the market, since insurance companies or cyber security companies are commercially motivated to point out the cyber risks to the business community.

It is also important to determine what instrument would be best suited to achieve a particular objective. The current emphasis on public–private collaboration in policy carries the risk of people losing sight of any alternative means and collaboration becoming an end in itself. Collaboration, for example in the form of sharing experiences, sharing data on attacks or jointly testing cyber resilience, can be a useful way for organisations to become digitally more secure. However, setting up and subsidising collaborations is not always the best way for the government to achieve a particular goal. Legislation, such as security or transparency obligations, can also contribute to cyber security.

4.5.3 Risks of a local approach

The multitude of initiatives in collaboration and the provision of information can lead to inefficiencies or inconsistencies. There are several subsidy schemes and, sometimes, collaborations overlap, which can be confusing to companies in where to go and who to join. There is also overlap between target groups and the content of the various information websites. This overlap can lead to inefficiencies, such as duplications, or to important issues remaining unaddressed. In addition to inefficiencies, overlap may also lead to inconsistencies, with some target groups unjustifiably being treated differently from others. For example, the NCSC is the first point of contact for companies in critical sectors. Non-critical companies fall under the DTC. However, this second group is extremely large and very diverse, ranging from small independent companies to large companies. This group probably includes companies that are important within the network around the critical sectors. In cases of failure or disruption, the domino effect may also cause them to have a disrupting impact on critical processes. In the event of an incident, these companies cannot formally call on the assistance of the NCSC. They may also miss important information provided by ISACs to critical organisations. In the long term, the DTC would like relevant information that is distributed by the NCSC to also be accessible to the DTC target group. In the meantime, the DTC is focusing primarily on companies that are still at the start of secure digital entrepreneurship. Incidentally, the risk of inefficiency is also identified in the Dutch Cyber Security Agenda: ‘the effects of the various efforts can be improved by making communication campaigns in the public domain more coherent’. (p. 40)

Greater evaluation commitments are needed in order to improve policy-making. Regular assessments are required to determine whether the various initiatives are effective. This is particularly relevant when public funds are used to finance collaborations or information campaigns. Although purely measuring the effects will often not be possible, results from pen tests (digital branding exercises) or interviews with participants in collaborations can be used as an indication of the effectiveness. The current number of initiatives can also be used as an experimental setting to determine what works well and what does not. However, this requires initiatives that are consciously designed to be easily compared. At the moment, the first steps are being taken to measure the effects in collaboration with Statistics Netherlands (CBS).

Lessons learned in neighbouring countries may provide starting points for the Netherlands, for further policy development. Various countries are adopting a variety of approaches to conduct information campaigns and to encourage collaborations. An interesting case in point is that of the United Kingdom, where the National Cyber Security Centre is the central point of contact and information for citizens, small and large companies and government organisations. This approach differs from that in the Netherlands, which focuses

on different target groups in different initiatives. The positive and negative experiences with the working method in the United Kingdom may be helpful in further shaping Dutch policy.