National Coordinator for Security and Counterterrorism
Ministry of Security and Justice

Cyber Security Assessment Netherlands 2017

National Coordinator for Security and Counterterrorism

The National Coordinator for Security and Counterterrorism (NCTV) protects the Netherlands against threats that may disrupt society. Together with its partners within the government, the science community and the business sector, the NCTV ensures that the Dutch critical infrastructure is safe and remains so.

National Cyber Security Centre

The National Cyber Security Centre (NCSC), in collaboration with the business community, government bodies and academics, is working to increase the ability of Dutch society to defend itself in the digital domain.

The NCSC supports the central government and organisations with a vital function in society by providing them with expertise and advice, threat response and with actions to strengthen crisis management. In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention. The NCSC thus constitutes the central reporting and information point for IT threats and security incidents.

The NCSC is part of the Cyber Security Department of the National Coordinator for Security and Counterterrorism.

Collaboration and sources

In drawing up this report, the NCSC gratefully used information provided by the following parties:

- The various ministries
- Dutch embassies
- Military Intelligence and Security Service (MIVD)
- Defence Computer Emergency Response Team (DefCERT)
- General Intelligence and Security Service (AIVD)
- Dutch National Police (National High Tech Crime Unit)
- Public Prosecution Service
- Representatives of critical infrastructure organisations, members of the Information Sharing and Analysis Centres (ISACs) and other NCSC partners
- National Management Organisation for Internet Providers (*Nationale Beheersorganisatie Internet Providers*)
- Internet Standards Platform (*Platform Internetstandaarden*)
- Bits of Freedom
- The Dutch employers' organisation in the technology industry (FME)
- ICT Netherlands (Nederland ICT)
- Dutch Payments Association
- Confederation of Netherlands Industry and Employers (VNO-NCW)
- Scientific institutions
- Universities
- Experts in the field of cyber security

The contributions of these parties have, together with substantive reviews, publicly accessible sources, a survey, information from the critical infrastructure and analyses from the NCSC, contributed to the substantive quality of this assessment.

Table of Contents

Key findings

Professional criminals and state actors continue to be the most significant threat and inflict most damage

Digital attacks are being used to influence democratic processes

The vulnerability of the Internet of Things has resulted in disruptive attacks that endorse the need to enhance digital resilience

Many organisations are dependent on a limited number of foreign digital infrastructure service providers which means that the social impact of disruption is large

The resilience of individuals and organisations is lagging behind the increasing threat

Summary

The Cyber Security Assessment Netherlands (CSAN) 2017 offers insight into interests, threats and resilience, as well as related developments in the field of cybersecurity. This CSAN focuses primarily on the Netherlands, for the period from May 2016 to April 2017. The CSAN is published annually by the National Coordinator for Security and Counterterrorism and is drawn up in cooperation with public and private partners.

Key findings

- Professional criminals and state actors continue to be the most significant threat and inflict most damage
- Digital attacks are being used to influence democratic processes
- The vulnerability of the Internet of Things has resulted in disruptive attacks that endorse the need to enhance digital resilience
- Many organisations are dependent on a limited number of foreign digital infrastructure service providers which means that the social impact of disruption is large
- The resilience of individuals and organisations is lagging behind the increasing threat

The impact that digital attacks have on society has become clear in recent years. The almost unlimited scalability of attacks ensures that investing in cybercrime is an attractive proposition to criminals. This threat is growing: professional criminals are focusing on major companies to a greater extent, their purpose being financial gain. State actors continue to work on digital sabotage and economic and political espionage. They are intensifying their efforts and in addition they have focused on digitally influencing democratic processes for geopolitical gain in recent years. The scale of the digital threat is increasing. Globally, more than 100 countries are engaged in espionage using digital tools.

Cyber attacks have led to leaks of information concerning the US presidential elections and a number of countries have observed influencing of the democratic process or attempts to do so. In the run up to the elections for the Dutch House of Representatives, the Netherlands issued clarification to enhance the digital resilience of political parties and organisations involved in the elections.

The costs and benefits of cybersecurity do not always lie with the same party: exploitation of vulnerabilities can lead to damage to parties other than the users of devices. The Internet of Things shows that this can go wrong: many of these devices contain vulnerabilities for which security updates are not published. Last year vulnerable devices were exploited to conduct large-scale DDoS attacks a number of times using botnets, which resulted in major disruptions. The users of the devices usually suffer no consequences but the targets that are attacked do. The fact that these attacks could have been perpetrated by cyber vandals shows that it is not only sophisticated professional criminals or state actors who can carry out disruptive attacks.

The Netherlands is heavily reliant on services from a limited number of foreign internet infrastructure providers such as Amazon Web Services, Microsoft and Google. Although major service providers have more resources at their disposal to arm themselves against attacks, the social impact of disruptions are significant because many different services depend on a small number of providers.

Insight into the measures that organisations and individuals take to enhance their digital resilience is limited. The growth in the number of manifestations does, however, indicate that resilience in the Netherlands is lagging behind the growth of the threat.

Insight into threats and actors

Table 1 provides insight into the threats that the various actors have posed over the period between May 2016 and April 2017 to the targets 'governments', 'private organisations' and 'citizens'. Professional criminals and state actors continue to be an undiminished major threat to government, private organisations and citizens. Threats that are indicated in red may increase while the level is already high.

Threats that have increased or decreased in comparison with the CSAN 2016 are indicated by an arrow. State actors are also focusing on the theft and publication of information, to influence democratic processes for example, as well as espionage and conducting offensive actions. The threat posed by hacktivists has increased for all targets where this concerns defacements and for citizens where takeover of IT is concerned. In recent years they have demonstrated that not only are they capable of carrying out defacements and of taking over IT systems but that they actually do this. The threat of manipulation of citizens' information by professional criminals has decreased compared to last year.

Table 1 **Threat matrix**

	Targets		
Source of threat	Governments	Private organisations	Citizens
Professional criminals	Disruption of IT	Disruption of IT	Disruption of IT
	Manipulation of information	Manipulation of information	Manipulation of information ↓
	Theft and publication or selling of information	Theft and publication or selling of information	Theft and publication or selling of information
	IT takeover	IT takeover	IT takeover
State actors	Digital espionage	Digital espionage	Digital espionage
	Offensive cyber capabilities	Offensive cyber capabilities	
	Theft and publication of information	Theft and publication of information	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft and publication of information
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of obtained information	Theft and publication of obtained information	
	Defacement ↑	Defacement ↑	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover	IT takeover ↑
Internal actors	Theft and publication or selling of obtained information	Theft and publication or selling of obtained information	
	Disruption of IT	Disruption of IT	
Private organisations		Information theft (industrial espionage)	Commercial use/abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure

Relevance legend

Yellow: *No new trends or phenomena are recognised that pose a threat.*
OR (sufficient) measures are available to remove the threat.
OR no appreciable manifestations of the threat occurred during the reporting period.

Orange: *New trends and phenomena are observed that pose a threat.*
OR (limited) measures are available to remove the threat.
OR Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.

Red: *There are clear developments which make the threat expedient.*
OR Measures have a limited effect, so the threat remains substantial.
OR Incidents have occurred in the Netherlands.

Changes with respect to CSAN 2016:
↑ Threat has increased
↓ Threat has decreased

Reader's guide

The CSAN 2017 provides insight into interests, threats, resilience and manifestations in the field of cybersecurity and the corresponding developments. A factual summary and an indication for the period May 2016 and April 2017 is given. The CSAN has been written based on insights and expertise from government services and organisations in the critical processes themselves. The developments are described in a qualitative form. Where available in a reliable form, it is substantiated by a quantitative foundation and/or reference to sources.

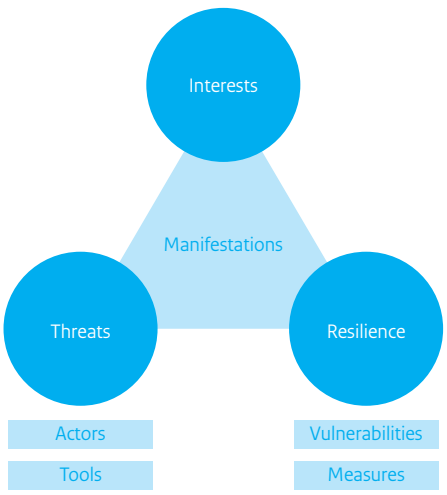
Monitoring developments is a continuous process, with the CSAN being one of the annual results. Matters that have not or have barely changed with respect to the previous editions have been described in brief or not at all.

The CSAN is subdivided into descriptions of manifestations, threats, resilience and interests.

The key questions of the CSAN 2017 are:

- What events or what activities by which actors could affect IT interests, what tools do they employ and what are the developments in this respect? (Threats)
- To what extent is the Netherlands resilient to vulnerabilities in IT, could these lead to an impact on IT interests and what are the developments in this respect? (Resilience)
- Which Dutch interests are being adversely affected, and to what degree, by restrictions of the availability and reliability of IT, breach of the confidentiality of information stored in IT or damage to the integrity of that information, and what are the developments in this respect? (Interests)

The triangle of interests, threats, resilience and manifestations is a model for the chapter format of the CSAN.



Chapter 1 describes which manifestations have occurred during the reporting period within the triangle of interests, threats and resilience. The chapter gives an overview of relevant manifestations both in and outside of the Netherlands. Foreign manifestations are mentioned where they are relevant to the Netherlands, although the Netherlands need not be directly affected.

Threats are set out in the chapters about actors and tools. Chapter 2 describes the capabilities and characteristics of actors, as well as their methods. Chapter 3 describes the tools that these actors employ and their development.

Chapter 4 gives an assessment of the resilience of the Netherlands. The resilience of the Netherlands can have an effect on the probability of a threat manifesting itself and can limit the impact of manifestations. Chapter 4 names both vulnerabilities and the measures that have been taken to limit those vulnerabilities, which together form the resilience of the Netherlands.

Chapter 5 discusses Dutch interests in the field of cybersecurity. The chapter focuses on the changes in these interests during the reporting period and their impact on cybersecurity.

The appendices provide an overview of the incidents handled by the NCSC, an assessment of cybersecurity within the various sectors and an explanation of the abbreviations used.

Democratic institutions have fallen victim to digital attacks

1 Manifestations

Information gathered by digital attacks is exploited in campaigns to influence public opinion. Victims of this include democratic institutions abroad. The digital theft and publication of information is used strategically by state actors. Exploitation of vulnerable devices allows larger disruptive attacks to be carried out.

This chapter describes the manifestations of digital attacks. There are various motives for an attack. This chapter considers activities aimed at influencing, disrupting or acquiring information and monetary gain. This chapter includes manifestations from within the Netherlands and from abroad. The manifestations from abroad are relevant because they could impact on Dutch interests or the resilience of organisations in the Netherlands.

Activities aimed at influencing

Democratic institutions have fallen victim to digital attacks

Several western countries are paying close attention to digital influencing of democratic institutions. The German political party CDU, the En Marche! movement of French President Emmanuel Macron and the American Democratic Party have all been victims of digital attacks. These activities appear to be aimed at disrupting and influencing the democratic process. They were attacks on the vulnerability of voters and not any (possible) vulnerability of the voting process.

In France, a large number of emails and documents from the movement of former presidential candidate Macron were published online shortly before the presidential elections in May 2017. As early as December, the movement had already detected that employees were being targeted by a phishing-email campaign.[1]

The TrendMicro security company announced in May 2016 that German Chancellor Angela Merkel's party had been the victim of digital attacks. Employees of the CDU received spear phishing emails that linked to a copied login screen for the webmail service that they used. The attacker hoped to acquire login details this way. Whether they succeeded is unclear.[2 3]

In the summer of 2016 it was announced that the American Democratic Party had suffered a number of successful attacks. Politically sensitive material was stolen in these attacks. According to the US intelligence services, the attacks were part of a campaign aimed at influencing the presidential elections. American security companies and the American government agree that Russian actors were behind the attacks.[4 5 6 7] The report describes how influence was exerted. Furthermore, it emphasises that there are no indications that the physical voting process was manipulated.

These activities were aimed at influencing decision-making processes and public opinion. In January 2017, the FBI announced that the Republican Party had also been targeted but stolen information had not been leaked. According to the FBI an email system belonging to the Republican National Committee (RNC) that was no longer in use had been comprised, among other things.[8] As far as we are aware, there has never before been an attempt on this scale to influence American elections with digital attacks on its democratic institutions.

In December, the American government announced diplomatic measures against Russia.[9] Russia has repeatedly denied involvement[10 11] and the individual who hacked the Democrats, calling himself or herself Guccifer 2.0. claims to have no ties with Russia.[12]

The various attacks on the American Democratic Party

The attack on the Democratic Party National Committee (DNC) that came to light in June 2016 has already been described in CSAN 2016. Eventually, there would be several attacks on the party. The Democratic Congressional Campaign Committee (DCCC) and many email accounts belonging to prominent members of staff were compromised.

- In March 2016, campaign leader John Podesta clicked on a link in a security email from Google which had been fabricated by the attackers and gave away his login details. This gave the attackers access to his personal Gmail account containing thousands of politically sensitive emails. Wikileaks started publishing parts of the stolen emails in July 2016.[13] Podesta wasn't the only target. Security company SecureWorks claims that the email was part of a spear phishing campaign targeting the accounts of 108 individuals connected with Hilary Clinton's presidential campaign.[14]

- In June 2016, media reports[15] appeared reporting that hackers had stolen data from the computers of the Democratic Party in the United States. Here the hackers specifically targeted the DNC's systems. They would have been able to read email and chat traffic of Democrats. The security company CrowdStrike connected the malware that was discovered to two Russian actors, who they suspect have strong ties to the Russian intelligence and security services.[16] [17] Responsibility for the attack was also later claimed by an unknown individual. He or she attempted to claim responsibility for the hack by releasing a number of documents.[18] In the aftermath of the hack, the FBI said it took ten months before the forensic analysis of the attack became available to the FBI.[19]

- In August 2016, 'Guccifer 2.0' published contact details for Democratic members of the House of Representatives and staff of the Democratic campaign (DCCC). Shortly afterwards, party documents from the same theft were leaked which included, among other things, details of the campaign strategy to be adopted in the various states. The information that was published would then be used by political opponents.[20]

The leaks were made in the blog of 'Guccifer 2.0', Wikileaks, the DCLeaks.com website and directly to various media. A storm of revelations about the Democratic party followed. Four highly-placed directors of the DNC resigned as a result of the information that was published.[21] DNC quickly replaced its computer systems and telephones. The DCCC shut down its computer network for a week.

Digital security of the Dutch elections under the spotlight

The media in the Netherlands was also full of reports about the digital security of political parties, election tools and the government in the run up to the elections to the House of Representatives. RTL took over the social media accounts of two politicians using passwords published in older data leaks.[22] Citizens and supervisors critically called the various election tools to account about vulnerabilities immediately after the launch of their websites.[23] Various Dutch organisations were targeted by DDoS attacks and defacements in the weekend of Saturday 11 and Sunday 12 March. Until suitable measures were implemented, the Stemwijzer and Kieskompas websites had limited availability the day before the elections due to DDoS attacks.[24]

Activities aimed at disruption

Mirai: botnets of (consumer) electronics caused large-scale DDoS

In the summer of 2016, the Mirai botnet took over tens of thousands of (consumer) devices on the Internet of Things (IoT), partly by taking over other botnets.[25] At the end of September the botnet attacked the website of cybersecurity journalist Brian Krebs. This resulted in Akamai, a supplier of anti-DDoS services withdrawing as Krebs' pro bono sponsor. The company said that costs were getting out of hand and paying customers had priority.[26] The French hosting provider OVH also fell victim to Mirai. The websites of OVH customers were temporarily slower for or not available to users in Southern Europe.[27]

Attacks were carried out by the LizardStresser-botnet earlier in 2016. This botnet also used infected IoT devices. Botnets as big as LizardStresser and Mirai are nothing new. The attacks were the first time that botnets of this size, exploiting vulnerable (consumer) electronics, were used to carry out large-scale DDoS attacks. We do not know who perpetrated the attacks with Mirai. The hacktivist-collective 'New World Collective' claimed responsibility for the attacks.

On 21 October, the Dyn DNS service provider was hit by major DDoS attacks carried out with botnets based on Mirai's source code. Dyn provides DNS services for 14% of the 1000 most popular domains in the world[28] and is supplier to Twitter, Spotify and Netflix, among others. These, and other service providers, were unavailable or hard to reach as a result of the attack. Despite the fact that it was systems on the east coast of the United States in particular that were affected, this also caused disruption for users in the Netherlands and reduced the availability of much-used services.

DDoS attacks the size of the attacks on OVH, Krebs and Dyn can only be prevented by the large-scale deployment of resources paired with significant investment. Only the largest parties or

coalitions of smaller parties collaborating very closely will be able to do this. In an analysis of the attacks, Dyn claims that competitors provided assistance with mitigation.[29]

Physical infrastructure as a target

In the night of 17 to 18 December 2016 there was a power outage in several districts of Kiev. The Ukrainian energy company Ukrenergo reported that the power outage had been caused by a cyber attack.[30] [31] In January 2017, security researchers from ISSP and Honeywell confirmed that it had been a cyber attack, just like the attack one year earlier.[32] The aim of the attack would have been to test attack techniques and the use of the distribution station as a testing ground.[33] In the same period, Reuters reported attacks on the Ukrainian ministries of Finance and Defence.[34]

Reports showed[35] that the attack in December 2016 cause a limited power outage of approximately one hour. The 2015 and 2016 attacks employed sophisticated malware. In 2016, attackers expanded the BlackEnergy-malware with modules aimed at attacking systems used by power distribution network managers. Infection would have occurred when managers opened phishing emails in the Ukraine on workstations they also used to manage power networks. The power networks of Saudi Arabia also fell victim to attacks in 2017 which employed the Shamoon malware. In addition to the power networks, government agencies and the financial sector in Saudi Arabia also fell victim.[36]

Activities aimed at acquiring information

Government agencies repeatedly targeted by large-scale and persistent digital espionage attacks

Last year, AIVD and MIVD saw that Dutch government agencies were repeatedly targeted by large-scale and persistent digital espionage attacks. For instance, the Ministry of Foreign Affairs and Ministry of Defence were attacked several times, including by countries that had not previously been identified as a threat to Dutch government networks.

The National Detection Network, among others, identified attacks at an early stage and then informed the bodies involved. The attacks attest to an extensive and structural interest in the Dutch government.

Foreign intelligence services conduct espionage campaigns to improve their country's economy and defence

Economically motivated digital espionage continues to be a concern for the Netherlands. The intelligence services detected the activities of various digital espionage campaigns in the Netherlands in 2016. Among other things, these activities targeted Dutch companies that are heavily involved in research and development, particularly in the IT, maritime technology, biotechnology and aerospace sectors. The activities varied from a few preparatory actions to the actual exfiltration of confidential business information.[37]

Several economically motivated espionage campaigns have been ongoing for years now and the majority have repeatedly attacked multiple domestic and foreign companies in the Netherlands in recent years. Confidential and advanced IT, maritime, energy and defence technologies were stolen in these attacks, in addition to personal data. Such attacks are a threat to the economic earning capacity and military capability and confirm a structural interest in sensitive information belonging to Dutch businesses.

On Wednesday 15 June 2016, the Volkskrant newspaper published an article[38] on the hacking of the Dutch-German defence company Rheinmetall. Chinese hackers would have been attacking this company since 2012. According to the Volkskrant, the hack would have been discovered by the Fox-IT security company at the end of 2015.

In December 2016, it was announced that sensitive commercial information had been stolen from the German company ThyssenKrupp in cyber attacks earlier that year.[39]

Five-year-old leaked account data now being exploited for phishing

LinkedIn was hacked in 2012. When it was, the account details of 167 million users were breached.[40] The leaked names, email addresses and password hashes remained unused for a long time. From May 2016, the dataset was publicly being offered for sale and exploitation became evident: in June, Fox-IT reported phishing campaigns in the Netherlands, personalised based on the LinkedIn data.[41] The NCSC also received an alert from various sectors that phishing emails were being sent based on the LinkedIn data.[42]

Vulnerable (consumer) electronics susceptible to eavesdropping

The iPhone of human rights activist Ahmed Mansoor was attacked in August 2016 using government surveillance technology. The installation of Pegasus spyware allowed the attacker to eavesdrop on the microphone, camera and communications as well as track the phone's movements. In this attack, security researchers discovered three unknown vulnerabilities in Apple products with an estimated market value of 1 million dollars.[43] Apple saw the need to roll out a critical security update across the globe.[44]

Less advanced (consumer) electronics are also vulnerable. An investigation by the Norwegian consumer association revealed that attackers used children's doll 'My Friend Cayla' as an eavesdropping device.[45] The children's doll, which is also sold in the Netherlands, was not safeguarded and could easily be eavesdropped, by nosy neighbours for instance. According to the Dutch Consumers' Association, Dutch toy shops withdrew the doll from sale and asked the supplier for an explanation.[46]

Activities aimed at monetary gain

Compared with the CSAN 2016, there has been little change in manifestations aimed at monetary gain in the Netherlands. Managed service providers indicate that responding to ransomware has become almost common practice. On the one hand, this results in attention to creating and restoring backups. On the other hand, these manifestations show that the resilience to ransomware infections still leaves a lot to be desired. The Dutch banks are seeing further decline of losses due to internet-banking fraud.[47] In March 2017, the House of Representatives had problems with a ransomware infection,[48] [49] distributed by email to several Members of Parliament.

CEO fraud is on the rise in the Netherlands. Last year the NCSC, the Fraud Help Desk and the police received a remarkable number of reports of CEO fraud. The financial sector and managed service providers also reported an increase in the number of fraud attempts. In this type of fraud, criminals try to get the financial department of an organisation to deposit money in the account of an accomplice using an email purporting to be from a Director or Head of Department.[50] When doing so they usually use domain names that are very similar to the domain name of the company concerned. To this end, fraudsters register false domain names en masse, although this trend appeared to decline in the Netherlands at the end of 2016.[51]

In 2016, there were multiple manifestations of attacks targeting banks abroad. On 7 November, Tesco Bank suspended online payment facilities for all account holders following fraudulent transactions on 9000 accounts on the days preceding, worth a total of 2.5 million pounds sterling.[52] On 3 February, researchers reported a series of malware infections in the Polish financial sector. Criminals appeared to have used the Financial Supervisor's website as the central source for distributing malware (Watering hole) to the internal systems of various banks.[53]

Hacks as the basis for influencing the stock market and exchange rate speculation

In January, Italian police arrested two suspects on suspicion of hacking and stealing state secrets. The police claim that the suspects wanted to invest based on the stolen information. Accounts belonging to lawyers, accountants, unions, the Police, Civil Servants at the Ministry of Economic Affairs and the Vatican would, among other things, have been compromised.[54] The Kaspersky antivirus company analysed the malware that was used and classified the pair as highly effective amateurs.[55]

Security researchers at the MedSec startup worked together with the Muddy Waters hedge fund to profit from vulnerabilities in pacemakers from the American St. Jude Medical. Investor Muddy Waters speculated on an anticipated fall in rates on the stock exchange following publication of a report of these vulnerabilities.[56] This resulted in criminal proceedings.[57] The vulnerabilities themselves appeared to be serious; they could be used to manipulate pacemakers and defibrillators and their functioning.

In January, it was reported that the supplier had issued an update patching the vulnerabilities. However, researchers who had discovered the vulnerabilities concluded that the update did not address all of the vulnerabilities.[58] The American Food & Drug Administration (FDA) issued a warning to St. Jude Medical in April 2017 stating that the actions to improve security had not been sufficient.[59]

Volume of data leaks and their confidentiality is increasing

Data breaches manifested themselves throughout the entire reporting period. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) received almost 5700 reports of data breaches in 2016.[60] These are all reported data breaches, not only leaks relating to cybersecurity.

In the first quarter of 2017 the Dutch Data Protection Authority received 2317 reports of data breaches. Twelve percent of the cases concerned data breaches involving incidents in the cybersecurity field, seven percent of these involved hacking, malware and/or phishing, five percent involved displaying the personal data of the wrong customer in a customer portal.[61]

The further increasing volumes and the degree of confidentiality of breached information discovered and reported in the incidents is notable. The Dutch Data Protection Authority also observes that data breaches are not always reported. Examples include malware infections and data breaches by processors, such as cloud providers.

In 2016, Yahoo twice reported the largest known data breaches in the world. In September, the company reported the loss of personal data for 500 million accounts as the result of a hack in 2014.[62] In December, Yahoo made a second report of a hack in 2013 where the personal data of 1 billion users would have been stolen.[63] Yahoo stored passwords insecurely and unencrypted and in addition to personal data it leaked a treasure trove of password information which could be exploited at other service providers, if passwords were being reused.[64] Both hacks were announced during the takeover of Yahoo by Verizon which announced a negative revaluation of 350 million dollars in February 2017.[65] The Stock Exchange watchdog SEC is investigating the timeliness of Yahoo's reports.[66]

In September 2016, Netbeheer Nederland and Energie-Nederland announced that the energy data of 2 million households had been stolen by an employee of a company working for an energy supplier. It was data from a central recording system for energy contracts that had been concluded, which could be exploited to make un-requested offers to consumers.[67]

The wage details of a couple of thousand (former) employees of ASML and Philips were published on Pastebin in November.[68] It appeared to be wage slips from 2010 that were left on the street by a supplier to these companies. Erasmus University Rotterdam reported a data breach as a result of a web server being hacked. The personal data of 17,000 people was leaked, including financial data, citizen service and document numbers, nationalities and data about health.

Not all data breaches are reported. At the same time, it later on appeared that many reports were not necessary, but they were reported proactively in connection with possible sanctions. Based on a random sampling of 66 municipalities under the Government Information (Public Access) Act, NPO Radio 1 claimed municipalities are not reporting half of the data breaches.[69]

Less advanced actors are capable of carrying out attacks with major impact on society

2 Threats: Actors

Compared with previous years, the threat level from various actors groups is largely stable; state and criminal actors are still the greatest threat to Dutch digital security and they develop more quickly than other actors. Last year, state actors conducted digital campaigns to influence public opinion.

This chapter deals with actors who affect the confidentiality, integrity or availability of information or information systems. When doing so, attention is focused on the intention of the individual actors, their capabilities and the developments in this field.

Attribution, discovering who is behind an attack, is difficult. Reasons for this include the actors trying to hide their identity and attempts to mislead with red herrings. At the start of 2017, news sites were reporting that digital bank robbers had hidden Russian texts in their malware while based on grammatical errors the suspicion is that Russian cyber criminals were not involved.[70] Another reason why attribution is difficult is that various actors sometimes use similar tools. This could indicate the same actor but it could also be a different actor using the same tools. In addition, an actor's intention in an attack is not always clear. For instance, a DDoS attack can be used to disrupt processes, but it can also be used to disguise other activities.

Professional criminals

The threat that criminal actors pose to Dutch digital security continues to develop at a high pace. Successful revenue models are being further explored, new scenarios are being developed[71] [72] and less traditional targets are being attacked.

Criminals are diversifying with the use of ransomware

The development of new methods by criminals is manifesting itself in, among other things, exploring the lucrative[73] revenue models of ransomware.[74] In addition to un-targeted attacks, criminals are employing ransomware more frequently to target organisations where the impact is significant and who will be more inclined to pay a higher amount of ransom.[75] This year the trend of these targeted attacks manifested itself worldwide, particularly at schools,[76] hospitals and other health institutions.[77] [78] Attacks by criminals are also having an even greater impact on everyday life because processes or services can be (unintentionally) disrupted. Examples include the ransomware attack that affected the payment system on San Francisco's public transport[79] [80] and the attack on the systems in an Austrian hotel which prevented the key passes from working.[81]

Researchers have demonstrated that ransomware can also be used against industrial control systems (ICS) and consumer electronics as part of the Internet of Things.[82] It is conceivable that criminals will target these areas also in the near future. In the case of ransomware in ICS in particular, this could lead to changes in the revenue model, given that it can be extremely important to restore functioning to the affected systems.

Criminals are targeting financial institutions more frequently

More often than in previous years, criminals are targeting their digital attacks on the systems of companies, banks and other financial institutions (the so-called high value targets) instead of targeting consumers only. When doing so, criminals are looking at how access to the network can be maximally exploited and turned into cash.[83] Although there have been no manifestations of these developments in the Netherlands yet, various European banks were targeted by cybercriminals in 2016.

This is illustrated by various standalone incidents. The British Tesco Bank announced that all online transactions were being suspended temporarily after approximately 9000 customers became victims of fraudulent transfers.[84] A criminal group, calling themselves Cobalt,

infiltrated the networks of a couple of European banks. Then, a large number of ATMs were emptied using money mules.[85]

In addition, banks across the globe were robbed by obtaining and exploiting access to the SWIFT (payment) system. A number of research companies have suggested the involvement of North Korea.[86] [87] In September 2016, in response to the attacks, SWIFT announced global information security requirements for participating banks.[88] [89] Criminals also exploited access to the systems of a bank in Liechtenstein to extort foreign account holders.[90]

Although these stand-alone attacks cost criminals more preparation time and resources, the financial gain is greater than (simple) attacks on consumers.

State actors

The professionalism and number of countries employing digital espionage is growing

In recent years, more and more countries have acquired the capability to gather intelligence from the digital domain. It is a relatively inexpensive method, it is quick and has fewer risks than traditional espionage because its use can be denied. Over the last year, Dutch government agencies were repeatedly the victim of large-scale and persistent digital espionage attacks by other countries, including by countries not previously identified as a threat to Dutch government networks.

More than 100 countries currently have the capacity for digital espionage and their professionalism is growing, as is the threat it poses. This growing digital espionage threat is aimed at both public and private parties and comes from countries that want to position themselves more favourably in the world both politically and economically. It is primarily used by intelligence and security services.

States continue to invest in offensive cyber capabilities and employ them

The AIVD and MIVD have identified that many countries are investing in setting up (military) offensive digital capabilities. When doing so, digital tools are used for influencing and information operations. Accounts are hacked to gather confidential information which is later published by an (apparently) independent party to sow confusion and division in opponents.

In addition, the intelligence services have also identified that many countries are investing heavily in setting up digital capabilities aimed at the (future) sabotaging of critical processes. The digital attack on Ukrainian power plants in December 2015 was followed in December 2016 by a new attack on Ukrainian critical infrastructure. This time part of the capital Kiev was temporarily without electricity. In Saudi Arabia, a number of government agencies and companies[91] were victims of a destructive virus (Shamoon 2.0). These events over the past year illustrate the potential of digital attacks to inflict political and physical damage, as well as the willingness to actually use this tool.

Hackers in the service of a state can hide themselves on the internet very professionally. The intelligence services have also observed that several state actors are structurally using private IT companies as a cover to disguise their espionage activities. In addition, IT companies and academic institutions are used to develop malware. This increases the potential of state actors to mount offensive cyber attacks.

State actors are seeking new methods

State actors are seeking new digital methods of infiltrating computer networks without being detected, possibly in combination with traditional methods. Although many digital attackers are still using spear phishing, USB sticks and watering holes to gain access to a computer network through malware infections, the methods of professional and sophisticated states are becoming increasingly difficult to detect.

Efforts are being targeted on hardware or routers for instance, or on malware-injection via WiFi networks. An attack could even be free from malware. Protocols upon which the internet functions were originally designed to transport data as efficiently as possible and without too much attention to security. States could exploit vulnerabilities in these protocols for digital espionage.

The highly developed IT infrastructure in the Netherlands remains attractive as a transit port for digital attacks. The AIVD and the MIVD have detected various state actors exploiting Dutch infrastructure to attack third countries. As a result, the Netherlands is unwillingly involved in the distribution of digital attacks that infringe the economic, military and political interests of other countries.

Terrorists

Jihadists are primarily responsible for the present-day terrorist threat. In the reporting period, manifestations on the digital front were mainly by ISIS and ISIS sympathisers (hereinafter referred to as ISIS).

Intention to mount cyber attacks

Although jihadists did not yet appear to be capable of mounting sophisticated digital attacks in the last reporting period, jihadists and certainly ISIS are intent on mounting cyber attacks. The primary objective of the attacks, defacements[92] and DDoS attacks[93], that have been carried out were of a propagandistic nature. This also applied to published lists containing information about individuals which ISIS claimed to have obtained from hacking and which were accompanied by calls to kill these people:[94] the death lists. In addition, it appeared that most of the information could

already be found on the internet[95] and no one who is on the list has ever been killed.

Jihadists also intend to mount cyber attacks targeting the lives of people, focusing on violence or on disrupting society. There have been no manifestations of this yet, as far as is known.

Jihadists have limited capability to mount cyber attacks

According to experts' estimates, jihadists – and terrorists in a broader sense – are not yet capable of mounting sophisticated, complex attacks. Relative little expertise and few tools were needed for the simple cyber attacks that jihadists have carried out. Their power to strike and recruiting potential may increase now that a number of hackers and hackers groups have united in the 'United Cyber Caliphate'.[96] They are calling for hackers to join them.[97] In addition, jihadists are gaining experience with simple cyber attacks.

It is a matter of concern that many products and services for cyber attacks are being sold through various forums. This could reduce the threshold for cyber attacks by jihadists. In any case, ISIS certainly has less money compared with previous years,[98] which makes the financial opportunities to purchase the most sophisticated products and services less credible.

Jihadists usually attack random targets

Insofar as terrorists have carried out cyber attacks, this was largely on random targets that displayed vulnerabilities. Publications mainly warn of jihadists mounting cyber attacks on critical infrastructure,[99] usually due to the disruption and publicity value that could result from this. However, mounting targeted, sophisticated attacks requires more IT expertise than they have demonstrated in cyber attacks they have perpetrated up to now. This makes targeted, sophisticated attacks less probable. This does not detract from the fact that small-scale attacks by jihadists, that are mainly of a propagandistic nature, generate media interest and can therefore lead to feelings of fear.

Hacktivists, cyber vandals and script kiddies

Hacktivists carry out digital attacks for ideological or activism reasons. Cyber vandals and script kiddies carry out cyber attacks as pranks, as a challenge, or to demonstrate their own capabilities. Both their motives and their skill levels can vary widely. For example, in March 2017 the rising diplomatic tension with Turkey was the reason various people mounted (small-scale) digital attacks for activism or nationalist reasons.[100] [101]

On 29 July 2016 in Vietnam, information screens at a number of airports displayed anti-Vietnamese and anti-Philippines slogans explicitly referring to the dispute in the South China Sea. The media reported that the 1937CN hackers group was behind the operation.[102] Although the origin of the attack is difficult to establish, a hacktivist motive is plausible. The escalation potential of such attacks is substantial because it is often difficult to discern the attackers' intentions.

The conceivable threat from hacktivists, cyber vandals and script kiddies is growing

Although no notable developments have taken place in the hacktivism field in recent years, the conceivable threat from these actors in increasing. This is because digital attacks that could have a significant social impact are easier to mount. This is partly as a result of the increasing availability of easy-to-use products, services and tools to mount these attacks.

A previously-mentioned example of this availability which can have a major effect is the large-scale DDoS attack on DNS provider Dyn, which used the (publicly available).'Mirai' botnet code.[103] Responsibility for this major attack was claimed by the unknown 'New World Collective', which calls itself a hacktivist collective that wants to test the security of websites.[104] However, whether or not this statement by the attackers is the real motive behind the attack cannot be checked.

Internal actors

Threats from internal actors is unchanged

The motive of internal actors is usually of a personal nature. They act from financial, political or personal motives such as revenge after dismissal. Threats from internal actors can, however, also come from unconscious actions and carelessness. Although there have been manifestations of internal actors over the last year too, there is no indication that the threat from internal actors has changed compared to the previous reporting period.

Private organisations

There are three types of threat from private organisations: organisations can attack the confidentiality of systems for financial gain, to improve their competitive position or to use the data gathered commercially without permission to do so having been given explicitly. As far as the latter is concerned, there has been a discernible shift in the US. In April 2017, the US Congress adopted a law clearing the way for providers to sell the surfing behaviour of users.[105]

Private organisations sometimes share information with others without permission

Private organisations can obtain a lot of data from customers by offering products or services such as apps. They can then use that data commercially themselves, pass it on or sell it to others.

Although users usually grant permission for this (wittingly or unwittingly) there were a number of media reports in 2016 and early 2017 of companies using data commercially or passing it on

without it being sufficiently clear that permission to do so had actually been granted. This concerned, for example, the placing of unwanted tracking cookies by websites that were offering self-tests for depression, alcohol consumption or stress or the placing of tracking cookies by the Stemwijzer (Voting Guide).

Other examples were the commercial use of user information from smart TVs, WhatsApp passing information on to its mother company Facebook or the transmission of WiFi details from Windows 10.[106]

Conclusion and looking ahead

The objectives of the individual actors have not changed in relation to previous years. More activities have been observed over the last year where state actors tried to influence public opinion using digital methods. The growth in the capabilities of various actors has remained stable by and large. Products, tools and services that can be obtained through various forums continue to reduce the threshold for cyber attacks (potentially with significant social impact) by actors with fewer own capabilities.

The threat to the Netherlands' digital and social security from criminals and state actors is increasing and continues to develop. In addition, successful models are being further developed and expanded. Attacks by professional criminals can gain greater impact on everyday life from this because much-used processes or services can be disrupted. In addition to this, criminals are increasingly targeting their digital attacks on the systems of companies, banks and other financial institutions instead of targeting consumers.

Many countries are investing in setting up digital capabilities focusing on the (future) sabotaging of vital processes as well as in digital tools that can be used to remedy influencing and information operations.

It is plausible that state actors and criminals will continue their further investment and innovation in the coming years. Although no threat to national security has yet been detected from terrorists as far as cyber attacks are concerned, this is conceivable due to the intention to mount cyber attacks, the bundling of forces, recruiting appeals to IT experts and the ability to acquire products, tools and services.

During the reporting period there have been occasional manifestations of hacktivists but this is highly dependent on events that could inspire hacktivists in the ideological field. Examples include attacks, conflicts and political themes. There is no clarity on the identity of the perpetrators or the motive for the Mirai and related botnets attacks but it is likely that it is not only state actors and professional criminals who are capable of carrying out these types of major, disruptive attacks.

The Internet of Things is abused to carry out DDoS attacks

3 Threats: Tools

Over the last year, the Internet of Things has been used for cyber attacks. Existing techniques such as ransomware continue to be popular with criminals. In addition, criminals are seeking new types of systems and ways to employ these tools. They are also improving the tools to work more efficiently and increase their profits. IoT devices will continue to be vulnerable over the coming years due to the conflicting interests.

This chapter describes developments in the field of tools that have been employed by actors to carry out attacks in the reporting period.

Internet of Things

In recent years, various security experts have warned of the increasing threat from the Internet of Things (IoT).[107] IoT devices, (consumer) electronics, generally have moderate to poor security.[108] This is due to, among other things, the use of default passwords and weak passwords, the lack of encryption, the lack of software updates to patch vulnerabilities and basic design faults. These vulnerabilities were exploited numerous times last year and IoT devices have been employed as a tool to carry out attacks. In addition, in a few cases devices were exploited to eavesdrop on their users or to manipulate the users' surroundings.

Internet of Things included in botnets

There was relatively little large-scale exploitation of IoT devices in the first half of 2016. However, in September 2016 there were a number of signs that malicious parties were making large-scale use of these devices. An IoT botnet with over a million devices was detected that month. Botnets carried out major DDoS attacks at that time. On 20 September 2016 the website of security journalist Brian Krebs was brought down by a 665 Gbps DDoS attack,[109] which is almost twice as large as the largest known attack prior to this. Shortly afterwards this record was broken once again when hosting provider OVH was attacked by a DDoS attack of more than 1 Tbps.[110] Large DDoS attacks are not new and are carried out frequently, with or without botnets. What is notable about these two large attacks is that they were carried out using large botnets of compromised IoT devices; home routers, webcams and digital television receivers.

The source code of the Mirai botnet, which was used in the attack on Brian Krebs' website, was released at the end of September 2016 and is publicly available.[111] The knowledge that was released with it has led to the earlier, less successful, NyaDrop IoT malware making a comeback with an improved attack technique.[112]

In November, 900,000 Deutsche Telekom customers were victims of another Mirai botnet.[113] The Speedport router of this group of people was infected by the botnet, bringing down their internet connection. In the same month, it was announced that a twelve-year-old vulnerability in OpenSHH had been exploited to gain access to embedded devices with an internet connection.[114] These devices were then exploited to mount further attacks on other systems.

Exploitation is facilitated by poor attention to the security of devices

DDoS attacks perpetrated with the aid of IoT devices are very difficult to counter. Little attention is devoted to the security of IoT devices. The users don't change default passwords and the device installation process does not make it mandatory. Software updates from the supplier to patch vulnerabilities are still not customary for IoT devices either.[115] As a result, IoT botnets can easily be created and remain undetected by the owner of an IoT device for a lengthy period of time. The speed with which these devices become infected is slightly higher than that of normal workstations because these devices are less resilient.

Denial of Service

The size of DDoS attacks is increasing

In addition to the size of the largest DDoS attack, the size of the average DDoS attack is increasing too.[116]

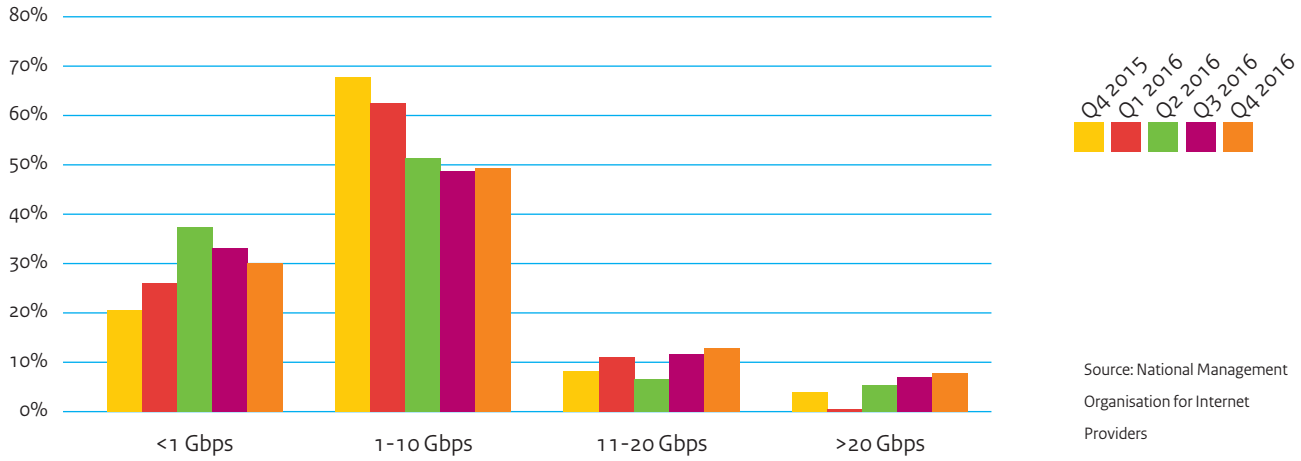
Vulnerable IoT devices make a significant contribution to the increase in the size of DDoS attacks.[117] It is notable that, unlike other DDoS attacks, no special techniques to increase the effect of the attack are used with IoT devices. Up until now, it has only been the number of vulnerable IoT devices that were used that determined the size of the attacks carried out using them.

In May 2017, TrendMicro reported the Persirai botnet that is capable of attacking 100 different IP-camera models,[118] and thereby mounting DDoS attacks. Currently, 120,000 cameras are estimated to be at risk of becoming part of the botnet due to a vulnerability in the camera.

In 2016, the National Management Organisation for Internet Providers (NIBP) processed 681 DDoS attacks, which is an average of almost two attacks every day. More than half of these attacks had a size of between 1 and 10 Gbps. Approximately 5 percent were larger than 20 Gbps and around 30 percent were smaller than 1 Gbps. The largest attack was 53 Gbps and lasted 14 minutes. In 2016, more than half of the attacks lasted less than 15 minutes. Almost five percent lasted longer than four hours with three attacks lasting longer than five consecutive days.

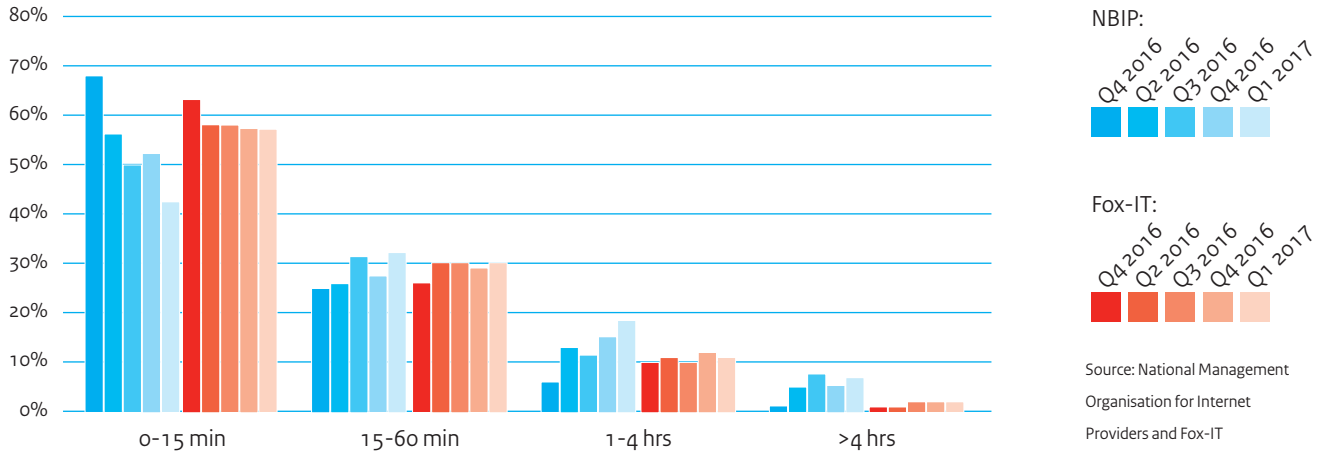
In 2016, Fox-IT in collaboration with DDoS.Watch used a monitoring system to observe approximately 1.3 million DDoS attacks both domestically and abroad. Approximately 25,000 of

Figure 1 **Size of DDoS attacks**



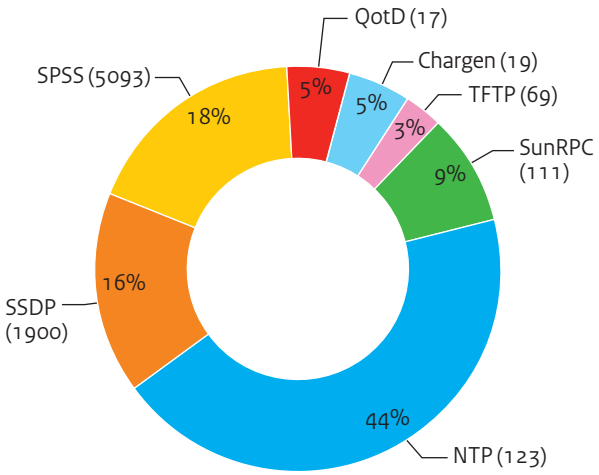
Source: National Management Organisation for Internet Providers

Figure 2 **Duration of DDoS attacks**



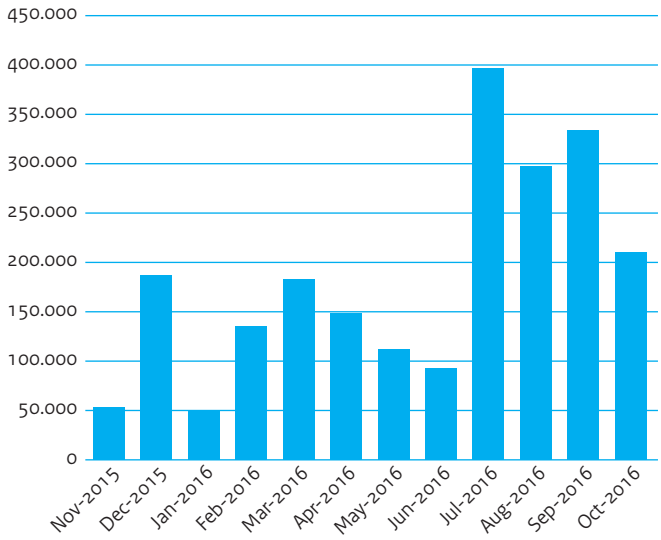
Source: National Management Organisation for Internet Providers and Fox-IT

Figure 3 **Protocols used for reflection attacks via the Netherlands**



Source: Akamai

Figure 4 **Number of users attacked by ransomware**



Source: Kaspersky Lab

them targeted IP addresses in the Netherlands. This puts the Netherlands in ninth place of countries that most frequently fell victim to DDoS attacks in 2016. A large number of these attacks targeted the internet connections of consumers and were of short duration. Only a small percentage of the attacks lasted longer than four hours. In 2016, DNS amplification attacks were still the most popular, but attacks based on NTP appear to be on the rise in 2017.

A Turkish hackers group is rewarding others for carrying out attacks. They have made a DDoS tool available for this and award points to those who attack a predetermined website.[119] These points can then be exchanged for other hacking tools.

Ransomware

Ransomware continues to be lucrative

Ransomware is still a very lucrative and growing branch of cybercrime.[120] Of the known cyber attacks, the percentage of ransomware attacks rose from 5.5 to 10.5 percent in the second half of 2016.[121]

In addition to the usual payment methods, often bitcoin, ransomware variants where iTunes or Amazon gift cards were demanded as payment of the ransom appeared in 2016.[122] [123] This choice is remarkable because they are much easier to trace than the usual payment methods.

Research has revealed that, worldwide, the healthcare sector is hit most often by ransomware.[124] The Dutch healthcare sector has problems with this too. Although it usually involves random distribution, the sector admits that it suspects that targeted attacks are sometimes involved.[125]

Last year, an expansion of the ransomware playing field became apparent. In addition to classic attacks on workstations by email, attacks were also mounted using exploits to infect servers.[126] The information in poorly safeguarded online databases can also be held hostage, where a ransom has to be paid to get this information back. This happened to a large number of MongoDB database software users around the turn of the year 2016–2017.[127]

It is becoming increasingly easy to conduct ransomware campaigns. Professional criminals can buy malware through ransomware-as-a-service to then distribute it themselves.[128] This development is not new but it has continued over the last year. In April 2017 there was a report of the Karmen ransomware variant being offered as ransomware-as-a-service for only 175 dollars.[129]

Android devices are also being targeted by ransomware

Ransomware on mobile Android devices is on the rise.[130] Users are tempted to install or update an app, after which the device is infected. The device is then locked and the user must pay a ransom to regain access. Payment via prepaid cards is demanded for this. Just as in the early days of ransomware on the PC, payment does always result in the release of the mobile device. Ransomware on a mobile device appears to have less impact than on a PC because these types of devices often have an automatic cloud backup. The potential reach of ransomware on smartphones is, however,

greater than on other devices; the smartphone has overtaken the laptop and it was the device most frequently used to access the internet in the Netherlands in 2016.[131] [132]

Infections using new methods and on different devices are emerging

A new way of getting ransomware onto a victim's computer is using an attack on the Remote Desktop Protocol (RDP).[133] This type of attack is used to gain access to the system which is then infected with ransomware. The WannaCry ransomware exploits a vulnerability in the SMB file sharing protocol to distribute itself.

Criminals are creative in their quest for new options to acquire money. This became clear in a case of ransomware on a TV set.[134]

Cybercriminals are adopting an even bolder approach

Attacks by criminals are not only more sophisticated from a technological standpoint. Criminals are seeking better opportunities to achieve their aim in other areas too. When doing so, they are seeking direct contact with their potential victims more and more often. For example, there was a report of ransomware with a live-chat function in early 2016.[135] In this way, the cybercriminals were offering the victims support when paying the ransom to receive the decryption key.

In addition to the option to pay to obtain the decryption key, victims of the Popcorn Time ransomware were given the option of infecting two others with the ransomware to obtain the decryption key for free.[136] This was on condition that the two new victims would actually pay for their decryption key.

At the end of 2016, victims of the CryptXXX ransomware were offered a discount on the purchase of the decryption key as a Christmas offer.[137] The aim of this temporary discount was to convince doubters to pay.

Email

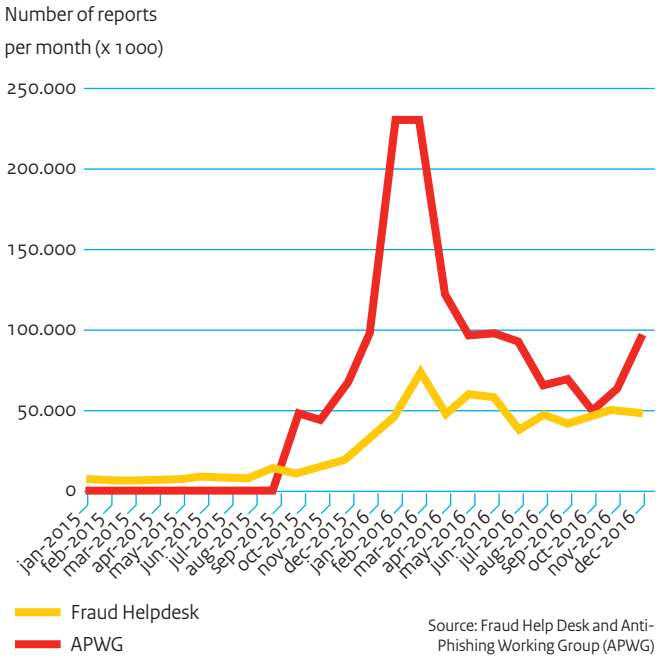
Email is still popular with attackers

Email was still the most used medium for distributing ransomware in 2016.[138] There is no universally correct method of protecting email. This allows criminals to easily reach large numbers of potential victims. It is difficult for the average email recipient to establish if the sender is authentic.

Phishing, particularly using email, is still heavily used by cybercriminals. Messages are becoming more refined and look more professional. Phishing was used to initiate a cyber attack in 91 percent of cases.[139] Last year, the Fraud Help Desk stated there had been a large number of reports of phishing emails.[140]

A research report on the 'Cloud Hopper' campaign appeared at the start of April.[141] This campaign targeted managed service providers

Figure 5 **Number of reports of phishing emails increased significantly in 2016**



Source: Fraud Help Desk and Anti-Phishing Working Group (APWG)

in particular. Spear phishing emails containing malware were sent to gain access to these providers' networks. After successful infection with malware, a search was made for sensitive data belonging to customers, such as intellectual property and personal details. The information that was found on the systems of the provider's customers was siphoned off to the network of the provider itself and then fed through to the attacker's own infrastructure.

CxO fraud, which often uses spear phishing, caused significant economic losses across the globe last year.[142] In the previous period, the NCSC received a number of reports of attempted CxO fraud from various sectors. Only a few of these attempts led to the actual theft of financial resources.

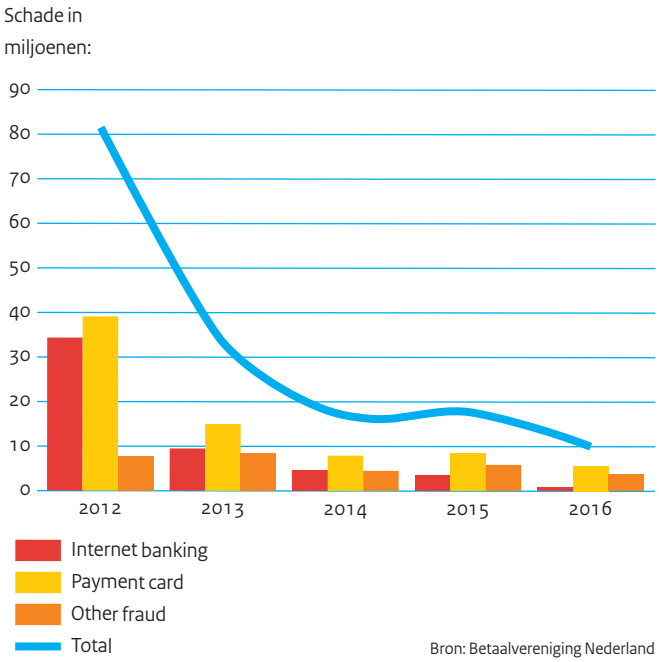
Although the existing tools are being used extensively and lucratively, cybercriminals are constantly seeking new tools. In addition, they are seeking new ways of using the existing tools more effectively. As soon as the resilience to tools increases, the cybercriminals start looking for other tools.

Financial sector

Banks are combating fraud more effectively

Banks are learning how to combat internet banking fraud increasingly effectively. The losses arising from fraud fell by 78

Figure 6 **Losses from fraud in the payment traffic in the Netherlands**



Bron: Betaalvereniging Nederland

percent in 2016 compared with 2015.[143] [144] Cybercriminals are not only targeting consumers in this way but are also increasingly targeting companies and the banks themselves. There is a discernible difference here: there is still a large group of criminals targeting consumers and taking the easy money. Another, smaller group of professional criminals are capable of conducting major campaigns. The number of attacks they perpetrate when doing so is lower than the number of attacks targeting customers, but the tools they use to do so are more sophisticated and the return per attack is many times greater.[145] By attacking business transactions, criminals benefit from the fact that these transactions are less well linked to set patterns which makes them more difficult to protect through transaction monitoring.

A report from the security researcher Group-IB on the criminal group calling themselves Cobalt, which attacked ATMs, was published in November 2016.[146] Spear phishing emails to a number of foreign banks were used to gain access to the bank's local network. This allowed Cobalt to infect the ATM network which is protected from the internet in stages. They then emptied a large number of ATMs in a short period of time.

There have been manifestations of malware on ATMs outside of the Netherlands

Security companies TrendMicro and FireEye have noticed an increase in the use of malware for ATMs. The companies publish analyses of the new variants that target middleware, a software platform which allows ATMs from different manufacturers to be attacked. Both types of malware are used as a tool in a physical attack and there have been no manifestations in the Netherlands. Moreover, the Dutch banks had already implemented measures prior to this which largely makes such attacks impossible.

TrendMicro issued a report on ATM malware Alice which they discovered in a joint research project with Europol EC3.[147] FireEye has detected ATM malware Ploutus-D, a new variant of the already known malware Ploutus, in research in Latin America.[148] The company claims that this type of malware will mainly be more effective in countries with less stringent physical protection measures on ATMs. Whether or not Alice and Ploutus-D are related remains unclear.

Advertising industry

Click fraud is causing losses in the advertising industry

At the end of 2016, cybercriminals were able to steal money from the advertising industry using the Methbot botnet. To do this, they registered domain names in such a way that it appeared as if they belonged to large, well-known organisations. These domain names were then subscribed to an advertising network for advertisements to be placed on them.

The advertising network's algorithm was misled by the domain name registration method, as a result of which it incorrectly judged that it was a large, interesting website and then placed an advert on it. A botnet was then used to automatically click on the advertisement link, where the advertiser paid a sum to the owner of the domain name for each click. Real users were simulated by automatically logging on to social media accounts and simulating mouse movements and mouse clicks from a browser specially developed for this purpose.

Fewer cases of malvertising

Infecting systems by distributing malware through advertisements on websites, malvertising, appears to be happening less frequently in the Netherlands. The sectors have only reported dealing with a small number of cases. Although there are reports from all over the world that the number of cases of malvertising continues to increase in relation to previous years,[149] the Netherlands appears to be unaffected by this. RiskIQ is reporting a good 132 percent increase in the total number of cases of malvertising worldwide. Over the last year measures to prevent infections from malvertising have been implemented on both the user side and the website owners side. According to figures from PageFair, use of adblockers in the Netherlands has risen to 17 percent over the last year compared with 13.9 percent in the second quarter of 2015.[150] [151]

Espionage software

The espionage software of intelligence services is being compromised

In August 2016, unknown hackers calling themselves the Shadow Brokers alleged that they had compromised a U.S. espionage campaign. They claimed to have stolen espionage malware through intrusion.[152] They then published some of this malware, hacking tools and exploits in order to strengthen their claim that the material came from U.S. intelligence services. Some undisclosed material was offered for bulk sale via a public auction[153] and some of it was published later. The published files contained espionage malware that facilitates attacks on firewalls including those of the Cisco, Fortigate and Juniper companies. Part of this was malware associated with the actor the Equitation Group; according to Kaspersky Labs they are allied to American intelligence services.[154]

In March 2017, Wikileaks[155] published information about another leak. This is alleged to be an internal wiki belonging to the CIA, documenting the CIA's hacking tools and malware. The hacking tools and malware itself was not released.[156] Wikileaks gave an undertaking to share this information with the suppliers of products or services with vulnerabilities that are being exploited.[157]

In April 2017, the Shadow Brokers once again published espionage malware. They claimed that this also originates from the American intelligence services. The most discussed tools were EternalBlue, an exploit that takes advantage of the SMB file sharing protocol on Windows systems to compromise those systems and DoublePulsar, a backdoor that can be installed on infected systems to execute various malicious code.[158] It is noteworthy that the exploited vulnerability had already been patched by Microsoft one month previously with a security update for Windows.[159]

At the start of May 2017, the vulnerability exploited by EternalBlue was exploited on a large scale. The WannaCry ransomware distributed itself to computers on the same network by exploiting the vulnerability. This severely affected many organisations across the globe; there was a limited impact in the Netherlands. The organisations affected include the Spanish Telefónica company, FedEx and the British National Health Service (NHS).[160] [161] The ransomware infections caused serious disruption to services in many NHS organisations is England and Scotland.[162]

Conclusion and looking ahead

The arrival of the Internet of Things (IoT) brings with it a host of opportunities and applications. However, it also provides many opportunities for cybercriminals. Insecure devices are infected to then be exploited for various attacks. This presents a limited threat to the owners of the devices. A bigger problem is that the infected devices are exploited to mount attacks on third parties, such as DDoS attacks.

Events from the previous year allow us to conclude that cybercriminals are still making extensive use of the tools that are known to exist already. Tools such as ransomware, CxO fraud and phishing continue to be very effective and lucrative. In addition to the ways in which they are known to be used, criminals are also seeking ways in which these tools can be used in a more effective and profitable manner. Attacks continue to take advantage of vulnerabilities in software that is often not updated in good time, together with manipulating users, using phishing emails for instance.

On a number of occasions researchers demonstrated that, in addition to the IoT devices already mentioned, there are vulnerabilities in industrial control systems (ICS)[163] in production environments and in computers in vehicles. It is not inconceivable that criminals will discover the vulnerabilities in these types of systems and start exploiting them to achieve their aim.

The past has taught us that security is not the prime consideration when designing new products. It is certainly the case that in recent years many organisations have considered turnover, brand recognition and market share to be more important than delivering a secure product.[164] [165] Because of this, there is an expectation that in addition to IoT devices already purchased and connected to the internet, newly designed IoT devices will contain vulnerabilities that are relatively easy to exploit.

The use of cloud services for shadow IT incurs additional risks

4 Resilience

The Netherlands is implementing more and more measures in the digital field but cannot keep pace with developments in the field of vulnerabilities. Over the last year, the Internet of Things has turned out to be particularly vulnerable. Organisations continue to choose the easiest way, but awareness is increasing.

Resilience is the degree to which measures have been implemented to reduce the vulnerability to security problems. This chapter describes the developments in the field of the measures that are being implemented and the vulnerabilities that are still exposed. The resilience of the Netherlands is covered below based on individuals, technology and organisations.

Individuals

Employees arrange online services themselves: shadow IT limits the grip on security

Organisations are increasingly becoming involved in shadow IT.[1] [166] When doing so, they use IT solutions that have not been procured via the formal route, such as hardware or online services they themselves have bought. The consequence is that the management processes are not always applied to those systems and processes. As a result, their security level cannot be managed. The use of cloud services for shadow IT incurs additional risks.

End users often need simple ways of carrying out their work. This consideration is probably the basic reason behind the increase in shadow IT. Organisations mainly cite the use of personal email, cloud services (often for file exchange) online file converters and chat apps for business purposes as points of concern.[167]

Browser developers are helping users protect themselves better
Internet browsers are implementing measures to keep users better informed. For instance, Google Chrome[168] and Mozilla Firefox[169] have announced that they will mark all websites that do not use https as being insecure. Initially, the browser makers are opting to only display the security comment when a web page on http contains a form with a password field. Eventually, the makers intend to indicate the risk on all http pages.

Although the average user may care little about this type of notification on an informative web page, this measure could encourage website owners to use https.

Marking unencrypted http traffic as insecure helps users protect themselves against communications eavesdropping. However, the use of https does not guarantee communication with the correct party. The emergence of *domain validated* certificates ensures that everyone who controls a domain name can apply for a valid certificate for that domain name. However, the user can still be misled if this is done for domain names that are similar to legitimate names.

1 Shadow IT are IT resources that are being used out of sight of the management organisation.

Technology

SMS is becoming less satisfactory for two factor authentication

In July 2016, the American National Institute of Standards and Technology (NIST) published a draft guideline in which SMS is no longer considered suitable for two factor authentication.[170] The interception of SMS messages is alleged to have become so low-threshold for attackers that NIST recommends considering alternative second factors.

An attack was detected in Asia in January 2017 where TAN codes for internet banking sent by SMS were intercepted. The attack was carried out using falsified messages in accordance with the SS7 protocol. The vulnerability of this protocol has been known for some time and is inherent in SMS traffic. In addition to intercepting SMS messages by exploiting the SS7 protocol, the capability to synchronise SMS messages across different devices poses a threat to the use of SMS for two factor authentication. Researchers have demonstrated that both Android and iOS are susceptible to attacks where received SMS messages can be accessed via the recipient's computer.[171]

Two important uses of SMS for two factor authentication in the Netherlands are ING internet banking (for TAN codes) and the government's DigiD (for login codes). Minister of the Interior and Kingdom Relations Plasterk has stated that the current DigiD authentication options are not considered secure enough for all purposes.[172] DigiD will therefore be enhanced with what is known as DigiD Substantieel, which will start rolling out in the second quarter of 2017. DigiD Substantieel requires a second factor, such as a passport or driving licence. A DigiD app has also been developed as an alternative to SMS authentication.[173]

In addition, the Idensys and iDIN pilots will be continued in 2017.[174] Both Idensys and iDIN are systems from different suppliers of authentication tools. It is comparable with iDeal for payments, where the user is given a choice of how they want to log in. Idensys and iDIN fit in with the new European legal framework of the European Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

Internet of Things is vulnerable and is being exploited

The vulnerability of the Internet of Things was manifested in the autumn of 2016 by Mirai botnets. Because the software source code of the Mirai botnet has been published, various actors distributed variants.[175] A large number of devices were infected: the infections that led to defects became apparent but this may just be the tip of the iceberg.[176] At the start of May 2017 the European Commission released a statement announcing that measures for certification to make IoT devices more 'cyber ready' will be proposed later in the year.[177]

Mirai infects devices by exploiting default passwords. The owner of a device is responsible for changing this password but experience shows that the user is unaware of the fact that the device uses a default password. Because neither the manufacturer nor the user experience the harm or the liability of reduced security directly, they have no sense of urgency to do anything about it. This leads to a lack of sustainability in IT.

Mirai botnets have been involved in extraordinarily large DDoS attacks. Defending against attacks on this scale is now only financially feasible for major parties. There is still no solution to the unwanted side-effects of the Internet of Things, so a lack of sustainability in IT will continue to be a problem. There have been calls to draw up a legal framework for product responsibility if the sector cannot regulate itself.[178]

Research by the WODC into the opportunities and threats from the Internet of Things has revealed that the poor security of IoT applications poses a threat to security and privacy. The research report named four factors that inhibit the development and use of secure and privacy-sensitive IoT applications: complexity of technology, dealing with big data and the playing field; lack of knowledge and awareness; lack of stimulus; lack of supervision and enforcement.[179]

Vulnerabilities are becoming more fundamental in nature

Suppliers have been rectifying software vulnerabilities for many years now using security updates. However, the reporting period has shown some vulnerabilities that are of a more fundamental nature and that are less easy to rectify.

In August 2016, a number of vulnerabilities in Android were announced under the name QuadRooter.[180] The vulnerabilities are in the drivers for the chip sets from the suppliers, such as the very common Qualcomm chip for WiFi. As a result of this, a patch for the higher-level Android operating system cannot rectify these vulnerabilities. The patch has to be distributed by the telephone manufacturer. Because this takes longer than a normal patch, Android users have been given some advice for mitigating measures until that time.[181]

During the reporting period, researchers at VU Amsterdam published a number of attack techniques that extend deeper than is normally the case. Dedup Est Machina,[182] published in May 2016, exploits memory duplication to take over a browser. Flip Feng Shui[183] appeared in August 2016 and in some cases allows an attacker virtual machine to affect the memory of other virtual machines. ASLR⊕Cache[184] was announced in February 2017; it can be used to circumvent the Address Space Layout Randomization (ASLR) security measure.

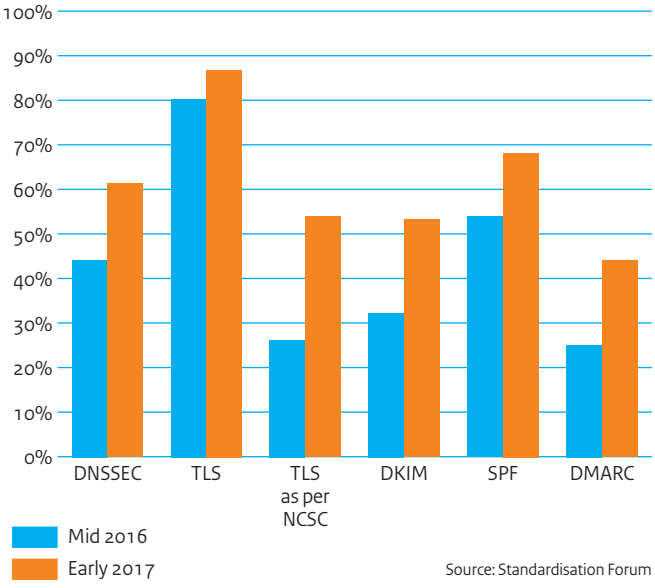
Standards to make email safer are slowly being adopted for use

The Dutch government and the business community launched a coalition for more secure email in February 2017.[185] The coalition aims to make email traffic in the Netherlands easier to secure to prevent exploitation such as eavesdropping and phishing. Email is a technology which, of itself, does not have any security measures against falsification, eavesdropping or manipulation. Applying a number of additional standards to the email delivery chain would make email traffic more secure.

The coalition wants to promote use of the SPF, DKIM, DMARC, STARTTLS with DANE and DNSSEC. Among other things, these standards should ensure that email cannot have a falsified sender address, its content cannot be changed and it cannot be read by third parties.[186] Because email is delivered by various different intermediate parties, it is important that those standards are applied by all parties. It is important that these parties adopt the standards because they account for a significant proportion of email traffic.

Research by the Standardisation Forum (Forum Standaardisatie) has revealed that the adoption of standards for making email more secure by government agencies has risen significantly in the last year.[187] There has continued to be strong growth in, among other things, the use of TLS in accordance with the IT security guidelines for TLS from NCSC,[188] DKIM and DMARC. However, ambitions are higher; the National Council (Nationaal Beraad) has stated a target of 100% adoption in 2017. This does not appear feasible based on the initial measurements.

Figure 7 **Adoption of security standards by government agencies**



Source: Standardisation Forum

Encryption is in great demand

The use of encryption is becoming increasingly popular. For example, more and more websites are using https. This is partly due to the lower costs for the necessary hardware and bandwidth and free certificates. Thanks to the Let's Encrypt initiative, certificates are free of acquisition costs and easier to use.[189]

In addition to this, there is even more media interest and awareness among end users which is increasing the demand for https. Publicity on the government's use of https has led to Minister of the Interior and Kingdom Relations Plasterk deciding to make the use of https mandatory for all government websites.[190]

Chat apps are also using end-to-end encryption. Since the time that the market leader in the Netherlands, WhatsApp, introduced it in April 2016, not having it has become inconceivable. Reports of an alleged backdoor that could circumvent the encryption in WhatsApp caused a great deal of fuss.[191] Eventually it transpired that there was no backdoor; it was functionality that prevents messages that have already been sent but not delivered getting lost if the recipient changes their phone.[192] The vulnerability continues to exist.

The disquiet caused by such reports appears to indicate that some of the end users understand the importance of encryption for all kinds of network applications. There is a growing demand for suppliers to provide it.

The increasing use of encryption also requires trust in certificate suppliers. In October 2016 Mozilla suspended trust in certification service providers WoSign and StartCom. WoSign was contravening confidentiality agreements by issuing certificates with a validity date in the past. In addition, WoSign failed to declare information about the acquisition of its competitor StartCom. Customers of WoSign and StartCom had to find a new supplier; new certificates from both companies were no longer trusted by Mozilla[193], Apple[194] and Google[195].

Encryption protects data for a limited period of time. As computers become more powerful, encryption that was once considered to be strong is seen to be cracked more easily. The arrival of quantum computers could have major consequences for data that is currently protected by strong encryption. Quantum computers work in a way that is fundamentally different to current computers and can crack the forms of encryption that are most commonly used. The NCSC has published a fact sheet on this.[196]

Organisations

Organisations don't have a tight enough grip on their suppliers' information security

Large organisations are increasingly capable of properly organising their information security with policy and procedures. However, they often use (smaller) suppliers where the level of maturity is lower. When acquiring hardware and software they often set security requirements that a product originally meets. Yet how the supplier has set up their management measures is not always clear to the purchasing party. As a result, later changes often fail to meet the security requirements.[197] This problem occurs throughout the entire chain.

Larger cloud suppliers are a positive exception to this. Because security problems at cloud suppliers have a direct impact on multiple customers at the same time, they devote serious attention to cybersecurity. The result of this is that these parties usually have compliance with their information security policy more in order and can demonstrate compliance.[198]

Reports emphasise the need for cybersecurity

An advisory report that Herna Verhagen of PostNL submitted to the government draws attention to the need for cybersecurity.[199] The report, drawn up for the Cyber Security Council, states that cybersecurity in the Netherlands must be enhanced post haste. It argues in favour of greater scope for coordinating control by the government and for stimulating the responsibility of the business community. It proposes a standard of 10 percent of the IT budget being spent on cybersecurity.

The Rathenau Institute also published a report on the resilience of the Netherlands in the cybersecurity domain.[200] Among other things, it concludes that there are market failures; there are no economic stimuli to build in cybersecurity. The Rathenau Institute recommends that the government sets a good example as awarding authority by creating sufficient capacity with supervisory bodies and security services, and by testing whether the Computer Crime III (*Computercriminaliteit III*) and modernisation of the Intelligence and Security Services Act (*Wet op de Inlichtingen- en Veiligheidsdiensten*) proposed legislation works in practice. The business community is advised to meet its duty of care and, together with the government, invest in cybersecurity training.

The Netherlands Court of Audit concluded in the State of Central Government Accounts 2016 that various ministries are not devoting sufficient attention to information security. According to the Court of Audit, administrative authorities need to devote more attention to better protecting sensitive information from citizens about a criminal past, organ donations, tax or medical information. Identity theft, hacking the system for operating bridges and locks or other critical systems must be countered more effectively. The protection and management of the financial system is still not adequate in the House of Representatives either.[201]

The government also recognises challenges at a local level. In April 2017 the Rotterdam Court of Auditors published a report stating that inadequate information security at the municipality was causing 'realistic risks of physical insecurity'. According to the Rotterdam Court of Auditors, sensitive information at the Rotterdam municipality is not in sufficiently safe hands.[202]

The Information Society and Government Study Group which was set up by the government to formulate advice to improve the functioning of the digital government published its report on 18 April.[203] It established that, at the current time safety and, specifically in the case of digitisation, cybersecurity is a growing issue requiring attention and recommended that the funding of the Generic Digital Infrastructure (GDI) be structurally guaranteed as infrastructure critical for the Netherlands.

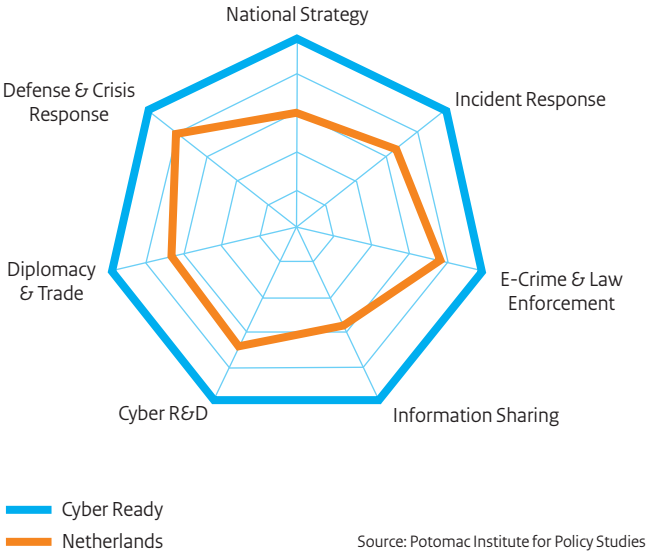
The Cyber Security Council has published a guide containing a summary of the duties of care in the cybersecurity field. The publication makes it clear that every company that uses IT has duties of care in the cybersecurity field and provides advice for fulfilling these duties.[204]

The Cyber Readiness Index indicates a lack of financial resources for cybersecurity in the Netherlands

The Cyber Readiness Index for the Netherlands from May 2017 reveals that the Netherlands has a robust cybersecurity strategy and is well on the way to enhancing digital security but is not yet fully cyber ready. The report, written by the Potomac Institute for Policy Studies, analyses Dutch policy based on 7 criteria.

The Netherlands has a clear vision, relevant strategies and ambition and is doing well in the research and innovation field. However,

Figure 8 **The Cyber Readiness Assessment for the Netherlands**



Source: Potomac Institute for Policy Studies

according to the researchers it lacks sufficient financial resources for cybersecurity. Only 0.004 percent of the gross domestic product is being spent on cybersecurity. In addition, it concludes that information sharing could be improved. The researchers see the lack of central control as an issue requiring attention because investments are being made in public-private collaboration in the cyber security field. The sharing of information from the private sector could also be encouraged more.

Elections: paper process is leading

In the Netherlands, votes are cast in the polling station using ballot papers and the ballot papers are counted manually by the electoral committee. These processes are therefore not vulnerable to cyber attacks.

Reports about possible vulnerabilities in the software (Supporting Software for Elections) which the municipalities, principal electoral committees and the Electoral Council use to process the counts from the polling station committees into the final result of the election were published in January 2017.[205] On 1 February 2017, the Minister of the Interior and Kingdom Relations therefore decided to implement measures to avoid there being a shadow of a doubt about the reliability of the result of the election.[206] The digital transfer of counting results was therefore prohibited and additional manual verification counts were added. The result of the measures that were implemented is that the paper process is leading throughout the entire chain, from casting a vote up to and including deciding the final result.

Ransomware and DDoS attacks are all in day's work for large organisations

DDoS attacks and ransomware infections are commonplace. Large organisations are affected so often that mitigation is seen to be an everyday activity.[207] Organisations often succeed in defeating DDoS attacks by investing in mitigation processes and mitigation tools.[208] Protection against large-scale attacks, like the attacks with the Mirai botnet, is difficult as they are not easily defeated. Restoring from backup after a ransomware infection has become routine for organisations which have now gained experience in doing this. Despite this, recovery operations are still expensive and time-consuming and data loss cannot always be undone.

These attacks can still disrupt smaller organisations. They lack the necessary expertise and scope for investment for DDoS mitigation and don't always have a properly functioning backup mechanism to recover from ransomware infections.[209]

Moreover, many small organisations are vulnerable because security updates are not installed in time. Research has revealed that small organisations implement relatively few measures. The measures they do implement are limited: almost all of the businesses investigated use a virus scanner but only one third, or even less, of the businesses implement other measures such as having a policy, trained personnel and recovery procedures for incidents. This is while 79 percent of the businesses say that the business processes are totally dependent on IT.

Police combating ransomware

The High Tech Crime Unit (Dutch National Police) is investigating various ransomware variants such as Locky, Shade, CTB-Locker, Torrentlocker, Cerber and Wildfire. Many Dutch citizens were affected by Wildfire in particular. Wildfire targets SMBs and is distributed by phishing emails with a malicious Word document containing macros.

The Police contained Wildfire after they located and impounded the command and control server. This server held the decryption keys for thousands of victims. Once they had secured these keys the Police, in collaboration with private parties, were able to publish a decryption tool for Wildfire. In addition, the criminal infrastructure was permanently shut down by court order. More than 20 percent of all Wildfire victims were able to recover their files with the tool. This ties in with the THTC's new approach where disruption is one of the four pillars to the approach.
The successors to Wildfire affected very few victims in the Netherlands; the malware appeared to focus on Flanders.

No more ransom
THTC, in cooperation with Europol EC3, Kaspersky Lab and Intel Security, has set up the No more ransom[II] website. This collaboration is working increasingly well and more parties are joining in. Since starting in July 2016, approximately 75,000 successful decryptions have been carried out internationally. The focus in the data for 2016 was on the Shade ransomware; its victims were mainly in Russia.

Since its introduction, the No more ransom website has been attacked more than 51,000 times and it therefore appears to be succeeding in its activities to disrupt cybercriminals and to unlock the victims' files.

II https://www.nomoreransom.org/

Conclusion and looking ahead

The government, business community, academics and citizens in the Netherlands are working hard on improving digital resilience. Nonetheless, keeping up to date with the growing vulnerability of society as a whole is a major challenge. For the time being this gap will continue if not grow.

People continue to find ease of use the most important aspect of their digital activities. In both their private and working lives they choose the quickest and easiest solution over the safest. Nevertheless, awareness is increasing: the encryption debate has featured in the news several times as a result of which the demand for encryption from end users in the form of https on websites and end-to-encryption in chat apps is greater than ever. Encryption applications for email are slower getting off the ground.

There have been unprecedented manifestations of the vulnerability of the Internet of Things. Product responsibility and product liability in this field is still not clear and the victims of exploitation are, for the time being, not the product owners themselves. As a result, no one feels that they bear ultimate responsibility leading to market failures. For now, there appears to be little prospect of change in this situation, while the number of devices connected to the internet is growing dramatically.

Organisations are becoming more aware, partly due to legislation and regulations. Large organisations have had their share of difficulties with DDoS attacks and ransomware and have therefore been forced to climb to a higher level of maturity. Nevertheless, basic measures such as installing security updates are often not implemented. Both large and small organisations are often failing to do this in a timely manner which facilitates malware infections. Small organisations are lagging behind but as suppliers to large organisations they are jointly responsible for their link in the chain. The increasing quality of commissioning in large companies and public authorities may lift their suppliers to a higher level in the future.

Costs and benefits of cybersecurity do not always lie with the same party

5 Interests

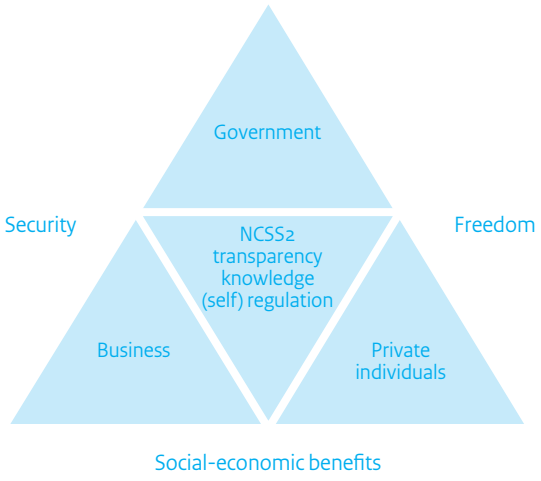
Dutch society's increasing dependence on IT and the importance of cybersecurity go hand in hand. The interests of the individual, organisations, chains and society are not always the same and the costs and benefits of cybersecurity do not always lie with the same party. As a result of the increasing importance of IT there is a demand for more clarity on the security characteristics of products and services. The government is adjusting legal frameworks to vest responsibility in market parties who fill new roles or take on existing ones. The internationalisation of IT providers affects national security interests. The control of the internet and international standards of behaviour for states in the digital field are areas of concern. There are divergent views on the responsible disclosure of vulnerabilities.

Balancing of interests

Various considerations form the basis for balance of interests

Various interests, including individual, organisational, chain and societal interests form the basis for making choices in relation to cybersecurity. They may coincide or they may be contradictory. Individuals and organisations make cost-benefit decisions on cybersecurity measures based on their own position and often in their own interest. Choices by citizens, the business community and the government affect freedom, security and societal growth where a balance must always be found.[210]

Figure 9 **Balance of interests according to National Cybersecurity Strategy 2**



Increasing dependence on IT and the importance of cybersecurity go hand in hand

Dutch society continues to be increasingly dependent on IT functioning properly. Technology facilitates efficiency improvements and improvements in effectiveness and the number of fields of application for IT is increasing continuously.

The discernibility of these fields of application varies. Digitising processes such as communication with the government and businesses affects individuals directly and is therefore apparent. The increasingly wide use of Message Box (Berichtenbox) for communication with the government is an example of this.[211] Within the EU, the Netherlands is now the front runner in the field of connectivity and the number of citizens that use the internet and have the skills to do so.[212] Another visible use relates to the integration of IT in cars which translates into (semi) autonomously driving cars and the increase in smart-home applications. Innovations in the field of energy supply[213] and agriculture[214] are, on the other hand, less apparent to the individual.

Cybersecurity, and with it the unhindered functioning of IT is increasingly a precondition for many social processes and for the further development of the digital economy.[215] This persistent trend has been highlighted a number of times in previous editions of the CSAN and is expected to continue in the coming years. The number of systems for which there is no longer an analogue alternative continues to rise. At the same time, a specific choice is being made based on the interest of individuals and society not to phase out certain analogue alternatives that shape society, such as cash.[216]

Manifestations of interests

The interests of the individual, organisations, chains and society remain constant, in a general sense and through time. Moreover, without specific context they remain abstract. Interests become more apparent and concrete, however, when they are actually affected, which often leads to reactions from the interested parties. The paragraphs below give an indication of illustrative developments in the field of interests in the reporting period for this CSAN.

Cybersecurity costs and benefits do not always lie with the same party

The interests of individuals, organisations and society as a whole sometimes differ, such as with DDoS attacks that are caused by the exploitation of poorly secured devices on the Internet of Things.[217] Users of the devices benefit from a working device and often suffer no direct damage themselves if the device is exploited. This group does not, therefore, directly benefit from investing in the security of these devices, by paying a surcharge for a more secure device or installing security updates for instance.

Because users do not demand better security within this context, suppliers do not have a direct stimulus to invest in security. On the other hand, the societal consequences and damage to third parties can be significant if the device is exploited, to mount DDoS attacks for example. The victims of these attacks will, moreover, have to make significant investments to defeat these attacks. The costs for implementing cybersecurity measures therefore fall on a party other than the party that occasions the measures.

Desire for more clarity on the security characteristics of products

In legal proceedings against Samsung, the Consumers' Association is demanding that they provide updates for at least two years after the purchase or four years after the introduction of (Android) devices.[218] In addition, the Consumers' Association is demanding that Samsung provides consumers with clear information about this. The previous edition of the CSAN observed that users set implicit quality requirements for IT in the broadest sense.

The Consumers' Association's action shows that as a result of the increasing importance of IT products, users feel a need for more explicit requirements and more transparent security characteristics. It is only then that they will be able to make a considered choice. Society also has an interest in this because without transparency products are mainly chosen based on the price and speed of introduction on the market. Greater market-wide transparency gives suppliers the opportunity to be distinctive in the security field.

Societal roles bring responsibilities with them

European legal frameworks are being adjusted to impose obligations on (new) market players. These market players are filling a new role in society, or they are partly or fully taking over the role of existing, and often regulated, players. For example, the European Commission has proposed replacing the e-Privacy directive with a regulation[219] whose scope will cover many other communications services in higher system layers, such as WhatsApp, Facebook Messenger and email providers in addition to traditional telecommunications providers.[220]

By doing so, they are trying to protect end users in a similar way and create a level playing field for suppliers.[221] The new parties are opposed to regulation while the established market parties support it.[222] In the United States it is becoming clear that such developments can work the other way too, where established parties are calling for less regulation to achieve a level playing field with the newcomers in this way.[223]

The eIDAS regulation is an example of regulating market players who fill a relatively new and important role in digital society, the so called trust services.[224] The regulation forms the legal basis for electronic signatures, seals, timestamps, documents and website certificates and the responsibilities of those who supply them.

The General Data Protection Regulation adopted on 27 April 2016 also brings new responsibilities to personal data processors, including in the field of information security and privacy-by-design.[225] The user is also given the right to obtain their personal data easily and to transfer their data to another supplier, also known as data portability. This prevents vendor lock-in, where users are tied to a single service provider.

Control of the internet transferred to a non-profit organisation

On 1 October 2016, the US government formally transferred control of essential functions of the internet from the American National Telecommunications and Information Administration to the private organisation ICANN.[III] To maintain a free and open internet, the management structure of ICANN has been set up in accordance with the multi-stakeholder model, where businesses, public authorities, technical experts and civil society are represented. This is an attempt to achieve a balanced representation of interests.[226]

The developments above tie in with the Dutch government's vision on control of the internet, also known as internet governance. In its response to reports by the Advisory Council on International Affairs (Adviesraad Internationale Vraagstukken, AIV) and the Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid, WRR) the Dutch government has stated that an open model of internet governance is crucial to the development of the internet and that self-organisation and self-regulation have played a crucial role.[227]

III The essential (IANA) functions comprise coordinating and issuing IP addresses and numbers for autonomous systems, the management of DNS root servers and management of a number of internet protocols.

Not all countries think the same way about the role of the government in controlling the internet. The underlying motives are often of a politico-economic and social nature. Examples include views on fundamental rights such as freedom of expression or economic interests relating to global digital provision of services. Russia and China are, for example, fighting for greater national control of internet infrastructure and the information that is sent using it.[228] According to these countries, states should be sovereign in the digital domain too and must therefore be able to exercise control.

This clashes with western principles on internet security. The Netherlands has also expressed views in this field. As stated in the International Cyber Strategy, the Dutch government is in favour of an open and unfragmented internet, where economic opportunities presented by global digitisation can be grasped and where fundamental rights and freedoms and security are guaranteed.[229]

Internationalisation of IT providers affects national security interests

Dutch society is increasingly dependent on IT and therefore on its suppliers too. The internationalisation of these suppliers can affect Dutch security interests. The government warns that shifting economic power relations is increasing the risk of takeovers in the telecommunications sector, partly motivated by geopolitical motives.

Due to concerns about improper political pressure from abroad and the confidentiality of communications, the government is proposing new powers for the Minister of Economic Affairs to prohibit unwanted control of a telecommunications party on the grounds of public order and national security.[230] In addition to telecommunications providers, telecommunications parties include, for example, hosting services, internet hubs, data centres, trust services and other categories of networks or services as yet to be designated pursuant to a general administrative order.

The transfer of non-telecom parties to foreign hands can also have consequences for national security, parties involved in protecting state secrets for example.[231] This could lead to requirements for additional guarantees. In addition, socio-economic interests could play a role, within the framework of hostile foreign takeovers of major Dutch companies for instance.[232] In this way, internationalisation brings along with it a clear tension between the interest of economic free trade and growth on the one hand and the safeguarding of national security on the other.

The importance of international standards of behaviour in the digital domain is increasing

In the run-up to the elections to the Dutch House of Representatives in March 2017 concerns were expressed about the possibility of the Dutch elections being influenced by digital attacks. This happened as the result of events relating to the US presidential elections. The unhindered functioning of the democratic institutions without influence from foreign powers is of great social importance.

The protection of the sovereignty of countries is an important principle in international law. The interpretation and application of international law in the digital domain is, however, not always clear. Use of the Tallinn Manual 2.0 on the Law Applicable to Cyber Operations can provide greater clarity on the interpretation of current law.[233]

The interpretation of codes of conduct can have far-reaching consequences. NATO has once again stated that a cyber attack could be the basis for invoking Article 5 (collective defence) of the North Atlantic Treaty. NATO recognises the cyber domain as the fourth domain of warfare.[234] The importance of international standards of behaviour in the digital domain is increasing.[235] Creating greater transparency and predictability on what is and is not permitted and the response permitted to this will make future conflicts more manageable.

There are divergent views on the responsible disclosure of vulnerabilities

Disclosure of vulnerabilities in IT systems, services, and hardware and software products can have a major impact. Coordinated vulnerability disclosure or responsible disclosure is therefore a topic which is receiving a great deal of attention.[236] On the one hand, disclosures ensure that the parties responsible can resolve the vulnerabilities and that users can implement countermeasures. On the other hand, disclosures could allow malicious parties to exploit the vulnerabilities sooner.

The length of time after which the discoverer makes a vulnerability public is a sore point.[IV] For instance, during the reporting period Google's Project Zero published a number of vulnerabilities in Microsoft products before a patch was available.[237] In accordance with Google Project Zero policy, automatic publication occurred 90 days after the vulnerability was discovered. This could damage the interests of users in the short term because malicious parties could exploit the vulnerabilities. Google claims that it wants to improve the industry's speed of reaction with this, which will eventually benefit all users and society.[238]

Another sore point is the wording of a suspected vulnerability. In response to a report, the New York Times tweeted that the intelligence services could circumvent the encryption of WhatsApp, Signal and Telegram but this turned out to be an over-simplification.[239] Media reports can, on the one hand, make an important contribution to awareness of cybersecurity but on the other hand insufficiently accurate reporting can lead to overreaction by society which could result in a decrease in trust in IT (services). It is therefore up to media companies and individual journalists to strike the balance between the importance of an

IV The NCSC's Responsible Disclosure Guideline uses a standard period of 60 days.

inviting and therefore much-read story and introducing the necessary nuance. The increasing interest and publicity surrounding technological vulnerabilities has already been noted previously in the CSAN.[240]

Conclusion and looking ahead

Cybersecurity is a precondition for the proper functioning of social processes and the further development of the digital economy. Individual, organisational, chain and societal interests, which can sometimes be contradictory, play a role in topics that affect cybersecurity. Individuals and organisations make cost-benefit decisions on cybersecurity measures based on their own position and often in their own interest.

Costs and benefits do not always lie with the same party and there is desire for more clarity on the security characteristics of products to allow a considered choice to be made when purchasing. We expect that the call for (government) intervention will increase if poorly secured devices that are connected to the internet disrupt the provision of services via the internet more frequently or on larger scales. Legal frameworks are being adjusted to have the responsibilities of market parties align with the role that they play in society.

The management and national control of the internet and the underlying infrastructure are important topics for discussion, as are international standards of behaviour for states in the digital field. We expect that these discussions will take place more intensively in the coming year, particularly if geopolitical tensions rise.

There are divergent views on the responsible disclosure of vulnerabilities, including on the length of time before publication and the wording used in reports of vulnerabilities. We do not expect that the lack of consensus on this will disappear or that the intense publicity interest in technological vulnerabilities will decrease in the short term.

Appendices

Appendix 1 NCSC statistics

This appendix offers a summary of the responsible disclosure reports, security advisories and incidents that have been handled by the NCSC. The NCSC keeps a record of incidents using a registration system. This system is the source for all of the graphs in this appendix. This year, the NCSC has dealt with almost the same number of incidents and has written four percent more new security advisories than the year before. Although the number of incidents dealt with has hardly changed in relation to last year, the spread across the types of incidents has changed.

The NCSC facilitates the making and processing of responsible disclosure (RD) reports for both its own infrastructure and that of the central government and several private parties. It issues security advisories for its participants and deals with cybersecurity incidents. For this reporting period (May 2016 to April 2017) statistics have been calculated that are presented below. Comparing these statistics to previous reporting periods, allows trends and developments to be revealed.

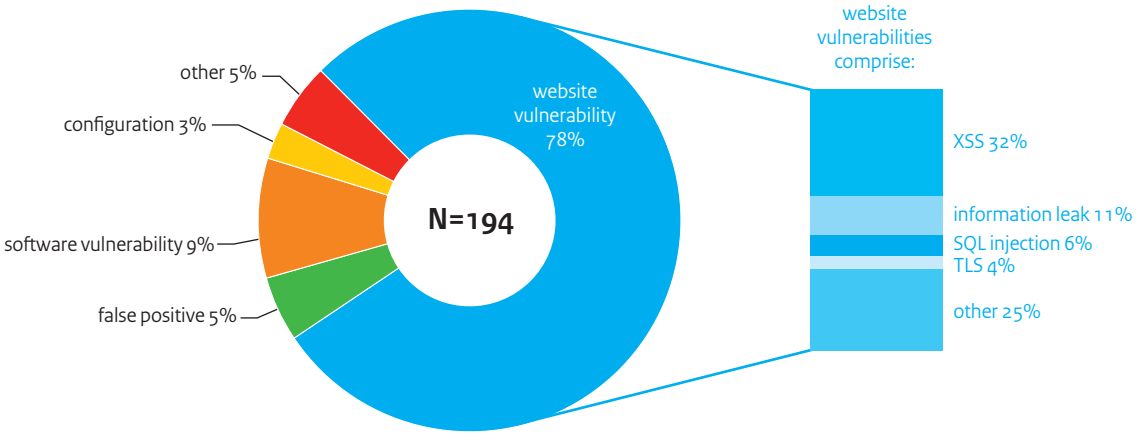
Responsible disclosure

During the reporting period, the NCSC received 194 RD reports. These concerned reports for its own systems as well as for other government systems and systems of private parties. In some cases, double reports are filed if, for example, two or more researchers report the same vulnerability. As a result, the total number of reports is not representative of the total number of vulnerabilities.

There were 113 reports last year. This means that 70 percent more reports were made last year. The increase can be explained in part by the expansion of NCSC's role as the RD point of contact for the central government.

In 5 percent of all reports, further research showed that there was no vulnerability or that it concerned an accepted risk. An example of this is the login page on a website that has no specific measures against brute-force attacks. These cases were classified as false positives. In the previous year, this concerned 20 percent of all notifications. This decrease can be explained in part by the increasing maturity of this process, particularly on the side of the reporter.

Figure 10 **Types of vulnerabilities in responsible disclosure reports**



Source: NCSC

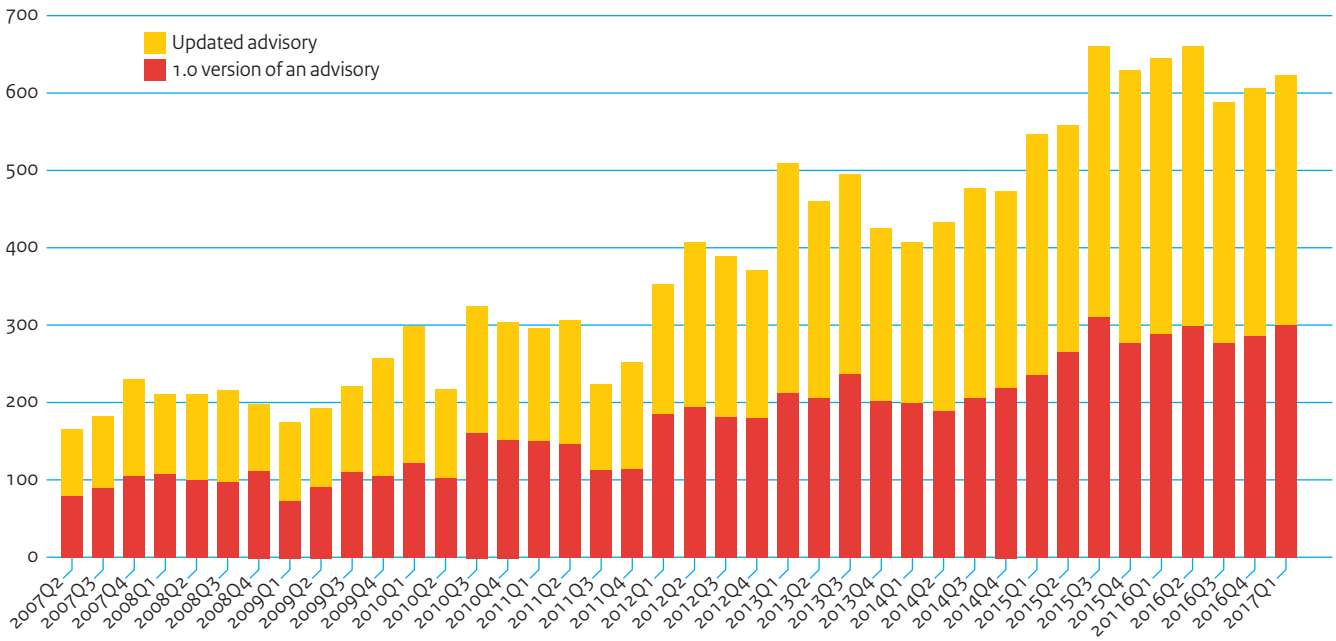
Figure 10 shows the different types of vulnerabilities that were reported. The majority (78 percent) of all reports concern a vulnerability in a website, a web application or infrastructure on which web applications run. Examples of such reports are weak TLS parameters, cross-site scripting (XSS), SQL injection and information leaks. An example of the latter is a vulnerability through which it is possible to see a configuration file or a version number of a web application. Nine percent of all reports concern vulnerabilities in software (excluding web servers and web applications). Relatively few reports (3 percent) concern configuration errors in hardware and software.

Security advisories

The NCSC publishes security advisories for software vulnerabilities or perceived threats. A security advisory describes what is going on, what systems may have been affected and what should be done to prevent an organisation becoming a victim. Figure 11 shows the number of advisories that the NCSC published per quarter between the second quarter of 2007 and the first quarter of 2017. Here, a distinction is made between new advisories (with version number 1.0) and updates of existing advisories. In total, the NCSC published 1179 new security advisories over the reporting period. This is about 4 percent more than the year before. The number of updates to existing advisories also rose slightly to 1336. This is an increase of approximately 1 percent.

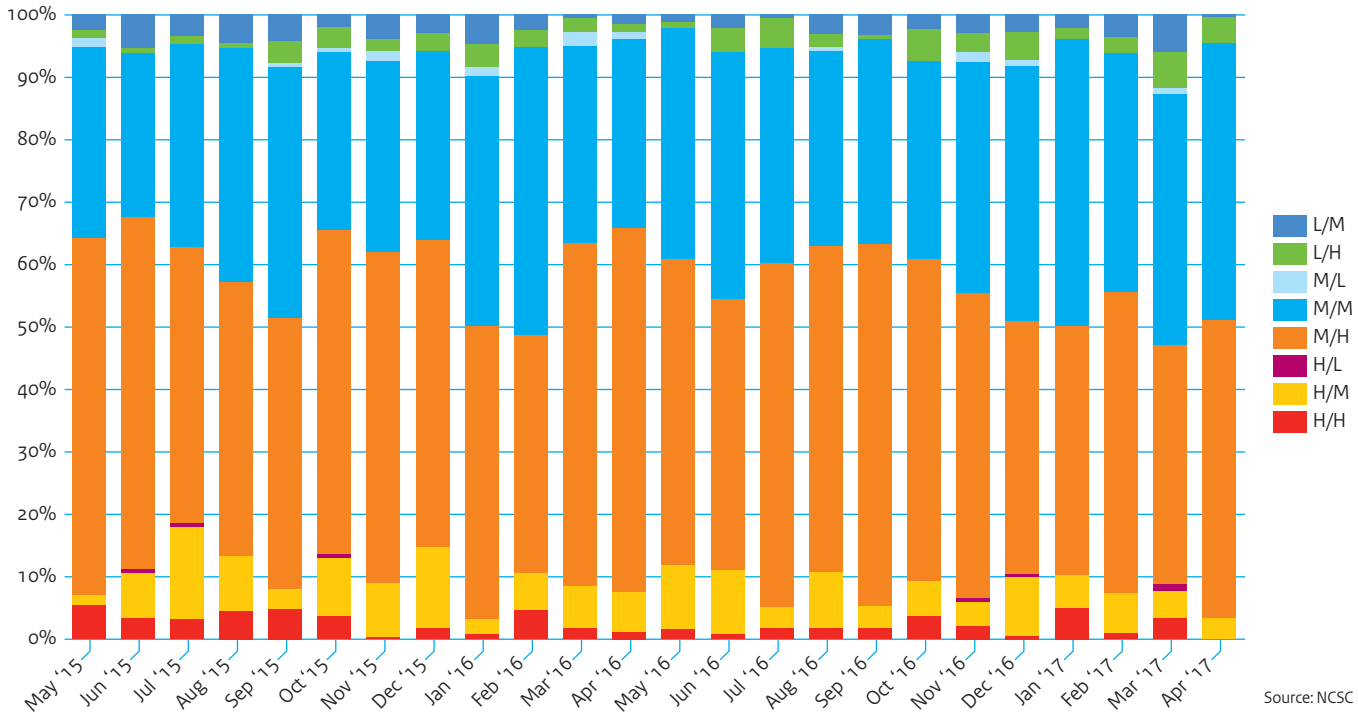
The NCSC security advisories are classified according to two elements. Firstly, it determines the likelihood that the vulnerability will be exploited. Secondly, the NCSC determines the damage that occurs when the vulnerability is exploited. Thus, the classification has two criteria: likelihood and damage. A level is estimated for both criteria based on a number of different aspects: High (H), Medium (M) or Low (L). If there is a high probability, for example, that a particular vulnerability will be exploited, but the expected damage caused by the exploitation is low, the corresponding security advisory will be classified as H/L. Figure 12 shows the relationships between these levels for all published advisories (including updates) per month for the past two reporting periods.

Figure 11 **Number of advisories per quarter (Q2 2007 – Q1 2017)**



Source: NCSC

Figure 12 **Classification of advisories per month (May 2015 – April 2017)**



Source: NCSC

Damage from vulnerabilities

Every security advisory comes with a description of the possible damage that malicious parties could inflict if the advisory is not followed-up on. Table 2 shows the percentage of advisories per damage description for the past three reporting periods. Here we can see that security advisories related to denial of service (DoS) still appear to have the largest proportion (61 percent), followed by remote code execution with user rights (42 percent), access to sensitive data (32 percent), escalation of privileges (19 percent) and bypassing a security measure (17 percent). These were also the most common security advisories in the previous reporting period. An advisory often comes with several damage descriptions. This gives rise to a total percentage higher than 100 percent.

Table 2 **Damage description in security advisories in CSAN 2015 up to and including CSAN 2017**

Damage description	2015	2016	2017
Denial of Service (DoS)	51%	56%	61%
Remote code execution (user privileges)	29%	37%	42%
Access to sensitive data	26%	32%	32%
Privilege escalation	14%	21%	19%
Security bypass	19%	25%	17%
Access to system data	9%	13%	13%
Manipulation of data	5%	8%	10%
Cross-site scripting (XSS)	6%	9%	8%
Remote code execution (administrator/root privileges)	4%	6%	7%
Spoofing	2%	5%	5%
Authentication bypass	4%	5%	3%
Cross-Site Request Forgery (XSRF)	1%	2%	2%
SQL injection	1%	2%	1%

Cybersecurity incidents registered with the NCSC

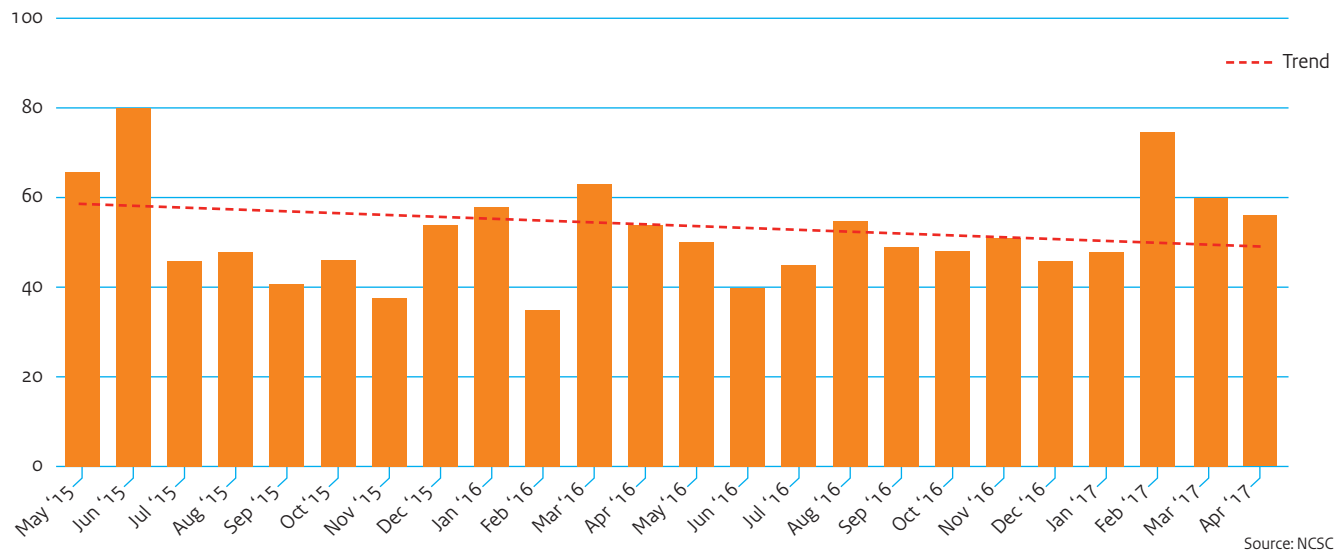
Cybersecurity incidents registered with the NCSC
The NCSC assists governmental departments and critical infrastructure organisations in the handling of IT security incidents. In this role, the NCSC receives reports of incidents and vulnerabilities and also identifies incidents and vulnerabilities itself, for example on the basis of various different detection mechanisms. At the request of national and international parties, the NCSC supports Dutch internet service providers in the fight against cyber incidents that originate from a malicious web server in the Netherlands, for example, or from infected PCs in the Netherlands.

Number of incidents handled

Figure 13 shows the number of incidents handled per month (excluding automated checks) for the last two reporting periods. In the previous reporting period, a total of 629 incidents were reported: an average of 52 per month. In this reporting period, 623 incidents were reported: approximately 52 per month. In broad outline, the number of (reported) incidents remains constant.

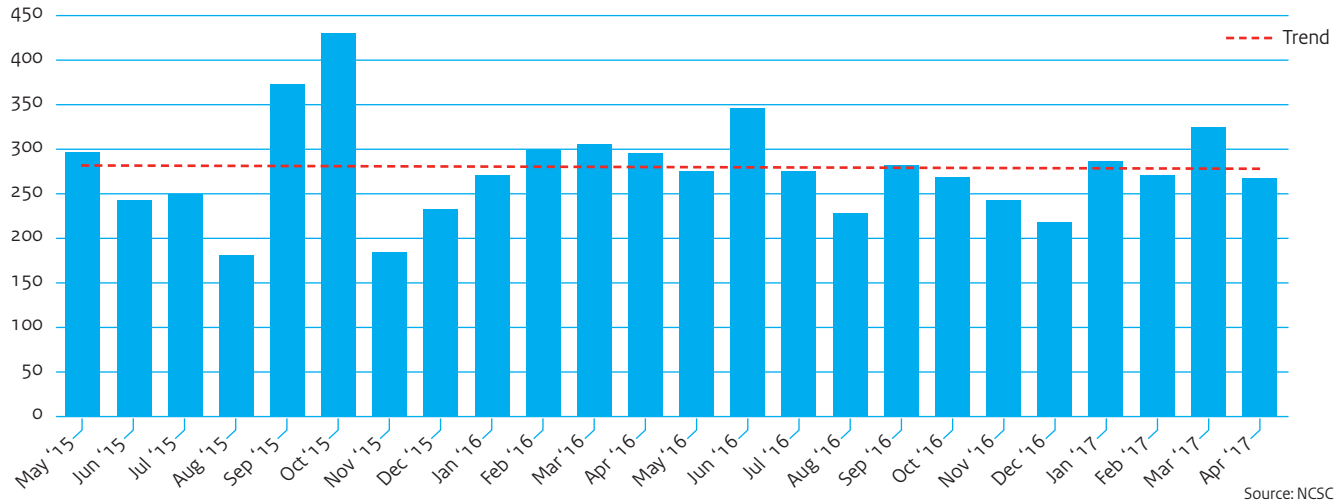
Figure 14 shows the results of automated checks for the last two reporting periods. This shows that, in the past reporting period there were, on average, 275 incident reports per month on the basis of this automation. In the previous reporting period, there was an average of 280 reports per month. A report may concern several infected systems within an organisation.

Figure 13 **Incidents handled (excluding automated checks)**



Source: NCSC

Figure 14 **Automated checks**



Source: NCSC

Distribution of incidents per report, category and handling

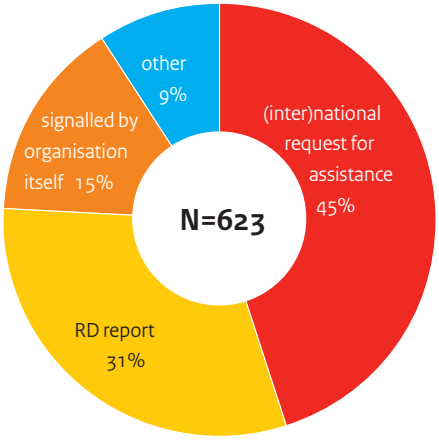
Figure 15 shows the distribution of incidents according to reporting type. This shows how an incident was reported to NCSC. Most of the incident reports (45 percent) come from outside: from national or international organisations. In 31 percent of all incidents, the incident is reported through responsible disclosure. In 15 percent of all cases, it concerns signalling by the organisation itself. Examples include a warning from one's own detection mechanism or a message from a public source. The remaining 9 percent of the reports concern various other reports or information that was accepted as a notification.

Compared with the previous reporting period, the percentage of RD reports has risen sharply, from 18 percent to 31 percent. One possible explanation of this increasing number is the expansion of NCSC's role as the RD point of contact for the central government. The percentage of national or international requests for assistance has, however, decreased since the previous reporting period: from 57 percent to 45 percent.

Figure 16 shows the distribution of incidents per category. The NCSC has used the incident taxonomy proposed by CERT.PT and ENISA for this distribution.[v] The inner ring shows the main categories while the outer ring shows the subcategories. This shows that incidents during which information was gathered made up more than a quarter (26 percent) of all incidents. The vast majority of these were phishing incidents; this also includes email fraud. Malware incidents were responsible for 18 percent of all incidents. The majority of these related to malware infections. Seventeen percent of all incidents related to unauthorised access or exploitation of a vulnerability. (Attempted) intrusions made up 16 percent of all incidents. This mainly involved the compromising of an account. Only 6 percent of incidents related to availability. Almost all of these incidents were related to Denial of Service (DoS) attacks or threats. The remainder (8 percent) was due to various incidents, including fraud or sending spam.

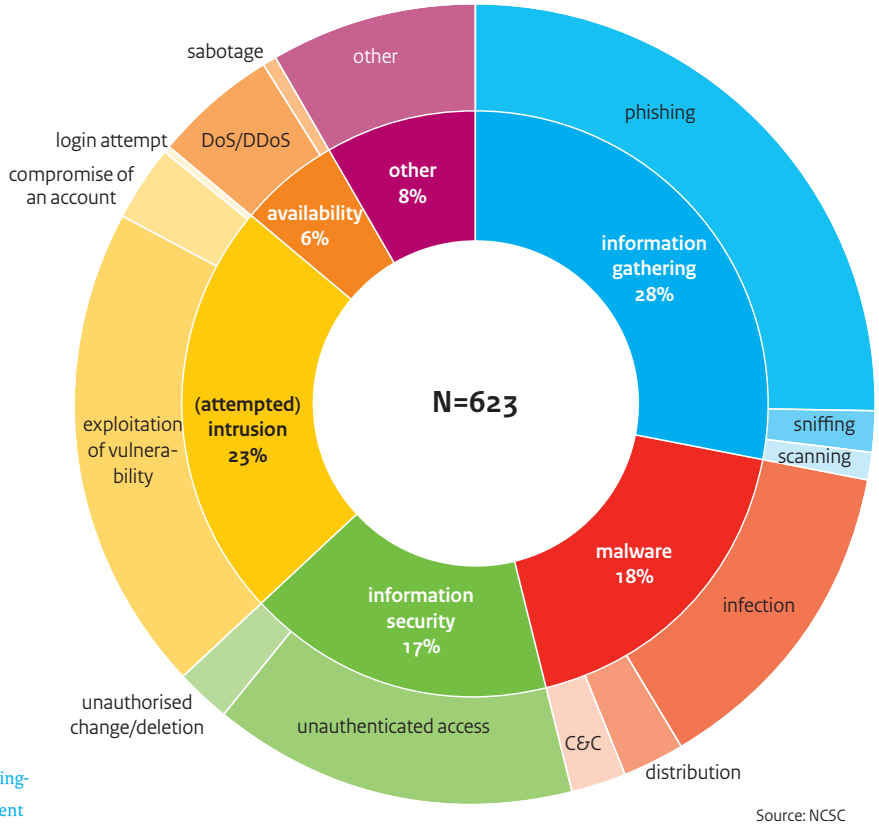
Compared with the distribution of incidents in the preceding reporting period we can see an increase in the exploitation of vulnerabilities at the expense of malware incidents. This increase can be partly explained by the large number of RD reports falling into this category. In addition, an increasing number of malware reports are automated which means they are not counted as incidents but as automatic checks.

Figure 15 **Incidents handled per reporting type**



Source: NCSC

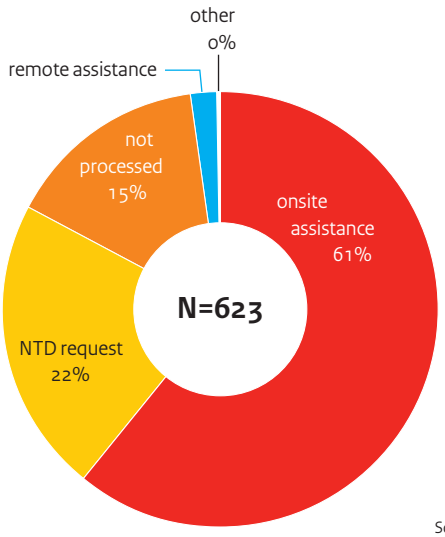
Figure 16 **Incidents handled per category**



Source: NCSC

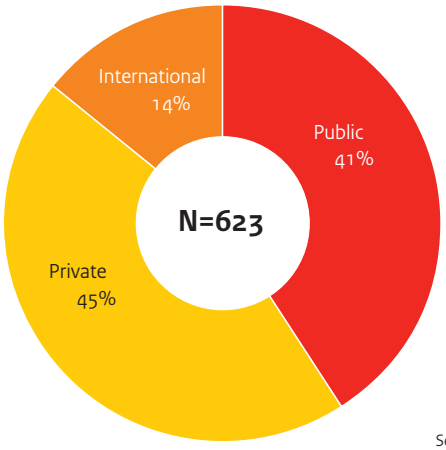
v https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

Figure 17 **Incidents handled, by handling**



Source: NCSC

Figure 18 **Incidents handled per month per type of organisation**



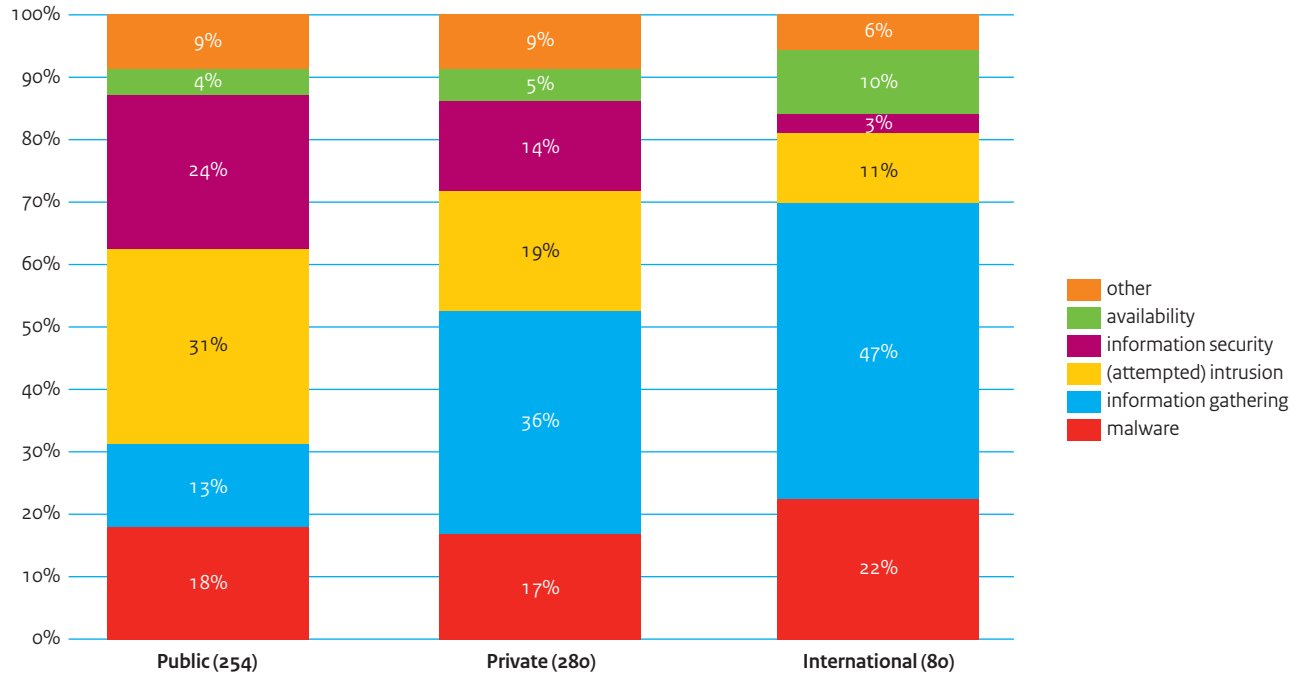
Source: NCSC

Figure 17 gives the distribution of incidents by handling. Incident handling is independent of how the report was received or in which category the incident falls, and the figure only looks at the actions that were carried out. The NCSC provided remote support in 61 percent of all incidents. In 22 percent of all incidents, the NCSC issued a 'notice-and-take-down' (NTD) request. This is done, for example, if a malicious website must be taken off-line. If an incident turns out to be a false positive, or if information is accepted as a notification, the incident is registered as not having been processed. The NCSC only provided on-site support in a few cases (2 percent). In broad outline, these ratios are the same as in the previous reporting period.

Division of incidents between government and critical sectors

The NCSC supports both the central government and the critical infrastructure in security incidents. In addition, the NCSC acts as a point of contact for international requests for assistance concerning information security. Figure 18 shows the distribution of the number of incidents handled, divided into public, private and international parties. A total of approximately 41 percent of the incidents involved a public organisation. Forty-five percent involved a private organisation. The remaining 14 percent involved an international party. An example of this is the receipt of a malware report from the national CSIRT of another country. A foreign organisation can also ask the NCSC to take a malicious website, which is hosted in the Netherlands, off-line.

Figure 19 Incident categories per type of organisation



Source: NCSC

Figure 19 shows the distribution between incident categories per type of organisation. The bottom of each column shows the type of organisation the distribution concerns and the number of incidents it represents.

Incidents involving malware are responsible for about 20 percent of all incidents, regardless of the type of organisation. With incidents under the category 'gathering of information', the difference is even greater. Forty-seven percent of all cases involving an international party fall into this category. In practice, most of these incidents concern phishing campaigns. This figure also shows that (attempted) intrusion occurs more frequently in incidents in the public sector (31 percent) than with a private party (19 percent) or an international party (11 percent).

A similar distribution can also be seen with incidents involving 'information security'. Such incidents are often related to unauthorised access to sensitive information or systems. An example of this is the reporting of a website vulnerability that allows an attacker to view a customer base. With incidents involving an attack on the availability of an organisation, there is a clearer difference between international organisations (10 percent) and the rest (4 to 5 percent).

Appendix 2 Sectoral assessment of cybersecurity

In the drafting of the CSAN, discussion sessions were held with representatives of Dutch organisations within the critical infrastructure and other sectors. These meetings have helped in shaping the analyses included in this CSAN and to substantiate insights. This appendix represents the picture outlined by these representatives during the meetings.

Sector	Manifestations	Threats: actors
Drinking water supply	In the last year, the drinking water sector has had to contend with ransomware infections and phishing attacks in the office automation environment.	The main threat detected by the drinking water sector came from professional criminals working for financial gain.
Energy	The sector has been greatly affected by ransomware infections over the last year. It has also suffered data breaches.	Professional criminals were the most significant threat.
Financial sector	The sector has mainly been confronted with fraud using debit cards sent by mail. A limited number of banks have been affected by successful phishing attacks. There have been DDoS attacks but they do not affect the sector severely.	Professional criminals are the main threat to the sector because of the financial gain they are seeking. Other actors may pose a threat, such as script kiddies in the case of DDoS attacks, but who carries out those attacks in not clear.

Threats: tools	Resilience	Interests
In a number of cyber campaigns, the (trusted) email addresses of suppliers were misused to misappropriate user details (phishing) or to infect them with ransomware.	Poor knowledge of security at suppliers sometimes leads to reduced resilience. Large (cloud) suppliers can reduce the risks provided they have sufficient knowledge. In the technological field, more measures will have to be implemented and more attention devoted to detection and prevention.	The drinking water supply is of vital importance to public health and to the functioning of society. Loss of supply will result in social disruption. These interests are stable.
The energy sector has been greatly affected by attempted CxO fraud, the distribution of ransomware and phishing attacks. In addition, the sector sees the development of ransomware for industrial systems (such as PLCs) as a (future) threat.	The dependence on suppliers is also seen as a risk; there is a feeling that this reduces resilience. A joint policy is being developed for protecting industrial systems, such as monitoring and network segmentation.	One interest in developments in the field of big data (both within and outside of the energy sector) is the wide availability of data for analysis, which often conflicts with other interests such as those of the individuals whose data is being gathered.
Ransomware has been detected; it does not appear to be specifically aimed at the financial sector. In addition, there are many instances of phishing with the aim of gathering information.	The possibility of attackers intercepting SMS messages for transactions is seen as a vulnerability, just like the possibility of using overlay apps to intercept users' data and possibly manipulate it. In addition, differences in expectations by organisations and suppliers reduce resilience. Organisations are implementing more measures themselves, such as enhanced monitoring, greater use of the four-eyes principle and participating in the secure email coalition.	The PSD2 directive, where institutions must share data with third parties when requested to do so by customers, is a development that provides opportunities but the risks inherent in this are also recognised: it is in the institution's interest that the data is secure with the third party too. Incidents can reflect badly on the institutions.

Sector	Manifestations	Threats: actors
Flood defences and surface water management	The sector has dealt with ransomware infections at a number of organisations, spear phishing based on the LinkedIn data breach, CxO fraud and a limited number of data breaches.	In addition to professional criminals, disgruntled employees also sometimes pose a threat.
Managed Service Providers	Many cases of CxO fraud/invoicing fraud have been detected over the last year. In addition to banks, DDoS attacks on the sector's clients are focusing more on the retail trade.	Professional criminals are becoming more sophisticated. This group is the most prominent because of the financial gain motive.
Nuclear	There has been a discernible increase in phishing attacks. In addition, the sector has dealt with ransomware infections and fake invoices.	State actors, professional criminals and internal actors are a threat to the sector.
Central government	This sector is coping with DDoS attacks, phishing attacks and ransomware infections.	State actors and professional criminals are major threats to central government. Furthermore, internal actors form an (often unwitting) threat.
Telecom	The telecom sector continues to be affected by DDoS attacks and CxO fraud. In addition, power failures have caused disruption in the provision of service.	The main threats to the sector are professional criminals, state actors and an organisation's own employees or those of resellers committing fraud.

Threats: tools	Resilience	Interests
The sector sees a threat from specific ransomware variants, malware specifically for embedded devices and the exploitation of other parties as a stepping-stone to gain access.	There is strong dependence on other parties which can limit the ability to influence resilience. Linking office automation to process automation is presenting new challenges. A sectoral CERT has been set up within the chain. On a technological front, micro-segmentation is being used and measures are being implemented in the field of asset management and whitelisting.	Far-reaching digitisation and the need to communicate more directly with citizens presents challenges. Links between process automation and office automation require proper measures.
Bank websites are copied to allow phishing activities to succeed. Tools are readily available to hacktivists, among others; these tools have become cheaper and more easily accessible. Many parties are capable of mounting DDoS attacks and a number of parties can mount large attacks.	The use of consumer services for business purposes, being manifested in the form of shadow IT, leads to situations that are not supported in the business community and which do not, therefore, have the right level of protection. Dealing with attacks perpetrated using certain techniques, such as ransomware and DDoS attacks has, by and large, become business as usual.	Privacy guidelines ensure customers devote additional attention to security.
CxO fraud, fake invoices and ransomware are seen as a threat.	The increasing desire to work remotely and the use of shadow IT sometimes results in reduced resilience. Tightening-up measures, awareness sessions and network segmentation are being used to increase resilience.	Given the external security aspects in the sector, nuclear security is of vital importance. IT supports the primary process.
There are large amounts of CxO fraud and phishing based on leaked information. Spear phishing attacks are mounted based on good profiles.	Patching middleware continues to be a challenge; just as with appliances, vulnerabilities here are often invisible. Https traffic ensures that measures have to be implemented at endpoints. Privacy is sometimes a more important consideration than security. Monitoring is extensive, which is making previously unknown problems clear, allowing them to be resolved.	Dependence on digital tools continues to grow. Chain dependencies ensure that third parties must implement security requirements.
In addition to existing tools, the Internet of Things is seen as a possible tool for threats. Attacks targeting humans (e.g. phishing) are seen increasingly frequently.	Human beings are the greatest vulnerability, particularly in the case of phishing and CxO fraud. The way in which the SS7 protocol has been set up could endanger the integrity of the network. Organisations are sharing knowledge in the cybersecurity field. In addition, they are cooperating in the area of exercises.	Over-the-top services depend on the organisations' networks.

Sector	Manifestations	Threats: actors
Transport (port, airport, rail)	The transport sector has dealt with incidents where banking details were changed, possibly after a supplier's mail server was hacked. Attackers masqueraded as organisations and may have stolen money in this way. Names and other details of employers have been exploited to complete transactions.	Professional criminals are the main threat to the sector. In addition, politically motivated activists, state actors and employees are a threat.
Insurers	A significant increase in ransomware, arriving in (phishing) emails sent by criminals has been detected over the last year. The sector is highly susceptible to data leaks because of its intensive data-processing nature. These are primarily caused by the unwitting actions of users. In addition, the sector suffered a limited number of DDoS attacks.	The main actors for insurers are professional criminals, who have focused more on financial gain than destruction over the last year. Employees commit human error. In addition, mistakes by chain partners and software suppliers form a threat.
Healthcare	The healthcare sector has had to deal with ransomware infections, social engineering by phone and phishing emails, and malware infections from drive-by downloads.	Professional criminals are seen to be the biggest threat. Internal employees continue to be an important group due to the possibility of them (unwittingly) leaking information.

Threats: tools	Resilience	Interests
Over the last year, many (spear) phishing attacks using data from data leaked from third parties, attempted defacements, CxO fraud and ransomware were detected.	The interwovenness of work and private life presents problems. In addition, organisations are heavily dependent on suppliers for industrial systems and IoT: the state of their security is unclear. The sector implements many measures to prevent incidents, such as working on combating phishing in the organisation's name, preventively blocking online advertisements and forming a coalition of suppliers to improve security.	Privacy guidelines ensure attention to cybersecurity on the one hand, but on the other hand they expose the shortage of resources to resolve the problem.
Over the last year, insurers have dealt with cases of fraud, ransomware, phishing, DDoS attacks and malvertising.	Shadow IT continues to be a problem in the insurance sector: individual employees are acquiring cloud services to accelerate their own work processes. Confidentiality is an area for concern because data ends up outside of the organisation's management. Ensuring cybersecurity in agile work processes is seen as a challenge.	Within the sector, the use of portals for information exchange and communications present a challenge. The relative balance between customer ease and security has to be sought constantly here. Big data is a challenge: linking information sources delivers efficient processes, where account has to be taken of (tightened) privacy legislation.
More ransomware has been detected over the last year, both targeted and random. In addition, phishing is common, usually based on publicly available data (e.g. from public websites or from datasets from the previous hacking of third parties). Cases of attempted CxO fraud, based on known details, have also been identified.	The human being remains the weak link. It is still not easy to determine the sender of emails which makes organisations vulnerable. There is little grip on the security of eHealth systems, people have to rely on suppliers for this. There is also major reliance on the suppliers in the case of cloud services. A start has been made on Healthcare-CERT to increase resilience. Some organisations implement technical measures such as blocking personal email to prevent infections by that route. Joint exercises are held, systems are set up to share files between organisations securely.	There is a great deal of cooperation in the healthcare sector, including with municipalities recently. Municipalities have been assigned numerous healthcare tasks and they request all kinds of information for this. Sometimes there is no legal basis for requesting and processing that information.

Appendix 3 Terms and abbreviations

o-day	See Zero-day vulnerability.
AIVD	General Intelligence and Security Service
Attack	The CSAN defines a digital attack as a series of actions targeted at information systems, where the availability, integrity or confidentiality of the information is affected.
Authentication	Authentication means finding out whether the proof of identity of a user, computer or application complies with the authenticity characteristics agreed in advance.
BGP hijack	Border Gateway Protocol is a protocol used by network equipment to tell each other which addresses and address blocks are available through them. A BGP hijack is an attack technique where internet traffic is diverted to communicate with neighbouring network equipment by false BGP messages.
Bitcoin	A currency, see cryptocurrency.
Bot/Botnet	A bot is an infected computer that can be operated remotely with malicious intent. A botnet is a collection of such infected computers that can be operated centrally. Botnets form the infrastructure of many types of internet crime.
Certificate	A certificate is a file that serves as a digital identification of a person or system. It also includes PKI keys used to encrypt data during transmission. A familiar application of certificates is an https-secured website.
Certificate authority	A certificate authority (CA) in a PKI system is an organisation that is trusted to generate, issue and withdraw certificates.
Cloud	A model for system architecture based on the internet where software and storage space is provided as an online service.
Confidentiality	A quality characteristic of data in the context of information security. Confidentiality can be defined as a situation in which data may only be accessed by someone with the authorisation to do so. This is determined by the owner of the data.
Cryptocurrency	An umbrella term for digital currencies whereby cryptographic calculations are used as an authenticity feature and for transactions. The bitcoin is the most common cryptocurrency.
CxO fraud	A type of fraud wherein a criminal poses as a director (CEO or CFO) of an organisation, specifically focusing on a financial officer of that organisation, to carry out a rogue transaction outside the procedures.
Cybercrime	Form of crime aimed at an IT system or the information processed by this IT system.

Cybercrime-as-a-service	Cybercrime-as-a-service is a method used in the underground economy in which criminals without technical knowledge can use the (paid) services of others to commit cybercrime.
Cybercriminal	Actors who commit cybercrime professionally, the main aim of which is monetary gain. The CSAN differentiates among the following groups of cybercriminals: • in a strict sense, those who carry out attacks themselves (or threaten to do so) for monetary gain; • criminal cyber service providers, those who offer services and tools through which or with which others can carry out cyber attacks; • cyber dealers or service providers for stolen information; • criminals who use cyber attacks for traditional crime.
Cyber researcher	An actor who goes in search of vulnerabilities and/or breaks into IT environments in order to expose weaknesses in the security.
Cybersecurity	The state of being free of danger or damage caused by a disruption or failure of IT or through the abuse of IT. The danger or damage caused by abuse, disruption or failure may comprise a limitation of the availability and reliability of the IT, violation of the confidentiality of information stored in IT environments or damage to the integrity of that information.
DANE	DNS-based Authentication of Named Entities is a protocol that allows certificates to be tied to domain names using DNSSEC.
Data breach	The intentional or unintentional release of confidential data.
DDoS	Distributed Denial of Service is the name of a type of DoS whereby a particular service (for example a website) is made inaccessible by bombarding it with heavy network traffic from a large number of different sources.
Defacement	A defacement is the replacement of a web page with a message that it has been hacked, possibly with additional messages of an activist, idealist or repugnant nature.
DigiD	The digital identity of Dutch citizens, used to identify and authenticate themselves on government websites. It allows government agencies to ascertain whether they are actually dealing with the individual in question.
DKIM	DomainKeys Identified Mail is a protocol that allows for the sending mail server to place digital signatures in legitimate emails. The owner of the sending domain publishes legitimate keys in a DNS record.
DMARC	Domain-based Message Authentication, Reporting and Conformance is a protocol used by the owner of a domain to state what needs to be done with non-authentic emails from their domain. The authenticity of emails will initially be determined on the basis of SPF and DKIM. The domain owner publishes the desired policy in a DNS record.
DNS	The Domain Name System (DNS) links internet domain names to IP addresses and vice versa. For example, the website 'www.ncsc.nl' represents IP address '159.46.193.36'.
DNSSEC	DNS Security Extensions (DNSSEC) is an extension to DNS with extra authenticity and integrity monitoring.
DoS	Denial of Service is the name for a type of attack that makes a particular service (for example a website) inaccessible to the customary users of that service. Websites are usually attacked by a DDoS attack.
Encryption	Encoding information to make it unreadable for unauthorised persons.

Exploit	Software, data or a series of commands that exploit a hardware or software vulnerability for the purpose of creating undesired functions and/or behaviour.
Exploit kit	A tool used by an actor to set up an attack by choosing from ready-made exploits, in combination with desired effects and method of infection.
Hacker/Hacking	The most conventional definition for a hacker (and the one used in this document) is someone who attempts to break into computer systems with malicious intent. Originally, the term 'hacker' was used to denote someone using technology (including software) in unconventional ways, usually with the objective of circumventing limitations or achieving unexpected effects.
Hacktivist	Contraction of the words hacker and activist: individuals or groups who mount activist digital attacks motivated by a certain ideology.
ICANN	The Internet Corporation for Assigned Names and Numbers (ICANN) is an organisation that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the internet.
ICS	Industrial Control Systems (ICS) are measurement and control systems used, for example, to control industrial processes or building management systems. ICSs collect and process measurement and control signals from sensors in physical systems and control the corresponding machines or devices.
Identify theft	The abuse of someone else's identity data to commit fraud.
Incident	An incident is an IT disruption that limits or eliminates the expected availability of services, and/or the unauthorised publication, acquisition and/or modification of information.
Information security	The process of establishing the required quality of information (systems) in terms of confidentiality, availability, integrity, irrefutability and verifiability, as well as implementing, maintaining and monitoring a coherent set of corresponding security measures (physical, organisational and logical).
Integrity	A quality characteristic for data, an object or service in the context of (information) security. This is synonymous with reliability. Reliable data is correct (legitimacy), complete (not too much and not too little), prompt (on time) and authorised (edited by a person who is authorised to do so).
Internal actor	An individual or a group in an organisation causing cybersecurity incidents from within.
IoT	The phenomenon in which the internet is not only used to grant users access to websites, email and the like, but also to connect devices that use the internet for functional communication.
IP	The Internet Protocol (IP) handles the addressing of data packages so that they arrive at their intended destination.
ISAC	An Information Sharing and Analysis Centre (ISAC) is an alliance between organisations to facilitate the exchange of (threat-related) information and joint resistance. The NCSC facilitates several ISACs for organisations in the critical infrastructure in the Netherlands.
Malvertising	The spreading of malware by offering it to an advertising broker, for the purpose of infecting large groups of users via legitimate websites.
Malware	Contraction of malicious software. Malware is currently used as a generic term for viruses, worms and Trojans, amongst other things.

MIVD	Military Intelligence and Security Service
NCTV	National Coordinator for Security and Counterterrorism
NDN	The National Detection Network (NDN) is a platform for the mutual exchange of indicators of exploitation by member organisations. Members can use these indicators to identify threats on their own networks.
NHTCU	National High Tech Crime Unit (Dutch National Police).
Patch	A patch may comprise repair software or contain changes that are directly implemented in a program with the purpose of repairing or improving it.
Phishing	An umbrella term for digital activities with the object of tricking people into giving up their personal data. This personal data can be used for criminal activities such as credit card fraud and identity theft.
PKI	A Public Key Infrastructure (PKI) is a set of organisational and technical resources with which one can process a number of operations in a reliable manner, such as encrypting and signing information and establishing the identity of another party.
Ransomware	Type of malware that blocks systems and/or the information they contain and only makes them accessible again against payment of a ransom.
RAT	A Remote Access Tool (sometimes referred to as a Remote Access Trojan) is used to gain access to the target's computer in order to control it remotely.
Resilience	The ability of people, organisations or societies to resist negative influences on the availability, confidentiality and/or integrity of (information) systems and digital information.
Responsible disclosure	Practice of responsibly reporting any security leaks found. Responsible disclosure is based on agreements that usually mean that a reporter will not share his or her discovery with third parties until the leak has been repaired, and the affected party will not take legal action against the reporter.
Script kiddie	Actor with limited knowledge who draws on tools which have been devised and developed by others, for cyber attacks motivated by mischief.
SIDN	Foundation for Internet Domain Registration in the Netherlands
Spear phishing	Spear phishing is a version of phishing that is directed against one person, or a very specific group of persons, deliberately targeted for their position of access in order to achieve as big an effect as possible without being noticed.
SPF	Sender Policy Framework is a protocol used by the owner of a domain name to indicate which servers are allowed to send legitimate emails on behalf of his or her domain. The owner of the domain name publishes the list of authorised servers in a DNS record.
SQL injection	A method of attack used by an attacker to influence communication between an application and the underlying database, with the main objective of manipulating or stealing data from the database.
STARTTLS	STARTTLS is a method of adding TLS encryption to an existing network protocol while retaining backward compatibility.
State actor	A state actor acts on behalf of a national government.

SWIFT	The Society for Worldwide Interbank Financial Telecommunication is an organisation that facilitates international payment transactions.
Terrorist	Actor with ideological motives who endeavours to realise social change, to spread fear among (groups of) the population or to influence political decision-making processes by using violence against people or by causing disruptive damage.
Threats	The Cyber Security Assessment Netherlands defines purpose and threat as follows: • The higher purpose (intention) may be strengthening an organisation's competitive position; political/national gain, social disruption or threatening a person's life. • In the Assessment, threats are categorised as follows: digital espionage, digital sabotage, publication of confidential data, digital disruption, cybercrime and indirect disruptions.
TLS	Transport Layer Security is a protocol for the purpose of setting up a secure connection between two computer systems. TLS forms the basis of the https protocol.
Tool	A technology or computer program used by an attacker to exploit or increase existing vulnerabilities.
Two factor authentication	A method of authentication requiring two independent proofs of an identity.
USB	Universal Serial Bus (USB) is a specification of a standard for the communication between a device (generally a computer) and a peripheral.
USB stick	Portable storage medium which is connected to a computer via a USB port.
Vulnerability	Characteristic of a society, organisation or (parts of an) information system that allows an attacker to hinder and influence the legitimate access to information or functionality, or to access it without the proper authorisation.
Watering hole	A watering hole attack is aimed at a location where many intended victims gather. The attacker spreads his or her exploit or malware via a website that they regularly visit by exploiting a vulnerability in this website or a CMS on which the website is based.
Web application	The entirety of software, databases and systems involved in the proper functioning of a website. The website is the visible part.
Zero-day vulnerability	A zero-day vulnerability is a vulnerability for which no patch is available yet because the developer of the vulnerable software has not yet had time to make a patch.

Appendix 4 Sources and references

1 https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html, consulted on 12 May 2017.
2 http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/, consulted on 22 March 2017.
3 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/espionage-cyber-propaganda-two-years-of-pawn-storm, consulted on 26 April 2017
4 https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/, consulted on 27 February 2017.
5 https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html, consulted on 27 February 2017.
6 https://www.fireeye.com/blog/threat-research/2017/01/apt28_at_the_center.html, consulted on 22 March 2017.
7 https://www.dni.gov/files/documents/ICA_2017_01.pdf, consulted on 22 March 2017
8 http://edition.cnn.com/2017/01/10/politics/comey-republicans-hacked-russia/, consulted on 19 April 2017.
9 https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity, consulted on 22 March 2017.
10 http://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK, consulted on 22 March 2017.
11 https://www.usnews.com/news/world/articles/2016-12-15/russian-officials-deny-vladimir-putins-involvement-in-election-hacking, consulted on 22 March 2017.
12 https://guccifer2.wordpress.com/2017/01/12/fake-evidence/, consulted on 22 March 2017.
13 https://motherboard.vice.com/en_us/article/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts, consulted on 20 March 2017.
14 https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign, consulted on 20 March 2017.
15 http://nos.nl/artikel/2111102-russische-hackers-maken-data-democraten-buit.html, consulted on 19 August 2016.
16 http://www.darkreading.com/attacks-breaches/russian-hackers-breach-democrats-to-steal-data-on-trump/d/d-id/1325909, consulted on 19 August 2016.
17 https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cfoo6cb4-316e-11e6-8ff7-7b6c1998b7ao_story.html?hpid=hp_hp-banner-main_dnc-hackers-1145a-banner%3Ahomepage%2Fstory, consulted on 26 April 2017
18 http://www.nu.nl/internet/4278512/hacker-guccifer-20-claimt-verantwoordelijkeid-hack-democratische-partij.html, consulted on 19 August 2016.
19 http://www.usatoday.com/story/news/politics/2017/03/21/dnc-cyber-attack-russia-highlighted-delayed-response-fbi-chief-says/99455634/, consulted on 22 March 2017.
20 https://www.nytimes.com/2016/12/13/us/politics/house-democrats-hacking-dccc.html, consulted on 22 March 2017.
21 https://www.nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html, consulted on 22 March 2017.
22 http://www.rtlnieuws.nl/nederland/politiek/rtl-nieuws-toont-aan-zo-makkelijk-is-het-hacken-van-politici, consulted on 22 February 2017.
23 https://autoriteitpersoonsgegevens.nl/nl/nieuws/toezichthouders-acm-en-ap-treden-op-tegen-stemwijzernl, consulted on 27 February 2017.
24 https://blog.fox-it.com/2017/03/23/turkish-hacktivists-targeting-the-netherlands-high-noise-low-impact/, consulted on 19 April 2017.
25 https://en.blog.nic.cz/2016/09/01/telnet-is-not-dead-at-least-not-on-smart-devices/, consulted on 1 March 2017.
26 https://www.bostonglobe.com/business/2016/09/23/cybercrooks-akamai/qOAhvHoohJcmkxIwg5ChKO/story.html, consulted on 1 March 2017.
27 https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac, consulted on 18 April 2017.
28 https://www.datanyze.com/market-share/dns/Alexa%20top%201K/Alexa%20top%201M, consulted on 17 March 2017.
29 Presentation "Dyn, DDoS, and DNS", by Andrew Sullivan (Dyn) op ICANN57. Slides & recording at https://schedule.icann.org/event/9npq/tech-day-part-2, consulted on 17 March 2017.

30 http://ics.sans.org/blog/2016/12/20/how-do-you-say-ground-hog-day-in-ukrainian, consulted on 22 March 2017.
31 http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA, consulted on 24 March 2017
32 https://www.slideshare.net/MarinaKrotofil/new-wave-of-attacks-in-ukraine-2016, consulted on 2 April 2017
33 https://motherboard.vice.com/read/ukrainian-power-station-hacking-december-2016-report, consulted on 22 March 2017.
34 http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC, consulted on 22 March 2017.
35 http://uawire.org/news/ukrenergo-claims-that-blackouts-in-kyiv-could-have-been-caused-by-hackers, consulted on 8 June 2017.
36 https://securingtomorrow.mcafee.com/business/shamoon-returns-bigger-badder/, consulted on 18 May 2017.
37 Source: AIVD and MIVD
38 http://www.volkskrant.nl/buitenland/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/, consulted on 4 July 2016.
39 http://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13XoVW, consulted on 2 April 2017
40 https://blog.linkedin.com/2016/05/18/protecting-our-members, consulted on 17 March 2017.
41 https://blog.fox-it.com/2016/06/07/linkedin-information-used-to-spread-banking-malware-in-the-netherlands/, consulted on 2 March 2017.
42 https://www.ncsc.nl/actueel/nieuwsberichten/65-miljoen-wachtwoorden-gelekt.html#ophef, consulted on 7 June 2012.
43 https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, consulted on 2 March 2017.
44 https://support.apple.com/en-us/HT207130, consulted on 2 March 2017.
45 https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws, consulted on 17 March 2017.
46 https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd, consulted on 17 March 2017.
47 https://www.nvb.nl/media/document/000254_0d15799-nvb-factsheet-veiligheid-en-fraude-06-06.pdf, consulted on 3 March 2017.
48 https://twitter.com/KeesVee/status/846613127559106560, consulted on 27 March 2017
49 http://nos.nl/artikel/2165391-software-die-computers-gijzelt-aangetroffen-in-tweede-kamer.html, consulted on 28 March 2017
50 https://www.fraudehelpdesk.nl/nieuws/ceo-fraudeurs-richten-pijlen-op-nederlandse-bedrijfsleven/, consulted on 22 March 2017.
51 Input Fraude Help Desk for NCSC Sectoral Threat Assessment Energy Sector Q4.
52 https://www.theguardian.com/business/2016/nov/08/tesco-bank-cyber-thieves-25m, consulted on 20 February 2017.
53 https://baesystemsai.blogspot.nl/2017/02/lazarus-watering-hole-attacks.html, consulted on 22 February 2017.
54 http://www.reuters.com/article/us-italy-cybercrime-idUSKBN14U1K2?il=0, consulted on 3 March 2017.
55 https://blog.kaspersky.com/eyepyramid-spyware/13838/, consulted on 3 March 2017.
56 http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/, consulted on 3 March 2017.
57 https://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/, consulted on 3 March 2017.
58 https://threatpost.com/fda-demands-st-jude-take-action-on-medical-device-security/124972/, consulted on 12 May 2017.
59 https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm, consulted on 12 May 2017.
60 https://autoriteitpersoonsgegevens.nl/nl/nieuws/1-jaar-meldplicht-datalekken, consulted on 27 February 2017.
61 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_meldingen_datalekken_q1_2017.pdf, consulted on 12 May 2017.
62 https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570, consulted on 27 February 2017.
63 https://investor.yahoo.net/releasedetail.cfm?ReleaseID=1004285, consulted on 27 February 2017.
64 https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-it-uses-md5-to-hash-my-password/, consulted on 27 February 2017.
65 https://www.verizon.com/about/news/verizon-and-yahoo-amend-terms-definitive-agreement, consulted on 27 February 2017.
66 http://www.reuters.com/article/us-yahoo-sec-probe-idUSKBN15709O, consulted on 22 March 2017.
67 https://www.security.nl/posting/485082/Energiedata+2+miljoen+Nederlandse+huishoudens+gestolen, consulted on 27 February 2017.
68 https://tweakers.net/nieuws/117829/ook-burgerservicenummers-asml-medewerkers-liggen-op-straat.html, consulted on 27 February 2017.
69 http://www.nporadio1.nl/onderzoek/2913-autoriteit-persoonsgegevens-wil-strenger-optreden-tegen-datalekken, consulted on 27 February 2017.
70 http://webwereld.nl/security/97134-bankrovers--kijk-daar--russen, consulted on 19 May 2017.
71 https://www.security.nl/posting/479242/Ransomwaremaker+zet+decryptiesleutels+concurrent+online, consulted on 19 May 2017.
72 http://www.dutchcowboys.nl/cybercrime/nieuwe-ransomware-laat-slachtoffers-vrij-als-ze-andere-vinden, consulted on 19 May 2017.
73 http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime, consulted on 19 May 2017.
74 https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIMoYoHvmc5g/pubhtml, consulted on 19 May 2017.
75 https://www.wired.com/2017/02/ransomware-turns-big-targets-even-bigger-fallout/, consulted on 19 May 2017.
76 http://money.cnn.com/2016/04/04/technology/ransomware-cybercrime/, consulted on 19 May 2017.
77 https://krebsonsecurity.com/2016/11/computer-virus-cripples-uk-hospital-system/, consulted on 19 May 2017.
78 http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victims-than-financial-firms.html, consulted on 19 May 2017.
79 http://www.sfexaminer.com/hacked-appears-muni-stations-fare-payment-system-crashes/, consulted on 19 May 2017.
80 https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/#more-37060, consulted on 19 May 2017.
81 https://motherboard.vice.com/en_us/article/luxury-hotel-goes-analog-to-fight-ransomware-attacks, consulted on 19 May 2017.

82 http://www.securityweek.com/simulation-shows-threat-ransomware-attacks-ics, consulted on 19 May 2017.
83 Source: police (NHTCU).
84 https://yourcommunity.tescobank.com/t5/News/Message-for-Current-Account-customers/td-p/6599, consulted on 19 May 2017.
85 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q?il=0, consulted on 19 May 2017.
86 https://tweakers.net/nieuws/111301/bankaanval-swift-netwerk-gelieerd-aan-sony-hack.html, consulted on 19 May 2017.
87 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0, consulted on 19 May 2017.
88 https://www.swift.com/insights/press-releases/swift-introduces-mandatory-customer-security-requirements-and-an-associated-assurance-framework, consulted on 3 March 2017.
89 https://www.swift.com/news-events/news/swift-launches-new-anti-fraud-payment-control-service-for-customers, consulted on 19 May 2017.
90 https://www.theregister.co.uk/2016/11/29/liechtenstein_bank_breaches/, consulted on 19 May 2017.
91 According to the Ministry of Foreign Affairs, over 9000 computers were infected in Saudi Arabia.
92 See for example 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, September 27 2016 (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/), consulted on 19 May 2017.
93 'United Cyber Caliphate Maken Threats in "Message to America," Claims DDoS Attacks', Site Intelligence Group, 27 December 2016.
94 'Pro-IS Hacking Group CCTA Identifies German Pilot to Kill', Site Intelligence Group, 14 March 2017.
95 See for example 'Western Countries | Understanding pro-IS hacking capabilities', Risk Advisory, September 27 2016 (https://news.riskadvisory.net/2016/27/western-countries-understanding-pro-is-hacking-capabilities/), consulted on 19 May 2017.
96 'UCC Announces Merger with Cyber Kahilafah, Claims "Kill Lists" arte Forthcoming', Site Intelligence Group, 24 December 2016.
97 'UCC Calls on Muslim Hackers to Join its Ranks Against "Disbelievers"', Site Intelligence Group, 10 March 2017.
98 'Caliphate in Decline: An Estimate of Islamic State's Financial Fortunes', ICSR & EY, London, 2017.
99 'Don't panic over cyber-terrorism: Daesh-bags still at script kiddie level', The Register, 16 February 2017.
100 http://nos.nl/artikel/2163055-turkse-hack-was-waarschijnlijk-online-vandalisme.html, consulted on 19 May 2017.
101 http://www.elsevier.nl/nederland/achtergrond/2017/03/turkse-hackers-openen-aanval-op-nederlandse-sites-470305/, consulted on 19 May 2017.
102 http://tuoitrenews.vn/society/36243/alleged-chinese-hackers-compromise-hanoi-airport-system-vietnam-airlines-website, consulted on 19 May 2017.
103 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, consulted on 19 May 2017.
104 http://www.cbsnews.com/news/new-world-hackers-claims-responsibility-internet-disruption-cyberattack/, consulted on 19 May 2017.
105 https://www.theregister.co.uk/2017/03/28/congress_approves_sale_of_internet_histories/, consulted on 2 April 2017
106 'Consumentenbond hekelt beveiliging gezondheidswebsites', Security.nl, 20 January 2017, 'Autoriteit Persoonsgegevens tikt stemwijzers op de vingers', Security.nl, 17 February 2017, 'Smart-tv's Sony en Panasonic volgen standaard kijkgedrag', Security.nl, 19 December 2017, 'AP wijst fabrikant Philips smart-tv's op privacyregels bij reclame', Security.nl, 26 January 2017, 'Toezichthouders willen opheldering WhatsApp over datadelen', Security.nl, 19 December 2016, , 'Franse privacywaakhond heeft kritiek op Windows 10', NOS.nl, 21 July 2016.
107 http://nos.nl/artikel/2133893-internet-der-dingen-wachten-tot-er-een-ramp-gebeurt.html, consulted on 19 May 2017.
108 http://www.networkworld.com/article/3118759/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html, consulted on 19 May 2017.
109 https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, consulted on 19 May 2017.
110 http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html, consulted on 19 May 2017.
111 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, consulted on 19 May 2017.
112 https://www.grahamcluley.com/nyadrop-exploiting-iot-insecurity-infect-devices-malware/, consulted on 19 May 2017.
113 https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/, consulted on 19 May 2017.
114 https://www.theregister.co.uk/2016/10/13/sshowdown_botnet/, consulted on 19 May 2017.
115 https://www.ietf.org/blog/2016/07/patching-the-internet-of-things-iot-software-update-workshop-2016/, consulted on 19 May 2017.
116 https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/neustar-2017-worldwide-ddos-attacks-cyber-insights-research-report.pdf, consulted on 12 May 2017
117 http://www.securityweek.com/iot-botnets-fuel-ddos-attacks-growth-report, consulted on 12 May 2017
118 http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/, consulted on 12 May 2017
119 https://www.bleepingcomputer.com/news/security/turkish-hackers-are-playing-a-ddos-for-points-game/, consulted on 19 May 2017.
120 http://www.itpro.co.uk/security/26993/ransomware-is-the-most-profitable-cybercrime, consulted on 19 May 2017.
121 http://www.emerce.nl/nieuws/ransomware-vorig-jaar-flink-gestegen, consulted on 19 May 2017.
122 https://www.security.nl/posting/469515/Ransomware+vraagt+losgeld+in+iTunes-cadeaubonnen, consulted on 19 May 2017.
123 https://www.bleepingcomputer.com/news/security/decrypted-alpha-ransomware-accepts-itunes-gift-cards-as-payment/, consulted on 6 March 2017
124 http://www.csoonline.com/article/3099852/security/health-care-organizations-114-times-more-likely-to-be-ransomware-victims-than-financial-firms.html, consulted on 19 May 2017.

125 Source: input from the healthcare ISAC.
126 http://www.faronics.com/news/blog/server-side-ransomware-rise-heres-beat/, consulted on 19 May 2017.
127 https://www.security.nl/posting/499094/MongoDB+waarschuwt+voor+aanvallers+die+databases+gijzelen
128 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-satan-offered-as-ransomware-as-a-service, consulted on 2 April 2017
129 https://www.recordedfuture.com/karmen-ransomware-variant/, consulted on 28 April 2017
130 Source: NHTCU.
131 Source: MSS 2016, NLO, NOM, SKO and VINEX.
132 http://www.adformatie.nl/sites/default/files/MSS_2016_Rapportage_infographic.pdf, consulted on 6 March 2017
133 Source: police and Fox-IT.
134 https://www.bleepingcomputer.com/news/security/android-ransomware-infects-lg-smart-tv/, consulted on 19 May 2017.
135 https://www.bleepingcomputer.com/news/security/padcrypt-the-first-ransomware-with-live-support-chat-and-an-uninstaller/, consulted on 19 May 2017.
136 https://www.wired.com/2016/12/popcorn-time-ransomware/, consulted on 19 May 2017.
137 https://blogs.forcepoint.com/security-labs/merry-cryptmas-cryptxxx-ransomware-offers-christmas-discount, consulted on 19 May 2017.
138 https://blog.barkly.com/ransomware-statistics-2016, consulted on 19 May 2017.
139 http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704, consulted on 19 May 2017.
140 https://www.bnr.nl/nieuws/economie/10305706/phishing-meldingen-overspoelen-fraudehelpdesk, consulted on 19 May 2017.
141 https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html, consulted on 12 May 2017.
142 https://www.ncsc.nl/actueel/nieuwsberichten/ceo-fraudeurs-richten-pijlen-op-nederlandse-bedrijfsleven.html, consulted on 19 May 2017.
143 https://www.nvb.nl/nieuws/2178/fraude-betalingsverkeer-wederom-fors-lager.html, consulted on 2 April 2017
144 https://www.betaalvereniging.nl/nieuws/fraude-betalingsverkeer-wederom-fors-lager/, consulted on 15 May 2017.
145 http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT, consulted on 19 May 2017.
146 http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q?il=0, consulted on 19 May 2017.
147 https://blog.trendmicro.com/trendlabs-security-intelligence/alice-lightweight-compact-no-nonsense-atm-malware/, consulted on 22 December 2016
148 https://www.fireeye.com/blog/threat-research/2017/01/new_ploutus_variant.html, consulted on 16 January 2017
149 https://www.riskiq.com/infographic/riskiqs-2016-malvertising-report/, consulted on 7 May 2017
150 https://pagefair.com/downloads/2016/05/2015_report-the_cost_of_ad_blocking.pdf, consulted on 7 May 2017
151 https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf, consulted on 7 May 2017
152 http://www.nu.nl/internet/4307673/hackersgroep-claimt-nsa-spionagesoftware-hebben-gestolen.html, consulted on 19 August 2016.
153 http://nos.nl/artikel/2126368-de-nsa-is-mogelijk-gehackt-maar-door-wie.html, consulted on 19 August 2016.
154 http://arstechnica.com/security/2017/01/nsa-leaking-shadow-brokers-lob-molotov-cocktail-before-exiting-world-stage/, consulted on 22 March 2017.
155 https://wikileaks.org/vault7/darkmatter/, consulted on 24 March 2017.
156 https://www.security.nl/posting/506475/WikiLeaks+onthult+hackingtools%2C+informatie+en+malware+van+CIA, consulted on 22 March 2017.
157 http://www.usatoday.com/story/news/world/2017/03/09/wikileaks-provide-tech-firms-access-cia-hacking-tools-assange/98946128/, consulted on 22 March 2017.
158 https://arstechnica.com/security/2017/04/10000-windows-computers-may-be-infected-by-advanced-nsa-backdoor/, consulted on 13 May 2017.
159 https://arstechnica.com/security/2017/04/purported-shadow-brokers-odays-were-in-fact-killed-by-mysterious-patch/, consulted on 13 May 2017.
160 https://www.theregister.co.uk/2017/05/12/spain_ransomware_outbreak/, consulted on 13 May 2017.
161 https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/, consulted on 13 May 2017.
162 http://www.bbc.com/news/health-39906019, consulted on 13 May 2017.
163 https://www.blackhat.com/docs/asia-16/materials/asia-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC.pdf
164 https://www.forbes.com/sites/davelewis/2014/10/29/internet-of-things-security-vs-time-to-market/#5923ffe215c4
165 https://www.arxan.com/wp-content/uploads/2017/01/2017_Security_IoT_Mobile_Study.pdf
166 Source: input from the energy, insurance, and MSP ISACs.
167 Source: input from all ISACs.
168 https://www.security.nl/posting/484543/Chrome+gaat+http-websites+als+%22niet+veilig%22+weergeven, consulted on 22 February 2017.
169 https://www.security.nl/posting/500740/Firefox+gaat+alle+http-websites+als+onveilig+weergeven, consulted on 22 February 2017.
170 https://pages.nist.gov/800-63-3/, consulted on 22 February 2017.
171 https://www.vvdveen.com/publications/BAndroid.pdf, consulted on 12 May 2017

172 https://zoek.officielebekendmakingen.nl/kst-798314.pdf, consulted on 23 February 2017.
173 https://www.logius.nl/diensten/digid/ontwikkelingen/, consulted on 24 February 2017.
174 https://www.idensys.nl/over-idensys-en-het-stelsel/, consulted on 24 February 2017 en https://www.digitaleoverheid.nl/dossiers/identificatie-en-authenticatie/, consulted on 2 May 2017.
175 https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/, consulted on 24 February 2017.
176 http://www.japantimes.co.jp/news/2016/12/01/business/tech/1-3-million-connected-devices-around-world-infected-viruses-study/, https://www.security.nl/posting/489469/Bijna+500_000+IoT-apparaten+besmet+door+Mirai-malware, https://telekomhilft.telekom.de/t5/Telefonie-Internet/Probleme-an-Telekom-Anschluessen/m-p/2294533#M694126, consulted on 24 February 2017.
177 https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-press-conference-mid-term-review-digital-single-market-strategy_en, consulted on 12 May 2017
178 https://www.security.nl/posting/493278/D66+wil+verkoopverbod+onveilige+Internet+of+Things-apparaten, consulted on 24 February 2017.
179 WODC, J.J. van Berkel, R.L.D. Pool, M. Harbers, J.J. Oerlemans, M.S. Bargh and S.W. van den Braak , (Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen, 2017 (pending).
180 http://blog.checkpoint.com/2016/08/07/quadrooter/, consulted on 24 February 2017.
181 https://www.ncsc.gov.uk/advisory-quadrooter-vulnerability-affecting-android, consulted on 8 June 2017.
182 https://www.vusec.net/projects/dedup-est-machina/, consulted on 24 February 2017.
183 https://www.vusec.net/projects/flip-feng-shui/, consulted on 24 February 2017.
184 https://www.vusec.net/projects/anc/, consulted on 24 February 2017.
185 https://www.forumstandaardisatie.nl/nieuws/nederland-zorgt-voor-veilig-e-mailverkeer, consulted on 24 February 2017.
186 https://www.forumstandaardisatie.nl/atom/136, consulted on 24 February 2017.
187 https://www.forumstandaardisatie.nl/thema/iv-meting, consulted on 23 May 2017.
188 https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html, consulted on 19 May 2017.
189 https://letsencrypt.org/2017/01/06/le-2016-in-review.html, consulted on 24 February 2017.
190 http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-verplichten-alle-overheidssites.html, consulted on 24 February 2017.
191 https://www.security.nl/posting/499791/Onderzoeker+waarschuwt+voor+backdoor+in+WhatsApp, consulted on 24 February 2017.
192 https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/, consulted on 22 March 2017.
193 https://blog.mozilla.org/security/2016/10/24/distrusting-new-wosign-and-startcom-certificates/, consulted on 3 March 2017.
194 https://support.apple.com/en-us/HT204132, consulted on 3 March 2017.
195 https://security.googleblog.com/2016/10/distrusting-wosign-and-startcom.html, consulted on 3 March 2017.
196 https://www.ncsc.nl/actueel/factsheets/factsheet-postkwantumcryptografie.html, consulted on 12 May 2017.
197 Source: input from the energy, insurance, transport, water, and healthcare ISACs.
198 Source: input from the energy, insurance, transport, and water ISACs.
199 De economische en maatschappelijke noodzaak van meer cybersecurity, http://www.mailswitch.nl/files/Px187NDcwMDM5MCowLTQ3NTI3MzcyMw==.pdf, consulted on 24 February 2017.
200 Rathenau Institute, Een nooit gelopen race, https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race, consulted on 22 March 2017.
201 http://rekenkamer.nl/Nieuws_overzicht/Persberichten/2017/05/Te_weinig_bekend_van_resultaten_rijksbeleid_knelpunten_bij_personeel_en_ICT_nog_zorgen_over_Belastingdienst, consulted on 29 May 2017.
202 http://www.volkskrant.nl/binnenland/burgemeester-aboutaleb-loopt-onnodig-groot-veiligheidsrisico~a4483405/, consulted on 29 May 2017.
203 https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar, consulted on 28 April 2017.
204 https://www.cybersecurityraad.nl/binaries/20170405_CSR_Handreiking2017_CompleetDEFweb_tcm56-253718.pdf, consulted on 12 May 2017.
205 https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections, consulted on 22 March 2017.
206 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z01527&did=2017D03236, consulted on 22 March 2017.
207 Source: input from the MSP ISAC.
208 ENISA Threat Landscape Report 2016, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, consulted on 21 February 2017.
209 Ponemon Institute: The Rise of Ransomware, https://www.carbonite.com/globalassets/files-white-papers/ransomware-report.pdf, consulted on 21 February 2017.
210 https://www.ncsc.nl/organisatie/nationale+cybersecurity+strategie, consulted on 24 April 2017.
211 https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/prive/aangifte_doen/praktische_informatie/belastingdienst_en_de_berichtenbox/belastingdienst_en_de_berichtenbox, consulted on 20 February 2017.

212 https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2017, consulted on 12 May 2017.
213 www.netbeheernederland.nl/smartgrids/, consulted on 20 February 2017.
214 https://www.technischweekblad.nl/nieuws/slimme-aardappelen-voor-precisielandbouw/item9986?PageSpeed=noscript, consulted on 20 February 2017.
215 https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf, consulted on 20 February 2017.
216 http://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/dnbulletin-2017/dnb352209.jsp, consulted on 20 February 2017.
217 https://www.cpb.nl/sites/default/files/omnidownload/CPB-Notitie-6juli2016-Risicorapportage-cyberveiligheid-economie.pdf, consulted on 20 February 2017.
218 https://www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start, consulted on 20 February 2017.
219 https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications, consulted on 24 April 2017.
220 http://europa.eu/rapid/press-release_IP-17-16_en.htm, consulted on 22 February 2017.
221 See CSAN 2016, p. 83 regarding the uneven playing field observed by the telecommunications sector.
222 https://www.mobileworldlive.com/featured-content/home-banner/facebook-vodafone-in-opposition-over-e-privacy-directive/, consulted on 24 April 2017.
223 https://tweakers.net/nieuws/122729/amerikaanse-senaat-stemt-in-met-verkoop-browsegeschiedenis-door-providers.html, consulted on 28 March 2017.
224 http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32014R0910, consulted on 24 April 2017.
225 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, consulted on 24 April 2017.
226 https://www.ntia.doc.gov/other-publication/2016/q-and-iana-stewardship-transition-0, consulted on 24 April 2017.
227 Reports 'Het internet, een onbegrensde ruimte met beperkte staatsmacht' by the AIV and 'De publieke kern van het internet: naar een buitenlands internetbeleid' of the WRR. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/08/22/kabinetsreactie-met-kabinetsreactie-het-internet-een-wereldwijde-vrije-ruimte-met-begrensde-staatsmacht-en-het-advies-de-publieke-kern-van-het-internet-naar-een-buitenlands-internetbeleid, consulted on 22 February 2017.
228 https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/, consulted on 24 April 2017.
229 https://www.rijksoverheid.nl/actueel/nieuws/2017/02/12/koenders-lanceert-internationale-cyberstrategie, consulted on 24 April 2017.
230 https://www.internetconsultatie.nl/telecommunicatie, consulted on 28 February 2017.
231 https://www.nrc.nl/nieuws/2017/01/24/overheid-eist-invloed-bij-cyberbeveiliger-fox-it-6382806-a1542772?utm_source=SIM&utm_medium=email&utm_campaign=Gesprekstof&utm_content=&utm_term=20170125, consulted on 28 February 2017.
232 https://fd.nl/economie-politiek/1190995/dijsselbloem-elf-van-25-aex-bedrijven-zijn-onvoldoende-beschermd-tegen-buitenlandse-overnames, consulted on 24 April 2017.
233 https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html, consulted on 24 April 2017.
234 http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en, consulted on 28 February 2017.
235 See also the AIV/CAVV report "Digitale oorlogsvoering", 2011, http://aiv-advies.nl/download/9fc55422-c96d-4563-9279-f434803coafd.pdf, consulted on 24 April 2017.
236 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html, consulted on 28 February 2017.
237 https://www.security.nl/posting/505252/Google+onthult+ongepatcht+lek+in+Internet+Explorer+en+Edge, consulted on 28 February 2017.
238 https://googleprojectzero.blogspot.nl/2015/02/feedback-and-data-driven-updates-to.html, consulted on 28 February 2017.
239 https://techcrunch.com/2017/03/07/is-signal-app-safe-wikileaks/, consulted on 21 March 2017.
240 See CSAN 2015.

Publication
National Coordinator for Security and Counterterrorism (NCTV)
PO Box 20301, 2500 EH The Hague, The Netherlands
Turfmarkt 147, 2511 DP The Hague, The Netherlands
+31 70 751 5050

More information
https://english.nctv.nl/
info@nctv.minvenj.nl
@nctv_nl

August 2017