National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Cyber Security Assessment Netherlands

CSAN 2019

Cyber Security Assessment Netherlands

CSAN 2019

Publication details

The Cyber Security Assessment Netherlands (CSAN) 2019 provides insight into threats, interests and resilience in relation to cyber security and the effect these factors have on national security. The Cyber Security Assessment Netherlands (CSAN) is published annually by the National Coordinator for Security and Counterterrorism (NCTV).

The NCTV protects the Netherlands against threats that may disrupt society. It is responsible for the coordination of counterterrorism, cyber security, national security and crisis management within central government. Together with its partners in the security field, the NCTV strives to ensure optimum safety and security in the Netherlands with a solid focus on preventing and minimising social disruption.

The National Cyber Security Centre (NCSC) is the central information hub and expertise centre for cyber security in the Netherlands. The NCSC is working towards increasing Dutch society's resilience in the digital domain, and towards a safe, open and stable information society.

The CSAN has been written by the NCTV and NCSC based on the insights and expertise of government services, organisations involved in critical processes, academia, and other parties. The NCTV made grateful use of the expertise and information provided by these parties both during expert sessions and during the validation of the CSAN.

Table of contents

Boosting resilience is the most important tool in reducing risk

Disruption of society looms ahead

The Cyber Security Assessment Netherlands (CSAN) 2019 provides insight into threats, interests and resilience in relation to cyber security and the effect these factors have on national security. The CSAN is published annually by the National Coordinator for Security and Counterterrorism and is written in cooperation with public and private partners.

Most critical processes and services are completely dependent on ICT. As a result of the near total disappearance of analogue alternatives and the absence of fallback options, dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage. Critical processes are highly dependent on the power grid and data communication, so any disruption or failure of such services can quickly impact a number of critical processes, within just a few hours even. The scale of the threat and the fact that resilience is lagging creates risks for national security.

Biggest threat posed by nation-state actors

Today, digital threats are a permanent fixture and the scale of the threat posed by nation-state actors continues to grow. Countries such as China, Iran and Russia have offensive cyber programmes against the Netherlands. This means that these countries are deploying digital resources in order to achieve geopolitical and economic objectives at the expense of Dutch interests. Disruption and sabotage have the greatest impact on national security due to their potential to cause social disruption. Acts undertaken for the purposes of preparing disruption and sabotage constitute a potential threat to Dutch autonomy and independence. The mere threat of disruption or sabotage (either explicit or implicit) could be enough to help an actor influence the decision-making processes. Economic espionage is a current threat to Dutch interests and criminal activities also have a major impact. Partly because of the scalability of cyber crime, the threats posed by these factors remain high.

Dependence on a limited number of providers and countries

To a large extent, the Netherlands is dependent on a relatively small number of providers of hardware and software, digital services, and platforms from a limited number of countries. This makes society more vulnerable to the shifting intentions of these providers and countries. This dependence creates risks to national security.

Advanced cyber attack capabilities easily accessible

Carrying out digital attacks often involves little risk for attackers. The ease with which advanced cyber attack capabilities can be obtained via commercial providers and through the substantial cybercriminal services sector is worrying. The latter sector frequently offers Dutch ICT infrastructure as part of its services. The number of actors possessing advanced offensive capacities is growing and as a result, the threat level and the likelihood of misattribution is increasing. This likelihood is further exacerbated by the fact that very few countries possess sufficient capacities to enable attribution based on intelligence gathering in a broad sense, in addition to attribution based on technical characteristics.

There is a risk that businesses, the media or even countries are unable to identify who executed an attack or that they attribute the attack to the wrong parties.

Resilience not in order in all areas

Boosting resilience is the most important means of reducing risk to citizens, businesses and government bodies. There is not yet a clear and precise picture of resilience. Affecting the various threats and dependency levels has proven to be a complex challenge. Measures are not always taken as the costs and benefits of cyber security are unevenly distributed. It is currently unclear whether the existing incentives to readjust the cost-benefit ratio are sufficient.

Increasing threat level

Geopolitical developments will further increase the threat from nation-state actors. This threat is amplified by the fundamental conflicts of interests between different countries and differences of opinion regarding international standards and values. Technology and its dominant role in modern society appears to have contributed to major geopolitical tensions.

Digitisation has greatly increased the range of opportunities to commit cyber attacks and caused both a growth of and a shift in the attention of actors to new and alternative strategic targets. Furthermore, the threat posed by criminals remains as high as ever. Disruptions and systems failures will have a greater impact on society in the future due to the complete dependence on digitised processes and systems. Insufficient cyber security can result in disruption of society.

Reader's guide

The CSAN 2019 provides insight into threats, interests and resilience in relation to cyber security and the effect these factors have on national security. Cyber security refers to the entirety of the measures to prevent damage caused by disruption, failure or misuse of ICT and to repair it should any damage occur. This damage could consist of impairment of the availability, confidentiality or integrity of information systems and information services and the data contained therein.

The CSAN was formulated based on the insights and expertise of government services, organisations involved in critical processes, academia, and other parties. The developments have been described in a qualitative manner. In the event that relevant and reliable data is available, quantitative substantiation or source references are also provided.

Monitoring threats, interests and resilience is a continuous process, with the CSAN being one of the annual results. Matters which have not or have barely changed with respect to the previous editions of the CSAN have been described in brief or not at all. The analysis included in the CSAN is based on the triangle of threats, interests and resilience. The risk is determined according to the interplay between these three factors.

The key questions of the CSAN 2019 are:

- What threats exist that could impair the availability, confidentiality or integrity of information, information systems or information services?
- Why is cyber security important? What are the potential consequences for national security in the event the identified threats become manifest themselves?
- What combinations of vulnerabilities and tools have played out on the global stage within the reporting period (May 2018–January 2019) and were or could be applied to the Netherlands (annual review)?
- How resilient is national security and the Netherlands as a whole against the tools that can or have been deployed against it, the vulnerabilities that could be exploited or the threats that could manifest themselves?
- To what extent can underlying causes or factors at the heart of the cyber security assessment be identified?
- Which broader developments are expected to influence future cyber security assessments?

The preceding text described the most notable developments within this Cyber Security Assessment. Chapter 1 describes the key problems, the root causes and factors that underlie the Cyber Security Assessment. These are based on the previous CSAN. Chapter 2 provides a more detailed description and explanation of the threats. Chapter 3 is about the importance of cyber security to society and national security. The fourth chapter contains the annual review. The Dutch resilience level is addressed in Chapter 5. In the sixth and final chapter, a broad look ahead is presented. Finally, the annexes provide a summary of the incidents dealt with by the NCSC and explanation of the abbreviations used.

Figure 1 **Interest, threat and resilience model**

Uneven distribution of costs and benefits

1 Key issues

This Cyber Security Assessment is based on a variety of key problems. These problems constitute the causes and contributory factors that in turn lay the foundations for the threats, interests and resilience described in this document.

Fallback options and analogue alternatives are virtually non-existent, costs and benefits within the field of cyber security are unevenly distributed, and there is a high dependency on a limited number of providers and nation states. Conducting digital attacks often involves little risk for attackers, the capacity to perform an attack is easily accessible, and unsecure products and services are the Achilles heel of cyber security. The increasing levels of complexity and connectivity in society is having a negative effect on resilience levels.

Digitisation fundamental to society

Our society has become almost entirely dependent on digitised processes and systems. As a result, cyber security is essential in order to enable social and economic growth and to prevent social disruption.

Fallback options and analogue alternatives virtually non-existent

Practically all critical processes and services are entirely dependent on ICT. Due to the near total disappearance of analogue alternatives and the absence of fallback options, dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage.

Uneven distribution of costs and benefits of cyber security

Cyber security measures are vital as a barrier against cyber threats, although such measures cost time and money. As a result, citizens, businesses, sectors and government bodies must always carefully weigh up their interests when implementing these measures. Sometimes, the interest of cyber security is directly interlinked with other interests. Sometimes, conflicts of interests can arise between different organisations or even within organisations, e.g. between the interest of user-friendliness for individuals and the broader interest of cyber security. In addition, the individual interests of businesses (especially commercial interests) can conflict with social interests. The uneven distribution of costs and benefits is the main cause of such conflicts of interest and as a result, measures are not always implemented. It is currently unclear whether the existing incentives to readjust the cost-benefit ratio are sufficient.

Dependence on a limited number of providers and countries

The dependency on a relatively small number of providers of hardware and software, digital services, and platforms from a limited number of countries is increasing. Due to the technological possibilities or the price-performance ratio offered by these providers, it can be tempting for businesses, citizens and nation states to do business with these providers. These providers often possess multiple means of protecting against attacks, although at the same time, if these systems are disrupted or otherwise compromised, the social impact can be substantial.[2] Products or services provided by foreign or domestic providers can be compromised by malicious actors either with or without the provider's knowledge. Moreover, providers must comply with legislation, meaning that in some countries, they may be forced to cooperate with espionage activities, or the preparations for sabotage, for example.

Dependence on (a limited number of) providers and nation states means that society relies on the intent of these providers and nation states and is hence vulnerable to any changes thereto. This creates risks for national security.

Permanent cyber threat

The scale of the threat posed by state-sponsored actors continues to grow. Countries will continue to use digital resources for the purposes of espionage or even sabotage in order to achieve their own objectives at the cost of Dutch interests. Furthermore, the threat posed by criminals remains as high as ever. The digital threat is permanent.

Execution of cyber attacks involves little risk

It is possible for cyber attacks to remain undetected for a long time. When attacks are detected, tracing the actors responsible and attributing the attacks to them are complex challenges. Even if attribution is possible, there are usually no consequences, especially when they are executed by nation-state actors or nation-state-affiliated actors. However, there has been a change regarding how cyber attacks by governments are publicly attributed. Many countries have attributed attacks to other countries or specific actors. The effect of these public attributions remains unclear. For the time being, it appears that the execution of cyber attacks involves little risk for attackers.

Advanced cyber attack capabilities easily accessible

Cyber attack capabilities can be easily obtained via commercial providers and via the substantial cyber criminal services sector. Nation states and criminals can purchase advanced attack capabilities, meaning they don't have to develop these capabilities themselves. Nation states can 'outsource' the preparation for and execution of cyber attacks to third parties. Due to their easy availability, more and more actors are capable of obtaining cyber attack capabilities or expanding their capabilities. This creates a higher risk level.

Digital resilience not high across the board

Organisations are being successfully attacked using simple methods and many such incidents could have been prevented or the damage mitigated if basic measures had been implemented. The increasing complexity and connectivity of the ICT landscape is putting more and more pressure on resilience levels.

Unsecure products and services: the Achilles heel of cyber security

Digitally unsecure products and services are a fundamental cause of incidents. Unsecure products and services boost accessibility for attackers, making it easier for them to successfully execute cyber attacks. Security lapses can be caused by providers supplying unsecure configurations as standard or not (or no longer) making updates available available due to compromised update mechanisms or the updates being difficult to install. Furthermore, even if updates are available, organisations do not always install them. It is unclear whether sufficient incentives (economic or otherwise) exist to promote the development of secure products or services. This creates a conflict of interests between the economic needs of organisations on the one hand and society's need for adequate cyber security measures on the other.

Negative effects of complexity and connectivity

It is becoming increasingly difficult to ensure a resilient digital infrastructure. Certain software is generically used by developers and suppliers as building blocks of their product/service. Some popular protocols for data exchange via the internet are decades old and therefore not resistant to contemporary attacks. In the years to come, the complexity and connectivity of digital infrastructure will increase due to ongoing digitisation. The organic growth and the relatively long service life of systems will result in an increasingly complicated landscape. Moreover, the increasing use of shared facilities such as partial products or complete cloud services makes it harder to maintain a clear picture of the situation and monitor it. In the past, such services were structured within individual organisations, although nowadays they are purchased by a wide range of parties and implemented externally. These parties also call upon the services of subcontractors. Monitoring of the entire supplier chain is an extremely complex challenge. Management of the ICT landscape is still contained within individual organisations, yet the execution thereof is becoming increasingly fragmented and spread across multiple parties. This causes a lack of clarity, creates new dependencies and increases the attack surface.

Nation-states pose biggest cyber threat

2 Threats

Today, digital threats are a permanent fixture. Nation-state actors pose the biggest cyber threat to national security, and that threat continues to grow. Countries are using digital resources for the purposes of espionage or even (preparations for) sabotage in order to achieve their own objectives at the cost of Dutch interests. Furthermore, the threat posed by criminals remains as high as ever. The threat from other actors has also remained virtually the same.

Disruption and sabotage have the greatest impact on national security. Even the preparation for these types of attacks create a potential threat to Dutch autonomy and independence. Simply by threatening to cause disruption or commit an act of sabotage (either explicitly or implicitly), an actor may attempt to influence decision-making processes. Cyber espionage remains an attractive means of achieving geopolitical influence and economic growth. Given that hacking tools are readily available and the efficiency of simple attack methods, the threat is posed by a wide range of actors. Very few countries possess sufficient capacities to enable attribution based on intelligence gathering in a broad sense, in addition to attribution based on technical characteristics. There is a risk that businesses, the media or even countries are unable to identify who executed an attack or that they attribute the attack to the wrong parties. Moreover, growing digitisation is increasing the threat of unintentional disruption and failure of systems in the Netherlands.

Increased threat from nation-state actors

The biggest cyber threat affecting national security is posed by nation-state actors. Countries such as China, Iran and Russia are operating offensive cyber programmes against the Netherlands. This means that these countries are deploying digital resources for espionage or even sabotage (or the preparation thereof) in order to achieve their own political, military, economic and/or ideological objectives at the expense of Dutch interests.[3] These activities to enable disruption and sabotage are increasingly targeting Western countries and as a result, the threat to national security and Dutch interests is growing.[4]

No substantial attacks by hacktivists against the Netherlands or its interests have been detected during this reporting period.[5,6,7] Script kiddies and cyber vandals mainly carried out disruptive attacks on organisations. These were mostly DDoS attacks.[8,9,10,11] Just like last year, criminal actors seem to be focusing more frequently on the creation of botnets[12,13] and spreading cryptominers.[14,15,16] Partly because of the scalability of cyber crime, the threat posed by criminals remains as high as ever.[17,18] Cyber attacks by criminals cause societal damage.[19] The threat posed by insiders has dwindled in the past year.[20] In addition, no cyber attacks by terrorists have been identified this year. That threat has been low for several years.[21] Terrorist groups focus more on committing physical attacks.

Disruption and sabotage have the most substantial impact

Disruption and sabotage by nation-state actors have the greatest impact on national security. These activities can cause (long-lasting) disruption to society, especially when critical processes and parties are affected.[22] A variety of nation-state actors have the capacity to conduct these kinds of attacks and tensions between countries can instigate the deployment of these capacities.[23] There is currently no intent by external actors to execute sabotage activities against critical national infrastructure in the Netherlands, although certain states have attempted to gain access to ICT systems governing critical processes. Due to the current geopolitical unrest, it is more conceivable that sabotage activities could be carried out. For example, Russia, among other states, operates an offensive cyber programme to disrupt and even sabotage critical national infrastructure. In addition, disruption to critical infrastructure (such as the power grid) in neighbouring countries could also affect the Netherlands.[24]

Examples of disruption and sabotage

In the past year, such activities have been identified in Europe. Systems belonging to Polish energy and transport firms were infected with potentially highly destructive malware (GreyEnergy).[25] In the past, other destructive malware such as Industroyer[26] was responsible for disrupting the power supply in Ukraine.[27] According to the United Kingdom, the group that presumably developed GreyEnergy is affiliated with Russia.[28] In December 2018, an oil processing facility in Italy belonging to the company Saipem was attacked, presumably by a different actor.[29] The attack disabled around 4,000 machines and computers for a short time.

Given the changing nature of geopolitical relationships, the greater the Dutch involvement in geopolitical conflicts, the greater the threat of disruption and sabotage will become.

Preparatory acts pose a threat to autonomy and independence

Preparatory acts, acts undertaken for the purposes of preparing disruption and sabotage of critical processes and parties by nation-state actors constitute a threat to national security.[30] Not only as preparation for use during geopolitical conflicts or the escalation thereof, but also to exercise influence on countries. Actors may conduct preparatory acts long before any actual conflict develops. By implicitly or explicitly threatening disruption or sabotage, actors can exercise economic, diplomatic or military influence on the target. The threat of disruption and sabotage, e.g. by 'visibly' conducting preparatory acts, is therefore a means of influencing or attempting to influence decision-making processes. This constitutes a potential threat to Dutch autonomy and independence.

Digital espionage for the purposes of influence and growth

In addition to the threat of digital disruption and sabotage, espionage by nation-state actors also constitutes a substantial threat to Dutch interests. States conduct spying activities to gain information for the benefit of their geopolitical, military and economic interests. Digital espionage is used frequently by nation-state actors.[31] An increasing number of countries is intensifying its focus on espionage, with China, Iran and Russia leading the charge.[32]

China poses the greatest threat of economic espionage by far. This espionage is fuelled by Chinese economic policy plans such as 'Made in China 2025' and the Belt and Road Initiative, which aim to expand the country's economic and geopolitical influence. China is deploying a wide range of both covert and overt resources that undermine the earning capacity of Dutch firms and could result in economic and political dependencies in the long term. One of these resources is economic espionage (including cyber espionage).[33]

For Russia, the Netherlands is also an interesting target for espionage. As a result of MH17, the strategic importance of the Netherlands to Russia has substantially increased. Furthermore, the Netherlands has long since been on Russia's radar due to the establishment of international institutions in the country and its membership thereof.[34]

Threat determined by intent, capacity and activity

The threat that an actor poses to (information) systems is determined by the combination of the degree of intent, capacity and activity. Intent relates to whether the actor has a specific objective (e.g. geopolitical or financial) and is willing to impair the confidentiality, integrity and availability of a system. Capacity comprises the necessary knowledge and access to resources that can facilitate a cyber attack. The distinction between intent and capacity can result in specific threats being interpreted differently. Detection or conceivability of concrete cyber attacks in the Netherlands and – to a lesser degree – Europe or allied Western countries are the core factors in determining the level of activity. It is possible for an actor to pose a threat if the actor has intent and capacity, even if little to no activity has been detected.

Nation states also spy on citizens. In this regard, we distinguish between the interest of nation states in personal data in general and targeted spying on particular individuals or groups (e.g. dissidents) for purposes such as influencing or intimidating these individuals/groups (among other objectives). Personal data can be used to prepare for other espionage or influencing activities. The various forms of espionage can undermine the democratic rule of law and the constitutional state, cause short or long-term damage to the economy[36] and restrict the freedoms of citizens.

Table 1 Threat matrix

	Government	Critical	Private	Citizens
States/state-affiliated	Espionage Data manipulation	Disruption Sabotage Espionage	Espionage System manipulation	Espionage
Criminals	Disruption System manipulation Data theft	Disruption System manipulation	Disruption Data manipulation Data theft System manipulation	Disruption Data manipulation Data theft System manipulation
Terrorists	Sabotage	Sabotage		
Hacktivists	Disruption	Disruption	Disruption Data manipulation	
Cyber vandals and script kiddies	Disruption	Disruption	Disruption	
Insiders	Data theft		Data theft	
Unintentional acts	Disruption/failure Leak	Disruption/failure Leak	Disruption/failure Leak	Leak

The threat matrix[35] gives insight into the threats that various actors pose to various targets. The table is not exhaustive and does not contain all conceivable threats: only those posed by actors who have been estimated to have sufficient intent and capacity or by actors who are known to have conducted activities in the past.

Caption:

Yellow: Actors have intent but lack the tools/knowledge (capacity)
OR activity has been detected but the actors possess limited tools/knowledge
OR activity has been detected but the actors only intend to attack specific targets

Orange: The actors possess tools/knowledge and substantial intent
OR the actors have substantial intent and activities have been detected.

Red: The actors have substantial tools/knowledge and very substantial intent
OR the actors have very substantial intent, possess substantial tools/knowledge and a great deal of activity has been detected.

The following threats are defined:

- Disruption: intentional temporary impairment of the accessibility of data, information systems or information services.
- Sabotage: intentional and very long-lasting impairment of the accessibility of data, information systems or information services, possibly resulting in destruction.
- Data manipulation: impairment of the integrity of information by means of the intentional editing of data.
- Data theft: impairment of the confidentiality of information by means of the copying or removal of data.
- Espionage: impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors.
- System manipulation: impairment of information systems or information services targeting the confidentiality or integrity of these systems/services. These systems or services are subsequently used to carry out other attacks.
- Breakdown/failure: impairment of integrity or accessibility due to natural causes, technical difficulties or human error.
- Data leak: impairment of confidentiality due to natural causes, technical difficulties or human error.

Cyber espionage in practice: Ministry of Foreign Affairs

Other countries could be interested in gaining insight into communication between the Ministry of Foreign Affairs and diplomatic posts abroad. Intelligence services have detected that in 2017 and 2018, a foreign intelligence service carried out cyber attacks against a number of Dutch embassies in the Middle East and central Asia. The cyber attacks on these embassies confirm the structural focus paid by foreign intelligence services to the Ministry of Foreign Affairs [37]

Threat due to availability of offensive capabilities

Given that hacking tools are readily available and and the efficiency of simple attack methods, a substantial threat is posed by a wide range of actors. Third parties are being more frequently misused.

Advanced cyber attack capabilities easily accessible

Actors have easy access to hacking tools. They can acquire these tools on the internet, or hire the services of attack facilitators. These facilitators are service providers who can provide actors with the means of executing a digital attack, including infrastructure, equipment and techniques, in exchange for payment. They frequently offer Dutch ICT infrastructure as part of their services.[38,39] The facilities they offer can be simple, such as DDoS attacks or bulletproof hosting, but they can also be more advanced in nature. Nation states can purchase advanced attack capabilities, meaning they don't have to develop these capabilities themselves. Nation states can 'outsource' the preparation for and execution of cyber attacks to third parties. Due to their easy availability, more and more actors are capable of obtaining cyber attack capabilities or expanding their capabilities. As a result, the threat level has increased.

Simple and universal hacking methods successful

Many actors, including nation-state actors, use the same hacking methods. Simple hacking methods are often successful. As a result, the group of actors capable of executing cyber attacks is sizeable. One of the methods that is being increasingly used by a wide range of actors is 'Living off the Land' attacks.[40] This method abuses products or services that are already installed on the victim's systems. After they gain access to a particular system or network, nation-state actors are able to deploy advanced tools. Defences can be established against simple hacking techniques in order to make potential targets less vulnerable and less attractive to hackers. Implementing 'basic hygiene' measures for ICT systems and networks substantially increases resilience against cyber attacks, including attacks by nation-state actors.

Compromising third parties remains attractive and is on the rise

In previous editions of the Cyber Security Assessment, it was established that supplier chains increase vulnerability levels,[41] and in this reporting period, we once again detected a number of highly successful attacks via third parties.[42,43] This type of attack is becoming increasingly attractive to hackers and further growth in the number of such attacks is expected.

According to the United States and Australia, the Chinese hacker group APT10 was very successful in its efforts to compromise service providers.[44,45] Through these providers, economic espionage was carried out against a wide range of businesses in many different countries. In addition, the ICT infrastructure of third parties was often misused for the purposes of executing attacks on other parties. During this reporting period, the Dutch ICT infrastructure (among others) was used by nation states such as Iran, North Korea and Russia to execute attacks on other nation states.[46,47]

Cyber attacks supported by physical operations

Physical operations can also be developed in order to supplement simple hacking tools, with such operations often being developed by nation-state actors. In April 2018, the Russian military intelligence service was willing to risk discovery by sending employees to the Netherlands to execute a cyber attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague from right outside the building.[48] This intelligence service has conducted many such operations in the past, although this was the first time that an operation was detected in the Netherlands.[49]

Effect of public attribution not yet measurable

Various government bodies have publicly attributed cyber attacks to specific nation states. This tactic is intended to create a deterrent by increasing the costs of transgressive behaviour.[50] In addition to public attribution, other tools also exist, such as the imposing of sanctions like travel bans or freezing funds belonging to individuals or groups to whom cyber attacks are attributed. The impact of attributing transgressive conduct to actors is currently not measurable. Attribution – the identification of the actor responsible for a cyber attack – is a complex challenge as it demands a highly specific set of technical, intelligence and political capacities, among others. While many nation states have the capacity to execute cyber attacks, few of them possess sufficient capacities to enable attribution based on intelligence gathering in a broad sense, in addition to attribution based on technical characteristics.[51] There is a risk that businesses, the media or even

countries are unable to identify who executed an attack or that they attribute the attack to the wrong parties.

Technical attribution complex due to diverse range of hacking methods

Technical attribution is a complex process. The complexity of technical attribution is affected by the easy access to hacking tools, the simplicity and wide range of hacking methods, misuse of third parties and the blurring of boundaries between actors.[52] The use of purchased hacking tools by criminals makes it more difficult for the police to trace cyber attackers. In addition, simple hacking methods and purchased or publicly available hacking tools substantially complicates the attribution of attacks to nation-states and other actors. Although in some cases, commercial businesses attribute certain methods and techniques to specific nation-state actors, this does not always mean that that particular nation-state actor is always the perpetrator. Conversely, methods and techniques attributed to criminals can also be used by nation-state actors. As a result, getting a clear picture of the threat posed by individual actors is a complicated challenge, which increases the complexity of this threat.

Threat from cyber criminals and other actors

Activities conducted by career criminals regularly make the news, as do pettier criminal activities by script kiddies or cyber vandals.[53,54,55] Due to the easy accessibility of hacking tools and the low level of knowledge required to carry out a cyber attack, it is expected that this will continue to be a problem for years to come. Attacks on targets such as banks or government offices can potentially damage trust in the use of digital services. The threat from criminals remains as high as ever; they cause damage to society.[56,57,58] In the last reporting period, DDoS attacks were conducted that temporarily impaired accessibility to a number of banks.[59] Government bodies were also regularly affected, with cyber attacks affecting accessibility to services such as the Tax and Customs Administration, Customs and DigiD.[60,61,62] Although such attacks do not directly affect national security, they can potentially damage trust in the digital society in the long term.

Increasing threat of breakdowns and failures

Systems failures and breakdowns remain a major threat, albeit a threat that does not involve any intent or malicious activity. Due to the interconnectedness of systems and the increasing degree of complexity, it is likely that breakdowns and failures will occur more often in the Netherlands. The failure of one individual system or network can cause breakdowns or failures in other areas.[63] This is especially the case if basic cyber security measures have not been sufficiently implemented and if no underlying systems are in place as a fallback option. Breakdowns and failures pose a significant threat due to the potentially major impact they can have, especially when central information hubs or critical processes are affected. For example, when the rail traffic control system at Schiphol Airport was hit by a systems failure, many trains were put out of action.[64] This failure was caused by a combination of many different circumstances, events and human error.

Digitisation causing a shift in targets

The unabating increase in digitisation is causing a shift in the dependency of underlying systems and infrastructure. Some systems are being phased out, while other systems are growing in importance or even becoming indispensable. As a result, these systems and infrastructures are now appearing on the radar of cyber actors and/or becoming increasingly attractive targets. They can be used either as a primary target – e.g. for the purposes of espionage or disruption – or as a platform from which to launch cyber attacks on other targets (system manipulation).

Two examples of this are the Internet of Things (IoT) and personal data. The digitisation trend means that all types of cloud application are becoming more attractive targets for hackers. Cloud applications are becoming increasingly vital building blocks of digitised processes and the increasing trend towards the IoT – including within critical processes – is also making attacks on the IoT more attractive.[65]

Personal data is easy for people to obtain, including malicious actors. Social media is a primary source of personal data, as are massive data sets obtained via data leaks. In the recent period, it has been found that personal data is being abused by nation-state actors and cyber criminals to address victims in an increasingly convincing manner.[66,67]

Essential analogue alternatives and fallback options practically non-existent

3 Interests

Digitised processes and systems are the foundations upon which our modern society is built. Cyber security – more specifically the confidentiality, integrity and accessibility of these digital foundations – is an essential facilitator of social and economic growth and a vital tool for the prevention of social disruption. Analogue alternatives have practically disappeared and fallback options are non-existent. Numerous chains of critical providers are dependent on suppliers that have not been designated as critical. To a large extent, the Netherlands is dependent on a relatively small number of providers of hardware and software, digital services, and platforms from a limited number of countries. This makes society more vulnerable to the shifting intentions of these providers and countries. This dependence creates risks to national security.

Digitisation fundamental to society

Dutch society and its critical processes are almost entirely dependent on digitised processes and their underlying (information) systems. These processes and systems are the digital foundations on which our modern society is built. Digitisation is transforming our economy and society. It is the primary source of growth, innovation and new commerce, as well as a vital factor in solving contemporary social problems. Among other measures, the government wants to make the very most of all social and economic opportunities by supporting and accelerating the digital transition in certain sectors.[68] For example, €165 million has been set aside to make communication between citizens, entrepreneurs and the government smarter, more accessible and more personal.[69] In addition, the government has earmarked €60 million for digital care in order to promote the use of e-health and further boost information exchange.[70] Naturally, organisations and private citizens will also go along with this process of digitisation.

Secure digital foundations essential

Impairment of the digital foundations of our society can impact national security, especially in relation to critical processes. It is not easy to predict exactly what consequences will result from cyber incidents, although we can say with certainty that such incidents could have major consequences.

Complete dependence on digitisation

Due to the almost complete dependence on digitisation, digital security of processes and underlying systems has become an essential factor. As a result, the interest of digital security has increased in importance. After all, the more these processes, data services and connections become digitised, the greater the consequences of any impairment of the confidentiality, integrity or accessibility of (information) systems. Furthermore, the intensifying complexity and connectivity means that a single incident in an individual network can cause a series of incidents in other networks.[71]

The increasing digitisation of critical processes means that cyber security is becoming an increasingly important national security interest. Critical processes include the provision of gas, water and electricity, water management, air and water transport, payment traffic, etc. Rather than being isolated to a single sector, cyber incidents often result in chain reactions that have repercussions for multiple sectors. Critical processes are almost entirely dependent on ICT and electricity, and therefore failure of these services can potentially have a major impact on society.

The interdependencies within critical national infrastructure mean that any disruption to a single critical process can result in chain reactions or cascade effects that impact other critical processes. The results of a self-assessment showed that many critical processes are highly dependent on electricity and data communication services.

Any failure of critical processes can often impact a number of other critical processes within a few hours. Electricity and data communication services are interdependent.[72]

A coordinated cyber attack resulting in the simultaneous failure of multiple systems – such as telephone services or electricity, gas or drinking water – could have particularly major consequences.[73] Impairment of critical processes in the Netherlands can also affect other countries and vice versa.[74]

Social disruption via cyber attacks

Recently, the Dutch newspaper NRC roughly outlined the consequences of longer-term simultaneous cyber incidents. Within this scenario, the Netherlands had been widely hit by ransomware. Screens were being blacked out, files were being held hostage and computer systems were being switched off as a preventive measure. At the same time, waves of DDoS attacks were being conducted, resulting in a game of cat and mouse between attackers and defenders. This resulted in myriad unpredictable chain reactions: telephone networks were overloaded, rail traffic around Amsterdam was immobilised, traffic jams piled up around Schiphol Airport, hospitals were unable to admit any more patients, social media and websites belonging to public broadcasters became inaccessible, electronic payment traffic was largely brought to a standstill, ready cash was running out and people were no longer able to buy food. The attack was remedied after three days, although the recovery efforts lasted for weeks or even months.[75]

Essential analogue alternatives and fallback options virtually non-existent

As a result of the near total disappearance of analogue alternatives and the absence of fallback options, dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage. This does not necessarily involve any malicious intent, as breakdowns and unintentional damage can also cause social disruption – a factor that will increasingly be a problem in the future. Furthermore, you have the paradox that the more robust the infrastructure becomes, the less people take potential incidents into account. For example, the telecom system in the Netherlands has become so reliable that many organisations were insufficiently aware of their dependence thereon and were insufficiently prepared for disruption.[76] There is no plan B if the networks go down.[77]

Analogue alternatives non-existent

According to experts, people in Eastern Ukraine were very lucky that manual backups were available when cyber actors shut down the power supply in winter. *'There, someone can flip a switch to start everything up again. Within six hours, the power supply had been restored. Although the software took longer to repair, the electricity supply was up and running again. In the Netherlands, we often no longer have this kind of manual backups, often relying on digital backups instead.'* [78]

Dependence on suppliers/subcontractors not designated as critical

The complexity and connectivity of information systems and networks has been increasing for many years. Organisations are often no longer capable of carrying out all of the tasks themselves. They operate in chains and depend on other organisations to supply data, conduct or support data processing activities, and many more. This is not without risk. Business processes can be disrupted if data is not exchanged with other organisations in a secure and reliable manner. When this occurs in the chains of vital providers, it can lead to major system failure, damage to physical security and social disruption.[79] The chains of critical providers can also be dependent on suppliers or subcontractors who have not been identified as critical parties. As a result, disruption to or cyber attacks on ICT systems outside the critical sphere can still affect critical processes. The number of unforeseen dependencies within critical processes is also increasing. For example, if a cyber actor decided to adjust the temperature setting of a substantial number of air conditioning systems in New York by three degrees, then this could result in power being cut across the entire city.[80]

A small number of providers and nation states dominate

The dependency on a relatively small number of providers of hardware, software, digital services, and platforms from a limited number of countries is increasing.81 For example, Facebook (including WhatsApp and Instagram), Amazon, Apple, Google and Microsoft hold a combined market share of 95%. They are a practically inextricable part of the average European's everyday life and the combined value of these businesses is equal to the gross national product of France. This all begs the question of how this increasing power and influence could affect the sovereignty and autonomy of the Netherlands and the European Union.[82] Moreover, an increasing number of digital services, such as online bookkeeping and authentication services, are based on an underlying cloud platform belonging to one of the major players (e.g. Microsoft Azure, Amazon Web Services or Google Cloud). This further increases dependence on these suppliers.

Economies of scale and influence of major players

In certain cases, the major providers are able to harness economies of scale to benefit organisations and their users. They are able to continually innovate, have larger financial reserves and their economies of scale allow them to operate competitively in the market. Major providers also have more resources to defend against attackers. However, a number of disadvantages are also associated with major providers. For example, once a particular cloud provider is selected, switching to a different provider is not a simple process and often involves substantial costs. The standards relating to these services are also effectively set by a small number of providers, which may allow them to strengthen their position at the expense of other parties. The social impact of a breakdown or a digital attack can be substantial as many different processes or services are dependent on a limited number of providers.

Dependence on a limited number of providers and countries

This dependence and the relatively small group of providers also makes the Netherlands dependent on a small number of countries. The vast majority of hardware and software is either designed or produced in China and the USA.[83] Third countries sometimes have different legislation or rules governing issues such as privacy or data access. According to the National Security Analysts Network, our society's mass usage of foreign devices and technology, which could potentially contain 'back doors', is an underappreciated problem.[84]

Products or services provided by foreign or domestic providers can be compromised by actors either with or without the provider's knowledge. Manufacturers and service providers have become an attractive target for actors due to their dependence on supplier chains. In addition, these providers must comply with legislation, meaning that in some countries in which they do business, the government may force them to cooperate with espionage activities, preparatory acts for the purposes of sabotage, etc.

Due to the technological possibilities or the price-performance ratio offered by these providers, it may be tempting for businesses, citizens and countries to do business with major providers or authorise others to do the same. However, this may create security risks in the longer term due to the increasingly strong dependence on these businesses or on the countries from which these businesses originate.[85] For example, warnings have been issued regarding the use of Huawei products during the development of 5G networks,[86] with the US informing its Western allies that collaboration with Huawei during construction of the 5G network could result in less information being exchanged with US intelligence services.[87]

The Netherlands is dependent on a relatively small number of providers of hardware and software, digital services, and platforms from a limited number of countries. This dependence creates risks to national security.

High concentration of data processing and storage conducted abroad

The dependence on a relatively small number of providers also applies to data. The process of digitisation in recent years has resulted in unprecedented quantities of data about all manner of things. The cabinet considers data to be a critical raw material for the new economy.[88] Others see data as being 'the new oil', the 'fourth factor of production' or a new 'technology' whose primary function is to increase productivity.[89] A huge quantity of data belonging to Dutch organisations and citizens is stored and processed via foreign platforms. The need for data processing activities means that countries, organisations and users are dependent on the intent of nation-state actors and commercial actors, making them vulnerable to any changes in the intent of these actors.[90] The high concentration of data means that data leaks can potentially have extremely large-scale impact.

Providers under the microscope

According to the German competition authority, Facebook is abusing its position by collecting people's personal data without asking their permission or informing them of exactly what is done with it.[91] According to seven European consumer organisations, Google is tracking its users via their location history and their web and app activity: settings that are integrated into all Google accounts. For users of Android phones, it is extremely difficult to avoid such tracking activities.[92] In the US, Facebook is facing a fine of billions of dollars due to privacy violations.[93] Furthermore, an ever-clearer picture is emerging of the opportunities and undesirable side effects involved in targeted advertising. For example, Facebook allows specifically targeted adverts to be sent to antivaccinationists, people interested in anti-vaccination propaganda and people who have 'liked' pages on these topics.[94] Targeted advertising based on political preferences is also possible. In the United Kingdom, efforts are being made to revamp legislation on election-related campaigning as legislation exists for physical leaflets and billboards, but not for digital campaigns.[95]

Advanced cyber attack capabilities easily accessible

4 Annual review

Advanced cyber attack capabilities are easy to obtain and simple hacking tools remain effective. Actors make use of publicly available tools and generic services to easily achieve their desired results. Supply chains and inadequate configurations have once again been misused to conduct successful attacks. In the last reporting period, Western critical infrastructure was compromised multiple times. More countries have resorted to public attribution of cyber attacks, although attribution remains a complex process that is prone to error. Cyber crime also continues to evolve. Breakdowns and systems failures illustrate the increase in complexity and interconnectedness of technology and modern society.

Western critical infrastructures compromised

The increasing number of activities to facilitate sabotage of critical European infrastructure in both the short and long term involving infiltration of certain systems by nation-state actors is a topic that has been covered before.[96] These activities appear to be increasingly targeting Western Europe. In this reporting period, a variety of providers of critical national infrastructure have been successfully attacked. These providers were subsequently used as a stepping stone in order to compromise intended targets. Many actors are becoming increasingly interested in exploiting vulnerabilities in the supply chain in order to facilitate disruption or sabotage, to exercise geopolitical pressure or to enable espionage activities.

In October 2018, the ESET security firm reported on cyber attacks using GreyEnergy malware.[97] GreyEnergy is considered the successor of BlackEnergy, a malware toolkit that has been linked to cyber attacks against the Ukrainian power grid in 2015 and 2016. GreyEnergy is alleged to have been used for a variety of attacks against Ukraine, although it has also been used for hacking activities against Poland.[98] The German Federal Office for Information Security (BSI), once again turned its attention to cyber attacks on the German energy sector.[99] German businesses in a variety of sectors are said to have been targeted multiple times by large-scale cyber attack campaigns, enabling attackers to gain access to the private office networks of many different businesses. It is suspected that the attackers wished to establish a position within this network for use at a later date.

Dragonfly

The US Department of Homeland Security has been warning against cyber attacks by groups such as Dragonfly for many years. This group is also known as Havex, Energetic Bear and Energetic Yeti. The US government attributes Dragonfly to Russia.[100,101] This actor group targets networks in the US belonging to businesses involved in critical national infrastructure as well as their suppliers. By carrying out targeted cyber attacks on the supplier chain, the attackers were able to gain access to the networks of suppliers and partners of their intended targets. The targets range from small businesses to major corporations that are responsible for the generation, transport and distribution of electricity. The access gained to these suppliers was used as a stepping stone to explore the networks of the intended targets. The attackers used these compromised networks to send spear phishing emails and watering hole attacks. Hundreds of businesses were affected. Eventually, the attackers successfully gained access to some of the networks of their intended targets, although how many networks were actually compromised remains undisclosed. The attackers used the networks to collect data on industrial control systems. Once the attackers had gained access to the networks, they attempted to establish permanent access to them. Ultimately, the actor group did not conduct any sabotage or disruption activities.

Advanced cyber attack capabilities easily accessible

Nation states can purchase advanced attack capabilities, meaning they don't have to develop these capabilities themselves. Nation states can also 'outsource' the preparation for and execution of cyber attacks to third parties. Research institute The Citizen Lab has extensively reported on one of the businesses providing spying software to more than 40 countries, not only for investigative purposes but also to spy on opposition leaders and dissidents.[102] Reuters has reported on how former employees of the US National Security Agency assisted the government of the United Arab Emirates with espionage activities.[103] The United Arab Emirates also used 'Karma' – a specialised hacking tool – to hack the iPhones of activists, diplomats and foreign leaders.[104,105]

Publicly available tools and generic services used as hacking tools

The use of publicly available tools and techniques to compromise or disrupt networks or to steal confidential data is nothing new.[106] Actors can also use generic services to conduct cyber attacks. In this regard, the term 'generic services' refers to public facilities such as online data storage or email services, as opposed to infrastructure set up by and for malicious actors. The use of generic services is one example of a readily available method that may be more difficult for users or detection tools to identify. A report published by a variety of Western governments described a number of these tools and the purposes for which they are deployed.[107] In October 2018, security firm Symantec reported on an espionage campaign by a new actor group. Rather than using malware to conduct its activities, this group – named Gallmaker – uses only publicly available tools and generic services, a strategy that enabled it to conduct activities for months without detection.[108]

Technical attribution complex and error-prone

In this reporting period, the technical attribution of operations to specific nation-state actors based on technical characteristics has proven to be a complex and error-prone process. In October 2018, Bloomberg published an article reporting that the Chinese government had implanted a chip into the server motherboards of Super Micro Computers Inc. in order to infiltrate US organisations.[109] The companies in question denied these allegations and were backed up in this regard by the UK National Cyber Security Centre and the US Department of Homeland Security.[110,111] Around Christmas, a Russian hacking group was linked to the publication of the personal data of German politicians,[112,113] although a German student was eventually arrested for this hack.[114]

In the last reporting period, it has become clear that the attributions of a number of cyber attacks by security firms have been incorrect.[115,116,117] Factors such as publicly available tools and generic services have amplified the complexity of technical attribution and as a result, security firms have become more reticent about attributing hacks.[118]

In February 2019, a number of media channels reported that the networks of a variety of Australian political parties had been compromised. Given the measures that Australia had implemented against Chinese businesses to prevent cyber espionage, it was assumed that China may have been behind the attack.[119,120] However, at the end of February 2019, other media channels reported that Iran was the guilty party. It was claimed that Iranian government hackers had been targeting the US and its allies and that this cyber attack was retaliation for the resumption of sanctions against the Iranian government.[121] Further investigation is required to determine exactly who is to blame.

Political attribution on the rise

The phenomenon of governments publicly attributing cyber attacks to specific nation-state actors is a recent development that was also addressed in the CSAN 2018. In this reporting period, a variety of governments have taken measures against certain actors. The United States has indicted hackers originating from Iran[122,123], North Korea[124], Russia[125,126] and China[127], among others. A variety of indictments were also supported by other governments.[128,129]

On 20 December 2018, the US Department of Justice indicted two Chinese hackers from the group APT10, accusing them of conducting cyber attacks on the orders of the Chinese government. The goal of the campaign was predominantly economic espionage via the theft of intellectual property and technical information. The campaign targeted a variety of sectors and was detected across a wide sphere.[130] Australia, Canada, Japan, New Zealand and the United Kingdom have since attributed this campaign to the Chinese government.[131,132,133,134,135]

Specific government measures

It would appear that governments are also implementing other measures in addition to public attribution. One example is the alleged cyber operation deployed by the US government during the November 2018 elections, when it allegedly authorised activities aimed at compromising Russian networks in order to prevent possible cyber attacks on the US.[136,137]

In May 2018, in response to national security concerns, the cabinet took the precautionary measure of phasing out government use of Kaspersky antivirus software and advised critical businesses and defence suppliers to do the same.[138]

The Czech Republic takes measures against Chinese 5G hardware and software

In December 2018, the Czech National Cyber and Information Security Agency (NCISA) issued a warning against hardware and software produced by the Chinese companies Huawei Technologies Co. Ltd and ZTE Corporation. According to the NCISA, the use of hardware and software supplied by these companies constituted a threat to national security. Businesses designated as critical national infrastructure, important information systems and essential providers are obliged to take note of this warning and to implement adequate countermeasures.[139]

A variety of countries such as the United States[140] and Australia[141] have already implemented measures, while other countries are still considering whether to do so.[142,143]

Cyber crime continues to evolve

Criminals are successfully capitalising on new technological developments, such as online services. It has become easier to conduct acts of digital crime as a result of Cybercrime-as-a-Service (CaaS), which enables actors with relatively limited capacity to execute cyber attacks. In this reporting period, cyber criminals have once again made substantial misuse of Dutch digital infrastructure.[144,145]

Criminals successfully targeting two-factor authentication

Two-factor authentication adds an extra layer of security to traditional user authentication tools. However, in this reporting period, criminals have also managed to get ahead of this system. This became apparant from a phishing attack targeting users of the government portal MijnOverheid [MyGovernment], for example.[146] Victims were tricked into logging in via a false login page, with the attackers also misusing the code sent via text message. The attackers would then automatically log in to the victim's MijnOverheid page. As a broader trend, attacks aiming to intercept text messages are still relatively rare, although the number of such attacks has increased.[147,148]

Rise in Cybercrime-as-a-Service continues unabated

Europol's Internet Organised Crime Threat Assessment (IOCTA) has shown that the rise of Cybercrime-as-a-Service has continued unabated.[149] Via criminal forums, actors with a relatively low level of ICT knowledge can purchase services facilitating every step required to execute specific cyber attacks. It is becoming easier to commit cyber crime due to the accessibility and user-friendliness of these services. In 2018, the website webstresser.org – a platform that assisted over 135,000 users in performing every step of millions of DDoS attacks with criminal intent – was taken offline[150,151] Scientific research shows that the provision of cyber crime services via general underground online marketplaces is not as successful as is often suggested[152] and that these kinds of services are offered on a huge scale via specific underground cyber criminal forums.[153] This criminal-services sector makes frequent use of Dutch ICT infrastructure in order to provide services.[154]

Hack_Right

Awareness of criminal liability for cyber crime is not yet universal. The police conducted a campaign through which they were able to determine that over 9,500 young people could be enticed to commit acts of cyber crime, such as hacking Instagram accounts or taking down electronic learning environments. Nearly a third of these young people were unaware that these intended acts were criminal offences.[155]

In some cases, young perpetrators are entered into Hack_Right, an alternative or supplementary punishment programme. Young people between 12 and 23 years of age who are convicted of a first-time cyber offence may be eligible for this programme. The goal of Hack_Right is to prevent recidivism and further develop the cyber talents of young people within the constraints of the law. This intervention was developed and is executed by criminal law chain partners, cyber security firms and the hacker community.[156]

Apparent decline in use of ransomware

Microsoft has observed[157] that after peaking at the beginning of 2018, the prevalence of infections via ransomware and cryptominers declined both in the Netherlands and at the global level. Businesses appear to be better prepared to recover data following infections of ransomware, resulting in fewer ransoms being paid. In addition, the use of cryptominers appears to be decreasing following the drop in value of a variety of cryptocurrencies. Symantec has also reported a decline in ransomware and cryptominers,[158] although the firm expects that these types of malware will continue to cause problems in the future. Symantec and Trend Micro[159] have observed an increase in the use of cryptominers on mobile devices. In its annual threat assessment[160], CrowdStrike reports an increase in targeted ransomware attacks on major corporations in order to obtain large ransoms in one fell swoop.

Emergence of formjacking

As well as ransomware and cryptojacking, cyber criminals appear to have been using other hacking techniques in this reporting period, such as formjacking. According to Symantec, the use of this technique by cyber criminals was notable. Formjacking involves adjustment of websites to allow the attacker to obtain the data entered by visitors. Attackers can adjust websites in a variety of ways, by hacking the website and adjusting the website code themselves, for example. They can also adjust the code of shared sections of websites, such as web shop software. Finally, they can also change the website's functionality through advertisments displayed on the website.

These techniques enable criminals to intercept data such as credit card numbers belonging to web shop users.[161,162] Symantec reports that every month, 4,800 unique web shops around the world fall victim to formjacking, particularly small and medium-sized retail firms.[163]

Simple hacking tools effective

During this reporting period, simple hacking tools such as phishing or misuse of usernames/passwords once again proved effective.

Phishing remains successful

Phishing has been a successful method of conducting cyber attacks for a long time and still remains a popular, effective and widely used hacking method. Statistics[164,165] and examples[166] both show that phishing has been used frequently in this reporting period. Due to its consistent effectiveness, this method is used both by nation-state actors for the purposes of spying and sabotage[167,168] and by criminals[169,170]. Losses in the Netherlands as a result of phishing attacks targeting internet banking services increased from €1.05 million in 2017 to €3.81 million in 2018.[171]

Misuse of usernames and passwords

In the last reporting period, a variety of attacks were conducted in which the 'Domain Name System' (DNS) settings of organisations around the world were changed. DNS can be considered to be the 'phone book of the internet'. In January 2019, US-CERT and FireEye reported that malicious actors had temporarily changed the DNS settings of a number of domains.[172,173,174] According to FireEye, this attack affected organisations in a wide variety of sectors, including telecom/internet providers and government bodies in the Middle East, North Africa, Europe and North America. The security firm Talos had already reported on similar attack methods being used on targets in the Middle East.[175] The attackers were able to change the DNS settings by means of usernames and passwords to the DNS provider's customer portal. By changing these DNS settings, they were able to steal other usernames and passwords, e.g. from users who logged in to their organisation's webmail platform. Cyber attacks using this method were said to have been conducted from January 2017 onwards. In January 2019, FireEye attributed these attacks to Iran.[176] The Internet Corporation for Assigned Names and Numbers (ICANN) warned any parties who play a role in the DNS chain about these attacks and urged them to take countermeasures.[177]

Border Gateway Protocol (BGP) hijacks were also used in this reporting period for the purposes of diverting DNS traffic. In April 2018, it had already been ascertained that a BGP hijack had been conducted in order to misuse Amazon's DNS service.[178] In July 2018, it transpired that a similar technique had been used to divert the DNS traffic of American payment processing services.[179]

Ransomware infections via Remote Desktop Protocol

In the last reporting period, malicious actors were able to successfully find vulnerable Remote Desktop Protocol (RDP) servers. RDP enables remote access to and operation of systems. Dutch businesses fell victim to SamSam ransomware,[180] which attempts to gain access to RDP servers that are available online by exploiting weak passwords. By gaining access in this way, these malicious actors gathered information about the target organisation in order to demand a ransom.

Misuse of supplier chains

The previous paragraphs describe the misuse of service providers and software suppliers. Microsoft has written about the vulnerable software supplier chain, describing a number of cases that demonstrate how rogue code can be integrated into legitimate software,[181] e.g. via an infected update or installation package that then hitches a ride on the software's legitimate distribution process, including its security guarantees.

2018: new legislation in the Netherlands

In 2018, new and additional cyber security legislation came into force, including the Network and Information Systems Security Act (Wbni), the General Data Protection Regulation (GDPR) and the Intelligence and Security Services Act (Wiv).

Network and Information Systems Security Act (Wbni) comes into force

The primary objective of the Wbni is to implement the European Network and Information Security Directive (NIS Directive), the goal of which is to achieve a higher collective level of security within the EU as well as incorporating the applicable rules specified in the act that preceded it (the Data Processing and Cyber Security Notification Obligation Act or Wgmc). The majority of this new act came into force on 9 November 2018, with the remainder thereof entering into law on 1 January 2019. The Wbni aims to boost the digital resilience of the Netherlands, with particular focus on critical providers (energy providers, drinking water suppliers, the financial sector, etc.), central government and digital service providers. Critical providers are public organisations and private

legal entities that provide services whose continuity is – in the opinion of the Dutch government – vitally important to Dutch society. In the Wbni, digital service providers are defined as online marketplaces, online search engines and cloud computer services with at least 50 employees.[182]

Notification obligation and duty of care for critical providers and digital service providers

In line with the Wbni, providers of essential services, other providers designated as critical providers by general administrative order, and digital service providers are subject to a notification obligation in the event of incidents that could potentially have substantial consequences for the continuity of the services they provide. An incident is defined as any event that has a damaging effect on the security of the network systems and information systems used for the purposes of the services in question. These incidents must first be reported to the Computer Security Incident Response Team (CSIRT). For the aforementioned critical providers, this means the National Cyber Security Centre within the Ministry of Justice and Security. During the reporting period, one report was made to the NCSC in accordance with the Wbni.[183] Digital service providers report incidents to the CSIRT for digital services provided to the Ministry of Economic Affairs and Climate Policy. In addition, providers of essential services and digital service providers must also report these incidents to their sectoral supervisory body.

In line with the Wbni, providers of essential services and digital service providers are also subject to a duty of care: they are obliged to implement appropriate and proportionate organisational and technical measures to manage risks to the security of their ICT systems, to prevent incidents and to restrict the consequences of incidents to the greatest extent possible in order to guarantee the continuity of their services. These measures must ensure that the network systems and information systems are resistant to activities that jeopardise the digital security of the of data that is stored, sent or processed, or to the related services that are offered or are accessible via these systems.[184]

Other new legislation

Computer Crime Act III [185]
On 1 March 2019, the Computer Crime Act III (*Wet Computercriminaliteit III*) came into force. This act gives the police and judiciary new powers to combat computer crime. It gives them the authority to covertly and remotely conduct online research into computers, also known as 'the power to hack'. The act also criminalises online trade fraud and the handling of stolen digital data.

General Data Protection Regulation[186]
The General Data Protection Regulation (GDPR) came into force on 25 May 2018.[187] The GDPR supersedes the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*). The law is directly applicable in all EU member states. The GDPR guarantees two interests: the protection of natural persons in relation to the processing of their data, and the free movement of personal data within the European Union. Under the GDPR, citizens are granted new privacy rights and their existing rights have been reinforced. Organisations that process personal data will be subject to a greater number of obligations and must demonstrably comply with these regulations.[188]

Intelligence and Security Services Act 2017 [189]
On 1 May 2018, the new Intelligence and Security Services Act 2017 (*Wet op de Inlichtingen- en Veiligheidsdiensten 2017*) came into force. This act gives the intelligence and security services a number of new powers and establishes new guarantees. For example, the act includes stricter data storage periods and establishes that the use of special intelligence tools will be assessed in advance by an independent committee (the Central Review Committee (TIB)).

Breakdowns and failures

A number of ICT failures occurred during the reporting period. Breakdowns or failures of information systems are caused by unintentional human actions or system errors. During the reporting period, systems failures affected a number of hospitals. In August 2018, between 1,000 and 1,500 appointments had to be cancelled at the Amsterdam University Medical Centre following a systems failure that cut off access to the electronic patient files and shut down the email system.

The use of complex technology is further increasing[190] and as a result, minor errors are having increasingly substantial consequences. An example of this is the systems failure in the Schiphol tunnel in August 2018.[191] An error in the software of the dynamic rail traffic control system and an unfortunate concurrence of circumstances resulted in the automatic rail traffic control system becoming overloaded. As a result, all rail traffic around

Amsterdam and Schiphol had to be controlled manually, leading to delays and cancellations.

The increasing level of complexity and interconnectedness of processes and systems means that the failure of a single system can affect multiple processes or a chain of processes. When a system fails, it impacts all processes that are dependent on it. In August 2018, the electronic ankle bracelets of hundreds of prisoners in the Netherlands were affected by a systems failure at telecom provider Tele2,[192] which resulted in the bracelets being unable to connect to the control room for two days.

Most data leaks due to human error

According to the Dutch Data Protection Authority, the number of reported data leaks further increased in the first half of 2018 to 5,430 new reports in Q2.[193] This is double the amount recorded for Q2 2017 (2,468 data leaks). The Netherlands is one of the leading countries in Europe with regard to the reporting of data leaks.[194]

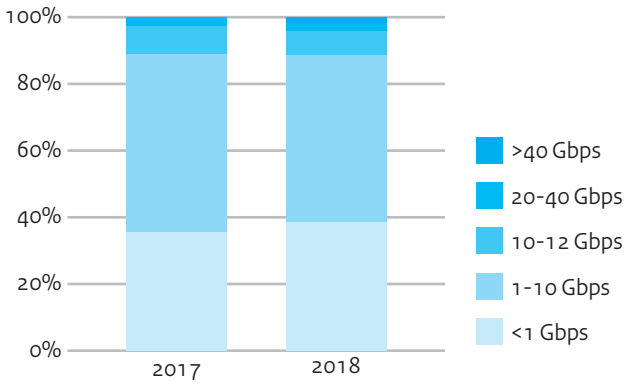
More than half of the data leaks reported in the first half of 2018 were the result of human error. Personal data sent to the wrong recipient or provided to the wrong person constituted 64% of the total number of reports.[195]

Increase in DDoS attacks

The number of websites targeted by a DDoS attack in 2018 was 15% higher than in 2017, according to the National Management Organisation for Internet Providers (NBIP) and the Foundation for Internet Domain Registration in the Netherlands (SIDN).[196] Webshops remain a popular target, with a peak in DDoS attacks on webshops occurring in December 2018.[197] Financial institutions and DigiD (among other targets) were also hit by DDoS attacks.[198,199] In December 2018, the FBI reported that in collaboration with the Dutch police, they had taken 15 websites offline that offered DDoS-attack services. [200]

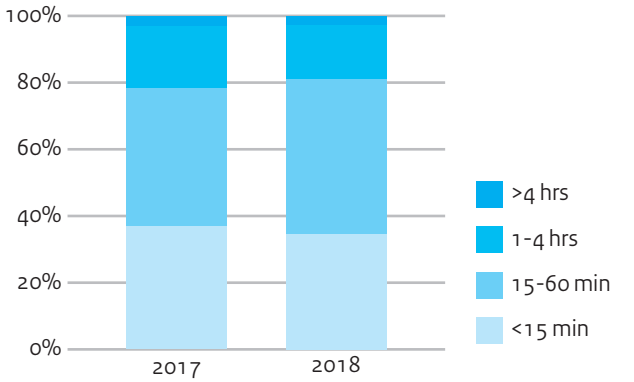
In the last reporting period, it was notable that no massive attacks were conducted such as the 1 terabit per second attack described in the CSAN 2018. In 2018, the NBIP processed 938 DDoS attacks. The biggest single DDoS attack in 2018 was 68 gigabits per second (Gbps), while in 2017, the biggest attack was 36Gbps. Just like in previous years, the majority of attacks were no bigger than 10Gbps, and just like in 2017, no DDoS attacks in 2018 lasted for longer than 1 hour. The statistics show that the number of DDoS attacks lasting 15 minutes or less is declining, while the number of DDoS attacks lasting between 15 minutes and 1 hour are increasing.

Figure 2 **Scale of DDoS attacks**



Source: National Management Organisation for Internet Providers (NBIP)

Figure 3 **Duration of DDoS attacks**



Source: National Management Organisation for Internet Providers (NBIP)

Organisations being successfully attacked with simple methods

5 Resilience

Certain aspects of digital resilience in the Netherlands are not yet in order. Methods to measure resilience are lacking. For this reason, an indirect picture of the situation has been outlined based on supervisory reports and extrapolation of incidents and events. There is not yet a clear and precise picture of resilience. Organisations are being successfully attacked using simple methods and many such incidents could have been prevented or the damage mitigated if basic measures had been implemented.

Digital resilience not in order across the board

Digital security – more specifically the confidentiality, integrity and accessibility of digitised processes and systems – is an essential facilitator of social and economic growth and a vital tool for the prevention of social disruption. Among other measures, the cabinet asserts that reinforcement of the resilience of citizens and organisations is necessary in order to capitalise on the opportunities that digitisation offers. Security and trust are essential building blocks of this resilience which will also lay solid foundations for an advantageous business climate, our competitive position and the acceptance and usage of digital tools.[201] In this regard, cyber security is not just a cost item or a necessary evil, but also a catalyst for further digitisation.

Digital resilience not yet in order across the board. Organisations are being successfully attacked using simple methods and many incidents could have been prevented or the damage mitigated if basic measures had been implemented. The increasing complexity and connectivity of the ICT landscape is putting more and more pressure on resilience levels. Boosting resilience is the most important means of reducing risk to citizens, businesses and government bodies. Affecting the various threats and dependency levels has proven to be a complex challenge. Legal measures such as the Network and Information Systems Security Act (Wbni) emphasise the importance of organisations increasing their resilience levels. The effects of these measures will become apparent over the next few years.

No measurement method for resilience

Gaining insight into resilience levels, and thus the efficiency and effectiveness of the measures implemented, is a complex challenge. Reliable methods and techniques to measure resilience are key prerequisites in order to gain clear insight into national security risks and to compare different organisations and sectors, but these methods and techniques are currently insufficiently developed. As a result, it is only possible to create an indirect outline of the situation based on supervisory reports and extrapolation of incidents and events. This means that no comprehensive and detailed picture of the digital resilience of all critical processes is available as yet.

Central government insufficiently resilient

On Accountability Day in May 2018, the Netherlands Court of Audit indicated that only two of the eleven ministries have established a sufficient level of ICT security. The president of the Netherlands Court of Audit stated that 'the top politicians and civil servants within ministries must pay more attention to ICT security'.[202,203]

Ministries indicate whether their data security is sufficient by means of 'In Control Statements' (ICSs). The Netherlands Court of Audit indicated that for 2017, the basis of these ICSs is ad hoc and implicit, which complicates efforts to get a clear picture of the situation across the entire breadth of central government. The ministries have a variety of definitions regarding what constitutes a critical system.[204]

On Accountability Day in May 2019, the Netherlands Court of Audit also established that the level data security is insufficient. The court identified major data security problems within eleven central government organisations, which means the situation has worsened in comparison to the previous year.[205]

Resilience of critical processes

A study[206] conducted by the Netherlands Court of Audit to investigate the cyber security of critical water infrastructure in the Netherlands found that there was room for improvement concerning the protection of tunnels, bridges, sluice gates and flood defences against cyber attacks. In recent years, a great deal of work has been done and essential measures have been identified in order to boost security of flood defences, although not all of these security measures have been implemented. Crisis documentation has become outdated and no comprehensive penetration tests have been conducted. The study shows that not all critical water infrastructure is linked to the Security Operations Centre, which creates a risk of cyber attacks going undetected or being detected too late.[207]

De Nederlandsche Bank states that within the Dutch financial sector, it has found that explicit attention is not continually paid to analysis of cyber security threats and measures[208] and that the focus on bringing and keeping data security measures up to speed is sometimes insufficient. Sometimes, undesired combinations of access rights for applications and processes occur. Attention to the detection and analysis of cyber attacks remains essential and more attention should be paid to the response to and recovery from cyber attacks.

As a clear and comprehensive picture of digital resilience is lacking, it is unknown whether the resilience of other critical processes is high or low. At the same time, it is conceivable that *in a general sense*, there will be no significant deviations from the situation as described above.

Organisations being successfully attacked with simple methods

Organisations are being successfully attacked using simple methods. As the recent period has once again shown, organisations could have prevented incidents and mitigated damage by implementing basic security measures, although many organisations are yet to do so.

Phishing remains an effective hacking technique

Cyber attackers continue to use existing hacking methods whose effectiveness is proven. This year, phishing once again proved to be a popular and successful hacking method[209] as the execution of such attacks is relatively simple. Although many organisations make efforts to raise awareness of this issue among users, the effectiveness of such attacks does not appear to be in decline. An analysis conducted by Microsoft[210] shows that an increasing percentage (approx. 250% in 2018) of emails investigated in the analysis are marked as phishing scams. Highly targeted spear phishing campaigns have proven themselves to be particularly successful and virtually unrecognisable to their victims.

Detection time lags behind the duration of attacks

A report by FireEye shows that organisations are still finding it difficult to detect whether or not their systems have been misused. In 2018, the average detection time for system infiltrations around the world was 78 days after the date of the infiltration.[211] However, this does represent an improvement: the 2017 average was 101 days and in 2014 it was as high as 205 days. CrowdStrike has observed that within just hours of accessing a network, sophisticated attackers can gain access to other parts of the company network.[212]

In many cases, initial access is gained via simple methods such as phishing, with attackers subsequently deploying advanced methods to explore and further penetrate the networks. During this second phase, it becomes much more difficult to detect attackers and completely remove them from the network environment. Improvement of basic digital hygiene is an effective barrier against cyber attacks.

Hardware and software vulnerabilities remain problematic

The number of reported vulnerabilities (high risk or otherwise) in 2017 and 2018 increased substantially according to the Netherlands Bureau for Economic Policy Analysis (CPB) in its Cyber Security Risk Assessment for the Economy 2018.[213]

Unsecure software creates vulnerabilities in systems and hence also processes. A study commissioned by the NCSC showed that in the Netherlands, nearly 1.5 million potentially vulnerable devices and services on these devices were connected to the internet, of which nearly 300,000 devices proved to be hackable in practice.[214] Last year, the Radiocommunications Agency Netherlands (AT) sounded the alarm in response to the rising number of unsecure IoT devices being linked to the internet.[215] For this purpose, the AT called for additional rules to be set and for the urgent establishment of minimum criteria.

Fundamental hardware vulnerabilities were also a relevant factor during this reporting period.[216,217] Exploitation of such vulnerabilities is becoming easier, meaning that this kind of exploitation outside laboratory conditions is becoming increasingly likely. No truly effective protection against these kinds of attacks exists.[218]

Complexity undermines resilience

A variety of studies[219] indicate that the complexity of the ever-evolving digital landscape will continue to increase, which in turn will increase the attack surface and make it more complex. The implementation of new applications in combination with existing (legacy) environments will give attackers a wider range of starting points from which they can attack organisations as well as increasingly enabling them to use generic services and easily available tools.

The organic growth and the relatively long service life of systems will result in an increasingly complicated landscape. Moreover, the increasing use of shared facilities such as partial products or complete cloud services makes it harder to maintain a clear picture of the situation and monitor it. In the past, such services were structured within individual organisations, although nowadays they are purchased by a wide range of parties and executed externally. These parties also call upon the services of subcontractors. Management of the ICT landscape is still contained within individual organisations, yet the execution thereof is becoming increasingly fragmented and spread across multiple parties. This causes a lack of clarity, creates new dependencies and increases the scope of attack. On the defensive side, the increasing level of complexity only amplifies the risk of vulnerabilities. This complexity also affects the data flows within large organisations and thus also the issues of responsibility for and insight into the data. The greater the levels of complexity and connectivity, the more challenging it is to establish a resilient digital infrastructure.

These increasing levels of complexity and connectivity makes it difficult for organisations to predict which vulnerabilities could be misused in the future and what measures must be taken now in order to guard against them. Organisations will be faced with unpleasant surprises such as unexpected incidents and cascade effects. These uncertainties, referred to as 'unknown unknowns', are the consequences of the digital infrastructure's complexity.

Sufficient incentives for improvement resilience?

6 Looking ahead to 2021

Geopolitical developments will further increase the threat from nation-state actors. This threat is amplified by the fundamental conflicts of interests between different countries and differences of opinion regarding international standards and values. Incentives to boost resilience do exist, although it is unclear whether they are sufficiently proportional to the applicable threat levels and interests. Technology and its dominant role in modern society appear to have created geopolitical tensions.

Digitisation has expanded the attack surface and caused both a growth of and a shift in the attention of actors to new and alternative strategic targets. Furthermore, the threat posed by criminals remains as high as ever. Disruptions and systems failures will have a greater impact on society in the future due to the complete dependence on digitised processes and systems. Artificial intelligence will be an interesting target for malicious actors, although it will also be a useful tool to defend against such actors.

Future effects of digitisation

Digitisation and an increase in the importance of digital security go hand in hand. Increasing levels of digitisation also affect threat levels and resilience.

Expansion and shift in relation to targets and scope of attack

Threat actors are focusing their attention on targets that are or could be of value to them. Partly because of the scalability of cyber crime, the threats posed by these factors remain high.[220] As a result of further technological developments and digitisation, threat actors are paying greater attention to a new range of valuable targets. Digitisation is increasing the attack surface for threat actors and expanding the range of attack opportunities. Digitisation affects the quantity, nature and value of digitised processes, data and connections. For example, the roll-out of 5G networks is expected to result in further expansion of possibilities relating to mobile networks. These improvements enable a whole range of new applications for the IoT, for example, in the automotive industry, healthcare and the media and entertainment sector. This enables organisations to integrate more processes as well as allowing more information to be collected and communicated via networks.[221] It will also make certain targets more attractive by increasing the potential returns of hacking them, e.g. for the purposes of sabotage. The commercial value of data sent via 5G networks in the future is expected to rise substantially[222] and the rising number of digitised processes will further expand the scope of attack and hence the opportunities for hackers to execute cyber attacks.

Greater impact of breakdowns and failures

Breakdowns and systems failures are also posing a greater threat. The more digitised society becomes, the more likely it is for breakdowns or failures to occur. The increasing levels of connectivity and interweaving of services will certainly be a factor in this trend as unexpected errors will always be a possibility when installing updates, for instance. The impact of a systems failure or breakdown can be substantial, especially when critical processes are affected.

Unexpected vulnerabilities

Increasing levels of digitisation also affect threat levels and resilience as it means even more potential targets have to be protected and a greater range of opportunities for both intentional misuse and unintentional systems failures must be taken into

account. Furthermore, defending against these threats is becoming more difficult due to the rising levels of complexity and connectivity, resulting in the appearance of unforeseen vulnerabilities.

Impact of impaired data integrity

Unintentional systems failures or intentional data manipulation can impair the integrity of data. It would appear that less attention is paid to these threats and the manifestations thereof. However, data manipulation can potentially have substantial impact and cause social disruption. For example, what would happen if property ownership data or bank balances were maliciously manipulated on a massive scale or corrupted as a result of a solar storm? What would happen when bank account balances were to be manipulated or corrupted on a large scale? Would the backups be sufficient, and even if they would, could they also be manipulated or corrupted? A precise answer to these questions is difficult to provide. Another type of data and system manipulation is the production, reproduction and/or distribution of 'deep fakes'. The consequences of possible intentional or unintentional impairment of data integrity are unclear, although they would appear to be potentially substantial.

Application of artificial intelligence

Another aspect of the ongoing digitisation of society is the development and application of artificial intelligence (AI). AI involves *'[...] self-learning systems that can independently (i.e. without human intervention) learn to perform new tasks and behaviour. These systems learn to recognise more and more patterns, to interpret human behaviour and to improvise. An ever-increasing number of systems are being given the responsibility to make important decisions based on their artificial cognitive skills.'*[223] AI applications assist humans with decision-making, for example, by identifying suspicious financial transactions or individuals with elevated risk profiles. Algorithms can also make decisions autonomously, e.g. in self-driving car systems.

AI an interesting target for malicious actors

AI can also be an attractive target for malicious actors, and the attraction is only going to grow in the future. Actors can attempt to manipulate algorithms or the data that they work with in order to influence the results.[224] Detection of such manipulation is a complex and time-consuming process. Researchers were able to illustrate this issue by manipulating the digital assistants Alexa, Siri and Google Assistant using hidden commands that had been added to audio or video files. In this way, malicious actors could potentially open doors or call certain telephone numbers without being detected.[225]

As well as enabling manipulation by malicious actors, AI can also deliver unexpected or unpredictable results.[226] The Dutch political party D66 is urging research to be conducted into Explainable Artificial Intelligence (XAI). XAI systems provide transparency into the decisions they make so that people can check them.[227] Strictly speaking, the factor of unexplainable or unpredictable results falls outside the scope of cyber security, although it does affect the integrity of processes.

AI a tool for both cyber attacks and cyber defence

n addition to being a target of cyber attacks, AI can also be used both to launch cyber attacks and to defend against them. For example, malicious actors could develop algorithms to discover what types of malware have the greatest chance of success under a range of different circumstances. They could also use AI to discover what type of users are the most susceptible to spear phishing or to search for vulnerabilities. On the other hand, AI can also be used to defend against cyber attacks in the form of prevention, protection, detection or response activities. For example, if a system administrator always logs in from location A and then suddenly logs in from location B, then algorithms can detect this anomaly and raise the alarm. Experts expect an arms race between developers of offensive and defensive AI, although attackers do not yet appear to be using AI at this time.[228]

Increasing geopolitical tension

Geopolitical tension between the major world powers is on the rise. As well as the United States, EU member states, the Russian Federation and China, other significant players include countries like Iran and North Korea. This tension has manifested itself in increasing assertiveness by China and Russia, growing nuclear uncertainty and deterioration of transatlantic relations. Furthermore, the global financial and economic order is being restructured and new networks are being forged. Examples of this include the growth in Chinese influence through the establishment of international standards; China's activism, which is challenging political unity within the EU; and the USA's protectionist policy.[229] These increasing tensions and shifts in the global financial and economic order are factors that affect cyber security.

Fundamental conflicts of interest increase the threat from nation-state actors

Fundamental clashes of interest between different countries amplify the threat posed by nation-state actors. After all, the internet is not merely a technical domain; it is also a political domain in which digital devices are increasingly being used for political or even military purposes. This can impact infrastructure, citizens and organisations within countries (collateral damage).[230] The traditional distinction between diplomatic reprisals or acts of war is no longer a black-or-white issue, with cyber attacks constituting a tool that blurs this boundary.

Threat posed to valuable targets

These threats predominantly affect specific targets that are attractive to nation-state actors, such as vital knowledge sectors, government bodies, military intelligence or units, critical processes and international organisations active in the

Netherlands. Some businesses expect that the trade war may cause a rise in the theft of sensitive commercial information by nation-state actors and businesses as well as disruption activities against governments, critical infrastructure and businesses.[231] In addition, attacks may be carried out on targets that could provide vital stepping stones for targeted cyber attacks in the future, such as entities that process personal data.

In addition to attacking the aforementioned targets, traditional and social media could also be potential targets. Nation-state actors can use cyber attacks to attempt to produce, reproduce and/or distribute disinformation in order to stoke tensions between or within countries or to portray their country in a more favourable light. The use of audio and/or video manipulation – in the shape of so-called 'deep fakes' – is also conceivable.

Differences of opinion concerning international standards and values increase the threat level

While the use of cyber attacks by nation-state actors has increased, there is insufficient consensus regarding international standards and values applicable in cyberspace. Western countries and a growing number of like-minded nations believe that the international rule of law applicable in the physical world should also apply in cyberspace, while a number of non-Western countries would like to see a new treaty framework on which they can exert influence. The lack of consensus raises the threat posed by nation-state actors as states don't feel obliged to comply with accepted standards.[232] Regulation of the internet at an international level is a complex challenge. There appears to be a joint need for widely applicable standards, although the issue of whether these standards will be Western or Russian/Chinese is a matter for heated debate.[233] In addition to the interest of a secure internet, the interest of an open and free internet is also very important. When it comes to maintaining an open and free internet, some countries respond to matters of privacy rights and jurisdictional issues in fundamentally different ways.[234]

Technological dominance potential source of tension

Technology and its dominant role in modern society has sparked major geopolitical tensions. Some believe that beneath the surface of the trade war between the US and China is a conflict with much deeper roots, namely a global struggle for technological dominance.[235] There are also concerns regarding possible misuse of products manufactured in a variety of nation states. In recent months, much has been said about the risks involved in using products created by Chinese companies – including Huawei – during the development of 5G networks. These risks are based on possible misuse by the Chinese state.[236] Separating ICT products from the countries in which they are manufactured is not a simple process. For example, typically American products like the iPhone are made in China and Chinese ICT products make extensive use of microchips designed in the US. In any event, a large volume of ICT products and components are made in China. However, who manufactures the products is less decisive than a number of other factors, such as who maintains them during their life cycle, who has administrative access to the products, who provides the updates and who provides the support. These factors enable more extensive and longer-term opportunities for misuse than manufacturing alone.

Effect of industrial politics on resilience

As a result of geopolitical developments, nation states are more critically examining businesses and products from certain countries. This can affect resilience levels, although it is difficult to evaluate this factor generically. This kind of 'industrial politics' can have a positive effect on resilience levels as it encourages implementation of mitigating measures, making potential misuse more difficult for nation-state actors. It can also result in greater awareness of risks, tougher cyber security measures and/or the deliberate choice to purchase and use a more diverse range of products. However, industrial politics also causes uncertainty regarding the reliability of certain ICT products, which in turn may lead to indifference ('there could be something wrong with any of them, so there's nothing we can do'). It is also conceivable that higher-quality or more secure products will no longer be available, which will lower resilience levels. Industrial politics can also potentially create a dilemma between short-term economic interests and long-term security interests.

Fragmentation of the internet conceivable

It is conceivable that fundamental conflicts of economic, political and military interests between countries may result in fragmentation of the internet, a phenomenon that has already occurred in a number of areas. For example, North Korea is completely cut off from the World Wide Web while China and Iran have substantial control of the data flows going in and out of their respective nations. In Russia, legislation is being designed to give the government greater control of the physical infrastructure of the Russian section of the internet. The EU has formulated specific privacy requirements, China is establishing requirements as part of a new cyber security law and Russia has done so via a privacy law. As a result, internationally operating organisations find it difficult to comply with all of these different legal frameworks. This reduces efficiency for these organisations, which affects the global economy at the macro level.[237] It is difficult to predict the consequences of a major fragmentation event for cyber security: on the one hand, it may affect the economy, although on the other, it could make nation states less vulnerable to attacks.

Are the incentives proportional to the threat level?

The role of cyber security in ensuring our society functions smoothly is substantially increasing and in view of geopolitical developments, it is conceivable that threat levels will continue to

rise. There is relatively little that individual organisations can do to influence geopolitical developments or the increasing levels of digitisation and dependence.

Consumers and supervisory bodies create incentives for organisations to take cyber security – including the more specific issue of privacy – more seriously. Some people expect government regulation and public opinion on privacy to become the main driving forces of data protection.[238]

In line with the Wbni, providers of essential services and digital service providers are also subject to a duty of care: they are obliged to implement appropriate and proportionate organisational and technical measures to manage risks to the security of their ICT systems, to prevent incidents and to restrict the consequences of incidents to the greatest extent possible.

The cabinet is also creating incentives to make cyber security a higher priority in addition to measures such as disincentivising unsafe hardware and software. Among other measures, the cabinet asserts that reinforcement of the resilience of citizens and organisations is necessary in order to capitalise on the opportunities that digitisation offers.[239] Via the Digitally Secure Hardware and Software Roadmap, the cabinet has created a package of measures to prevent unsecure hardware and software, detect vulnerabilities and mitigate the consequences of breaches.[240]

Wake-up calls from the past

The DigiNotar incident in 2011 was a wake-up call for the Dutch government concerning the importance of trust in data to Dutch society[241] and the KPN hack in 2012 hammered home the importance of cyber security to KPN's management team.[242] Wannacry and NotPetya – the total losses from which were estimated at between 4 and 8 billion and 10 billion respectively[243] – served as wake-up calls to governments around the world.[244]

Incentives to boost resilience do exist, although it is unclear whether they are sufficiently proportional to the applicable threat levels and interests. It is not easy to gauge how the resilience levels match up to developments concerning the interests and threats at hand.

Appendices

Appendix 1
NCSC statistics

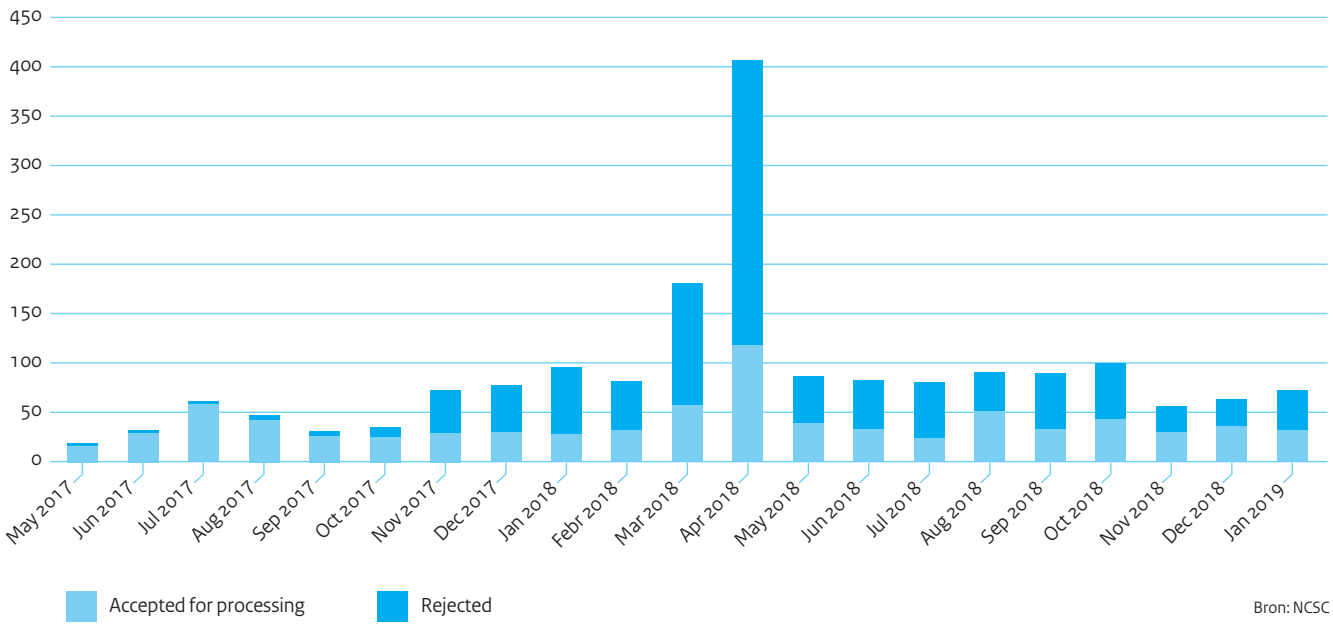
This appendix gives a rough overview of the relevant reports and incidents handled by the NCSC during the reporting period. The data used to compile the statistics was sourced from the NCSC registration systems. In this reporting period, the number of CVD reports remained more or less constant, although a substantially higher number of incident reports were processed.

Based on the available statistics, a number of conclusions can be drawn to a limited extent: a) the number of organisation affiliated with the NCSC and the National Detection Network (NDN) has increased over time, which complicates quantitative comparisons with past statistics; b) incident reports are made on a voluntary basis (with the exception of reports made under the statutory notification obligation[245]), which means it is unclear how the number of reports compares to the number of actual incidents detected; c) anomalous statistics are often influenced by multiple factors.

CVD reports remain a useful tool for detecting vulnerabilities

The NCSC receives and processes CVD (Coordinated Vulnerability Disclosure) reports in the interests of both its own infrastructure and the infrastructure of central government. CVD policy[246] enables people to notify system owners in the event they discover weak points in their ICT systems (especially websites). Any parties who report security problems that are as yet undetected will receive a token of appreciation in return for their assistance.

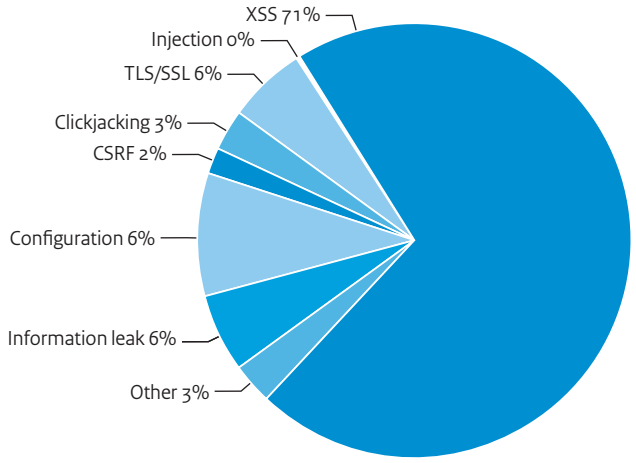
Figure 4 Number of CVD reports



Bron: NCSC

The number of CVD reports has remained the same compared with the previous reporting period. After peaking strongly in March and April 2018, the levels have returned to those observed in the months prior thereto. The substantial increase of rejected reports in the previous reporting period (e.g. due to verification of the problem proving fruitless or the reported problem already having been identified) has not continued to rise in this reporting period, although the number remains as high as ever.

Figure 5 Type of CVD reports



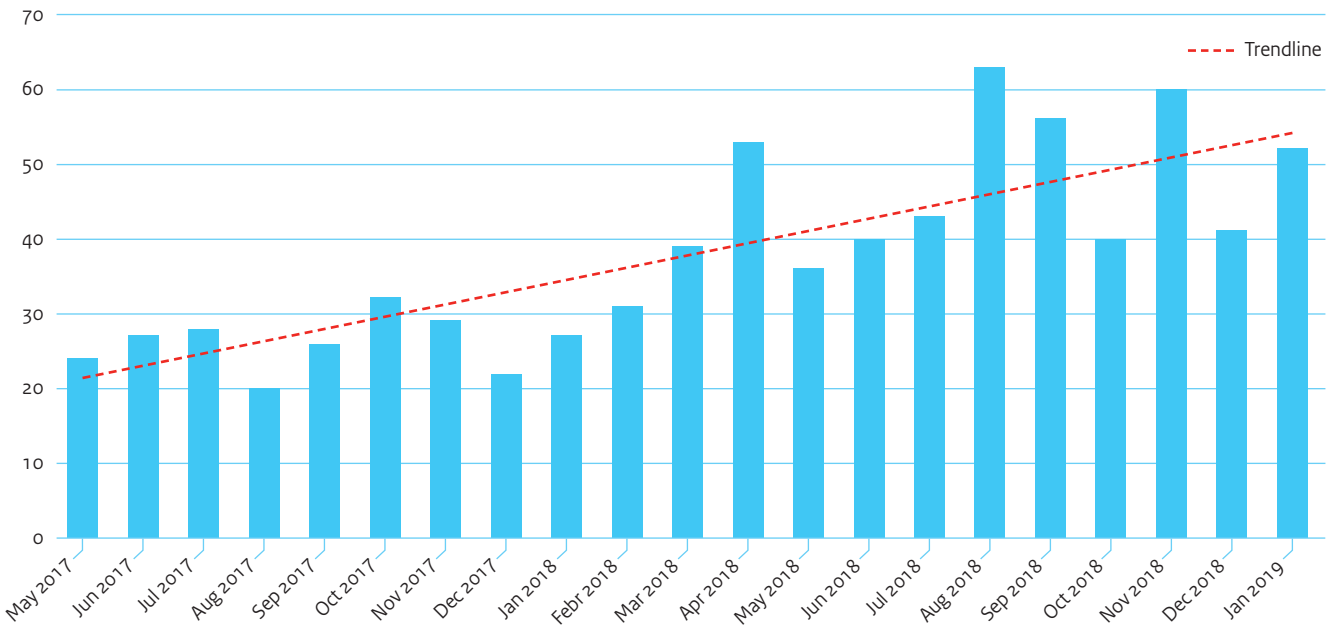
Source: NCSC

Increase in number of processed incidents

The NCSC provides support to central government and organisations involved in critical processes in order to facilitate processing of cyber security incidents. Organisations report incidents and vulnerabilities to the NCSC. The NCSC also identifies such security flaws itself based on detection mechanisms and in-house investigations, among other methods. Furthermore, on request by national and international parties, the NCSC works with Dutch internet service providers to support them in the fight against cyber incidents originating in the Netherlands (e.g. from a rogue web server or from infected computers in the Netherlands).

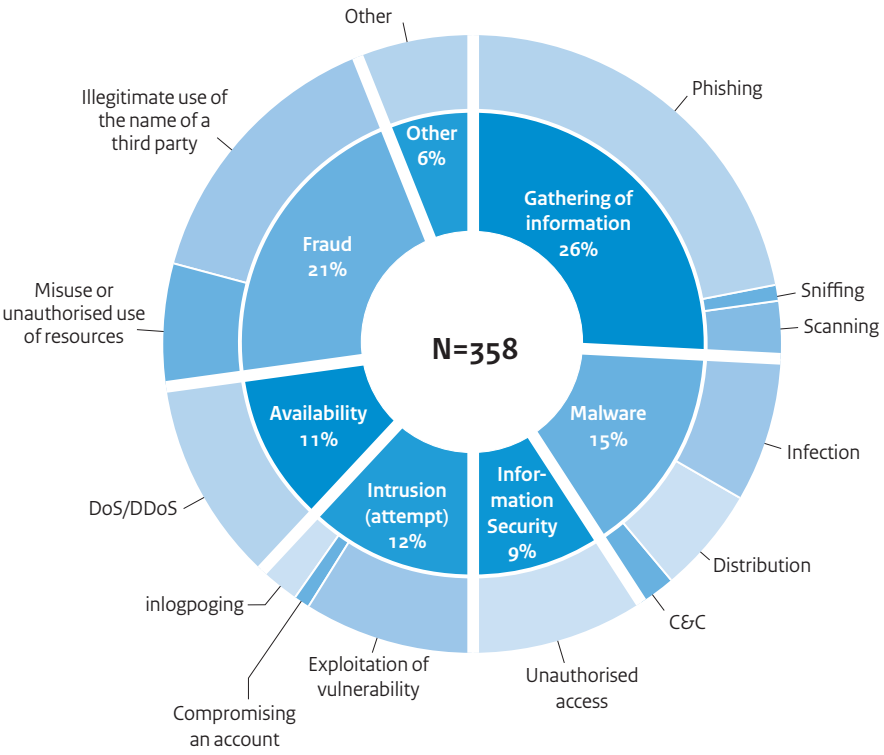
On average, 48 incidents per month were registered and processed during the reporting period. This is an increase of 50% compared to the previous reporting period, when the trend was slightly declining. The main reason for this increase is that more organisations have joined the NCSC's initiative, as well as the fact that organisations seem to be more willing to report them. During the reporting period, one report was made in line with the statutory notification obligation by an organisation in the critical sector. This report concerned an incident in which the criteria for making a statutory report could potentially have been infringed upon, although this eventuality did not materialise.
The main shifts in the prevalence of types of incidents compared to the previous reporting period are a decline in the number of malware reports and an increase in the number of fraud-related reports.

Figure 6 Incidents handled (excluding automated checks)



Source: NCSC

Figure 7 Number of reports per incident category



Bron: NCSC

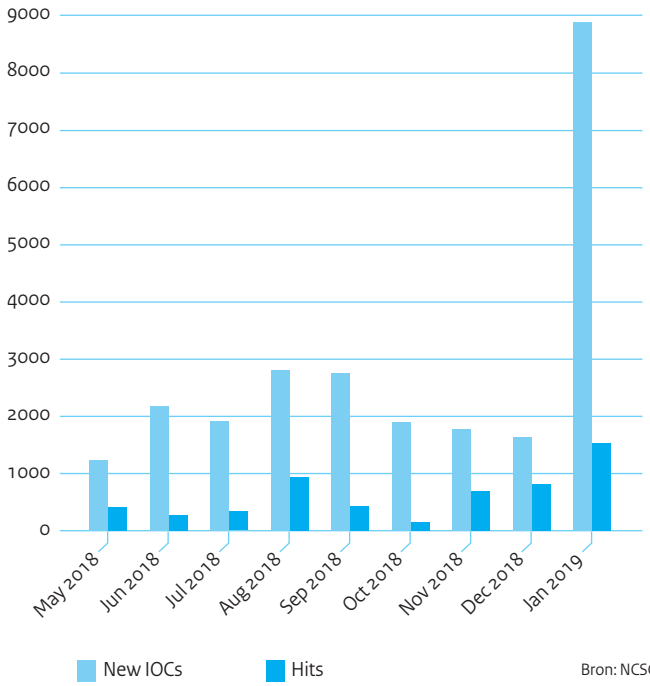
The substantial decline in the number of reports of malware infections is particularly striking. Detection and mitigation are becoming commonplace, meaning these factors are less likely to be reported. The number of automated reports of infections, which was not included in this summary, remained the same compared to the previous reporting period.

The rise in fraud incidents particularly stems from an increase in reported phishing campaigns and corresponding requests to take down the servers used for these campaign. In this regard, the label 'fraud' relates to the wrongful use of organisation names when sending phishing emails.

Rise in National Detection Network partners

The National Detection Network (NDN) is a collaboration to enable better and faster detection of digital threats and risks. By sharing information on threats, the parties can implement timely and appropriate measures on their own responsibility in order to prevent or mitigate possible damage. Within the NDN, indicators of compromise (IoCs) are shared with participants. IoCs provide

Figure 8 New IoC's and Hits



Bron: NCSC

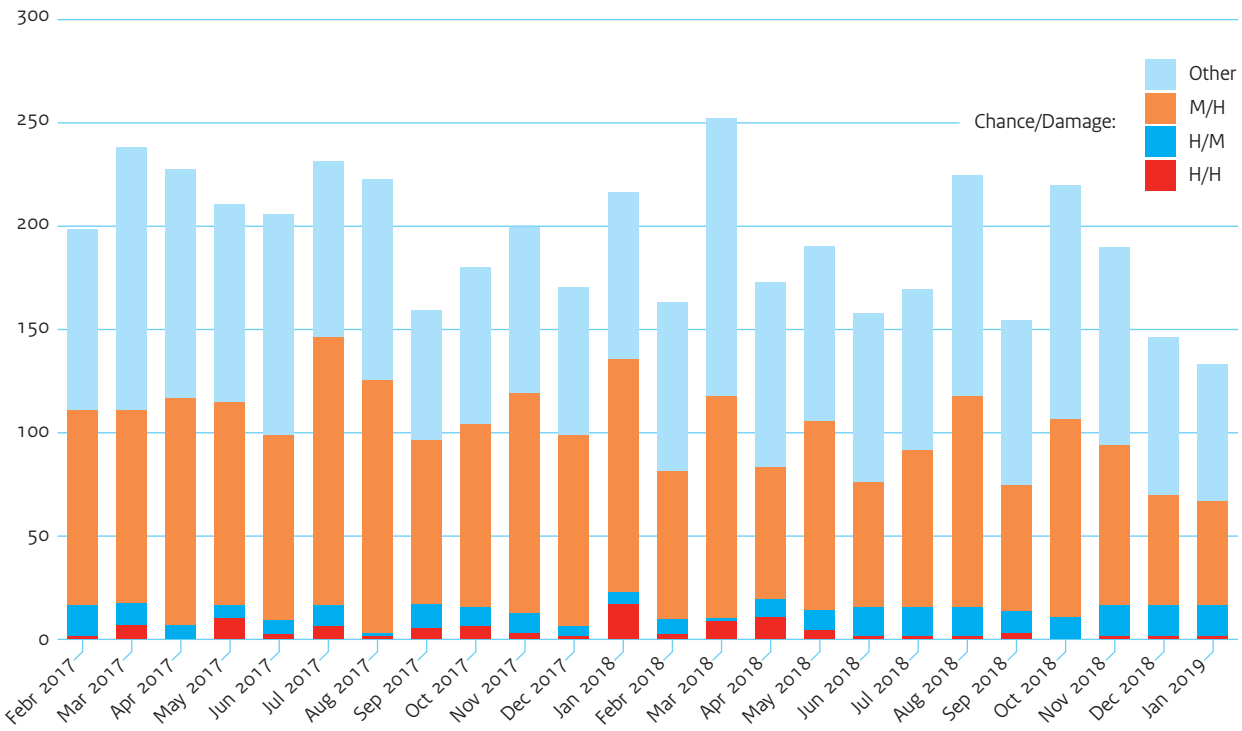
information that can help to identify specific rogue activity within a system or network, such as IP addresses or domain names. When a shared IoC results in detection of rogue activity by one of the participants, this is referred to as a 'hit'.

A hit only indicates that activity has been detected that matches the information shared and does not necessarily mean that the participant in question has been compromised. If a defensive measure such as a firewall, antivirus program or intrusion detection system (IDS) repels the rogue software or network traffic, then this is registered as a hit despite no actual infection having taken place. In January 2019, a number of new parties joined the MISP platform, which also shares IoCs. This resulted in a peak of new indicators and a substantially higher number of hits than in the months prior thereto.

Slightly fewer security recommendations issued

The NCSC publishes security recommendations based on software or hardware vulnerabilities or detected threats. These security recommendations describe what the problem is, which systems could be affected and what can be done to prevent vulnerabilities from being abused. The NCSC's security recommendations specify two particular factors: the possibility of the vulnerability being abused and the damage that would be caused were this to happen. A level – either high (H), medium (M) or low (low) – is subsequently defined for both criteria (possibility and damage) based on consideration of multiple aspects. The table below displays the security recommendations issued during this reporting period and the previous reporting period, with the number of urgent security recommendations (H/H, M/H, H/M) displayed separately. The number of security recommendations issued in the recent period declined slightly in the last period, with a notable decline in the number of H/H recommendations.

Figure 9 Security recommendations issued



Bron: NCSC

Appendix 2
Terms and abbreviations

0-day	See Zero-day vulnerability.
Accessibility	Accessibility relates to the process of guaranteeing that all data and related company resources (information systems) that users are authorised to access are available to them at the right moments.
Actor	A person, group or organisation that poses a threat.
AIVD	Algemene Inlichtingen- en Veiligheidsdienst [General Intelligence and Security Service]
AP	Autoriteit Persoonsgegevens [Dutch Data Protection Authority]
Attack	A cyber attack is an intentional infringement of cyber security.
Attack facilitator	An actor that develops and exploits tools and infrastructure in order to enable other actors to execute cyber attacks in exchange for money.
Authentication	Ascertaining the identity of a user, computer or application.
Bitcoin	Digital currency, see cryptocurrency.
Botnet	A collection of infected systems that can be centrally controlled by actors. Botnets constitute the infrastructure for many types of internet crime.
Breakdown	See 'failure' or 'disruption'.
Cloud service	ICT infrastructure made available as a service via the internet.
Confidentiality	Confidentiality relates to the process of guaranteeing that data is only accessible to the parties who are authorised to access it.
Criminal	An actor that conducts attacks based on economic or financial motives.
Cryptocurrency	An umbrella term for digital currencies whereby cryptographic calculations are used as authenticity feature and for transactions.
Cryptojacking	Using the computing power of systems to extract cryptocurrency without the knowledge of the system owner.

Cryptomining	Extracting cryptocurrency by conducting cryptographic calculations.
CVD	Coordinated vulnerability disclosure: the practice of coordinated reporting of detected security breaches. Coordinated vulnerability disclosure is based on agreements that usually mean that the reporting party will not share their discovery with third parties until the leak has been repaired, and the affected party will not take legal action against the reporting party. This was previously known as responsible disclosure.
Cyber crime	Form of crime aimed at an ICT system or the information processed by this ICT system. There are various types of cyber crime: • in a narrow sense, a type of crime targeting ICT (high-tech crime); • a type of crime that is predominantly executed using ICT (cyber crime); • in a broad sense, any form of crime that makes use of ICT in some way (digitised crime).
Cyber security	Cyber security is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to repair it should this damage occur. This damage could consist of impairment of the accessibility, confidentiality or integrity of information systems and information services and the data contained therein.
Cyber vandal	See script kiddie.
Cybercrime-as-a-service (CaaS)	Cybercrime-as-a-service is a method used in the underground economy in which actors can use the services of others (paid or otherwise) to commit cyber crime.
Data manipulation	Intentionally editing data; impairing the integrity of data.
Data theft	Impairment of the confidentiality of information by means of the copying or removal of data.
DDoS	Distributed Denial of Service is a form of Denial of Service in which a certain service (e.g. a website) is made inaccessible by swamping it with a large volume of network traffic from a large number of different sources.
Defacement	A defacement is the replacement of a web page with the message that it has been hacked, possibly featuring additional messages of an ideological, activist or provocative nature.
Disruption	Intentional temporary impairment of the accessibility of data, information systems or information services.
DKIM	DomainKeys Identified Mail is a protocol that allows the sending e-mail server to place digital signatures in legitimate e-mails. 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 e-mails from their domain. The authenticity of e-mails 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 links internet domain names to IP addresses and vice versa. For example, the website 'www.ncsc.nl' represents IP address '159.46.193.36'. Among other things, DNS records also specify how e-mails to that domain should be processed.
DoS	Denial of Service is the name of a type of attack whereby a particular service (for example a website) is made inaccessible to the customary users of that service. For websites, a DDoS attack is usually executed.

Encryption	Encoding information to make it unreadable for unauthorised persons.
Espionage	Impairment of the confidentiality of information by means of the copying or removal of data by nation-state actors or nation-state-affiliated actors.
Exploit	Software, data or a series of commands that exploit a hardware or software vulnerability for the purpose of creating undesired functions or behaviour.
Exploit kit	A tool used to set up an attack by choosing from ready-made exploits, in combination with desired effects and method of infection.
Failure	Impairment of integrity and accessibility due to natural causes, technical difficulties or human error.
Hacker/Hacking	The most conventional definition for a hacker (and the one used in this document) is someone who attempts to break into ICT 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: an actor who launches activist digital attacks motivated by a certain ideology.
ICS	Industrial Control Systems are measurement and control systems used, for example, to control industrial processes or building management systems. Industrial control systems collect and process measurement and control signals from sensors in physical systems and steer the corresponding machines or devices.
Incident	An incident is an event in which data, information systems or information services fail or are disrupted or misused.
Information security	Information security is the process of verifying the required reliability of information systems in terms of confidentiality, accessibility and integrity, as well as establishing, maintaining and monitoring a cohesive package of corresponding measures.
Injection	A cyber attack method in which user input is manipulated to contain system commands as well as data. SQL injection is often used to influence communication between an application and the underlying database for the purposes of data theft.
Insider	An internal actor who forms a threat from within due to their access to systems or networks, motivated by revenge, financial gain or ideology. Insiders can also be hired or externally commissioned.
Integrity	Integrity relates to the process of verifying the accuracy and completeness of data and the processing thereof.
IoT	The Internet of Things is a network of smart appliances, sensors and other objects (often connected to the internet) that collect data on their environment, can exchange this data and make autonomous or semi-autonomous decisions and/or take actions that affect their environment based on it.
IP	The Internet Protocol handles the addressing of internet traffic to ensure it arrives at the intended destination.
Leak	Impairment of confidentiality due to natural causes, technical difficulties or human error.

Malware	Contraction of malicious software. Malware is used as a generic term for viruses, worms and Trojans, amongst other things.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst [Military Intelligence and Security Service]
Nation-state actor	Nation states that execute cyber attacks on other nation states, organisation or individuals, primarily based on geopolitical motives. Their goal is to obtain strategically important data (espionage), exercise influence on public opinion or democratic processes (influencing) or to disrupt (disruption) or even destroy (sabotage) critical systems.
Phishing	An umbrella term for digital activities with the objective of tricking people into giving up data. This data can then be misused for the purposes of fraud or identity theft.
Ransomware	A type of malware that blocks systems or the information they contain and only makes them accessible again in return for payment of a ransom.
Sabotage	Intentional and very long-term impairment of the accessibility of data, information systems or information services. In extreme cases, this can result in destruction.
Script kiddie	Actor with limited knowledge who draws on tools which have been devised and developed by others in order to conduct cyber attacks, to demonstrate vulnerabilities or simply as a challenge to themselves.
Spam	Unwanted email, generally commercial in nature.
Spear phishing	Spear phishing is a version of phishing that is targeted specifically against one person or a specific group of persons due to their position of access, in order to achieve as widespread 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 e-mails on behalf of his domain. The owner of the domain name publishes the list of authorised servers in a DNS record.
State-affiliated actor	An actor affiliated with a nation-state actor.
System manipulation	Impairment of information systems and information services focusing on the confidentiality or integrity of these systems/services. These systems or services are subsequently used to carry out other attacks.
Terrorist	Actor with ideological motives who endeavours to realise social change, spread fear among population groups or influence political decision-making processes by using violence against people or by causing disruptive damage.
Tool	A technology or computer program used by an attacker to exploit or increase existing vulnerabilities.
Trojan	A type of malware that secretly grants the attacker access to a system via a back door.
Two-factor authentication	A method of identity verification requiring two independent proofs of identity.

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 approach it without the proper authorisation.
Wiperware	A type of malware that conducts sabotage by removing data or making it permanently inaccessible.
Worm	A type of malware that automatically spreads itself to other systems.
Zero-day vulnerability	A zero-day vulnerability is a vulnerability for which no patch is yet available because the developer of the vulnerable software has not yet had time (zero days) to resolve the vulnerability.

Appendix 3
Sources and references

1 Dutch National Cyber Security Agenda 2018.

2 NCTV, *Cyber Security Assessment Netherlands 2018*, June 2018. https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.

3 *General Intelligence and Security Service (AIVD)*, Jaarverslag 2018 [2018 Annual Report], April 2019.

4 NCTV, *Cybersecurity Assessment Netherlands*, June 2018. https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.

5 ENISA, *ENISA Threat Landscape Report 2018* (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

6 *Anonymous defaced Russia govt website against Telegram ban*, Security Affairs, 16-05-2018. https://securityaffairs.co/wordpress/72567/hacktivism/anonymous-hask-russia-site.html Consulted on 04-02-2019.

7 *DDOS on Bank of Spain Claimed by Anonymous Catalonia*, Latest Hacking News, 03-09-2018https://latesthackingnews.com/2018/09/03/ddos-on-bank-of-spain-claimed-by-anonymous-catalonia/ Consulted on 11-02-2019.

8 *Flink meer DDoS-aanvallen, 'vaak jongeren vanaf hun zolderkamer* [Substantial increase in DDoS attacks, 'often by young people from their bedrooms'], NOS.nl, 06-01-2019. https://nos.nl/artikel/2266370-flink-meer-ddos-aanvallen-vaak-jongeren-vanaf-hun-zolderkamer.html Consulted on 04-02-2019.

9 *Banken waren opnieuw doelwit van ddos-aanval* [Banks targeted by another DDoS attack], Tweakers 28-05-2018 https://tweakers.net/nieuws/139053/banken-waren-opnieuw-doelwit-van-ddos-aanval.html Consulted on 04-02-2019.

10 *DDoS-aanval belasting en douane* [DDoS attack on tax and customs authorities], NOS.nl, 10-05-2019. https://nos.nl/artikel/505247-ddos-aanval-belasting-en-douane.html Consulted on 04-02-2019.

11 *Kort problemen met website DigiD door DDoS-aanval* [Brief problems with DigiD website due to DDoS attack], NOS.nl, 31-07-2018. https://nos.nl/artikel/2244007-kort-problemen-met-website-digid-door-ddos-aanval.html Consulted on 04-02-2019.

12 *PyCryptoMiner botnet, a new Crypto-Miner Botnet spreads over SSH*, Security Affairs, 05-01-2018. http://securityaffairs.co/wordpress/67408/breaking-news/pycryptominer-botnet-miner.html Consulted on 04-02-2019.

13 ENISA, *ENISA Threat Landscape Report 2018* (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

14 *Cryptominer infecteert 157.000 ongepatchte MikroTik-routers* [Cryptominer infects 157,000 unpatched MikroTik routers], Security.nl, 15-08-2018. https://www.security.nl/posting/573546/Cryptominer+infecteert+157_000+ongepatchte+MikroTik-routers Consulted on 11-02-2019.

15 Trend Micro, *Unseen Threats and Imminent Losses: Midyear Security Roundup 2018* (2018).https://documents.trendmicro.com/assets/rpt/rpt-2018-Midyear-Security-Roundup-unseen-threats-imminent-losses.pdf

16 Radhesh Krishnan Konoth, Emanuele Vineti, Veelasha Moonsamy, Martina Lindorfer, Christopher Kruegel, Herbert Bos, and Giovanni Vigna, 'MineSweeper: An In-depth Look into Drive-by, Cryptocurrency Mining and Its Defense', *CCS '18: 2018 ACM SIGSAC Conference on Computer &Communications Security Oct. 15-19-2018, Toronto, ON, Canada* (2018).https://www.cs.vu.nl/~herbertb/download/papers/minesweeper_ccs18.pdf.

17 *Jaarverantwoording politie 2018* [Police Annual Report 2018], May 2019

18 *National Security Council cyber chief: Criminals are closing the gap with nation-state hackers*, 25-04-2019, https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/

19 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's* [3.81 million euros in damage due to phishing attacks on internet banking services in 2018 - Less fraud involving bank cards and direct debit payments], 27-3-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, Consulted on 27-3-2019.

20 Cyber Edge Group, *2018 Cyberthreat Defense Report: North America, Europe, Asia Pacific, Latin America, Middle East, Africa* (2018). https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf.

21 DNI, *Worldwide Threat Assessment of the U.S. Intelligence Community 2019* (2019).https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

22 N. Perlroth and C. Krauss, 'A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try', *The New York Times*, 15-03-2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html Consulted on 04-02-2019.

23 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', *Reuters*, 04-09-2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX Consulted on 11-02-2019.

24 *General Intelligence and Security Service (AIVD)*, Jaarverslag 2018 [2018 Annual Report], April 2019.

25 *GreyEnergy groep richt zich op vitale infrastructuur, mogelijk in voorbereiding op schadelijke aanvallen* [GreyEnergy group targets critical national infrastructure, possibly in preparation for larger-scale attacks], ESET, 17-10-2018. https://www.eset.com/nl/over/newsroom/persberichten-overzicht/persberichten/greyenergy-groep-richt-zich-op-vitale-infrastructuur/ Consulted on 11-02-2019.

26 A. Greenberg, 'Crash Override': The Malware That Took Down a Power Grid', *WIRED*, 12-06-2017. https://www.wired.com/story/crash-override-malware/ Consulted on 11-02-2019.

27 C. Osborne, 'Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout', *Zero Day* via *ZDNet*, 30-04-2018. https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/ Consulted on 11-02-2019.

28 J. Stubbs, 'Hackers accused of ties to Russia hit 3 E.European companies- cybersecurity firm', *Reuters*, 17-10-2018. https://www.reuters.com/article/russia-cyber/hackers-accused-of-ties-to-russia-hit-3-eeuropean-companies-cybersecurity-firm-idUSL8N1WP37F Consulted on 14-02-2019.

29 S. Jewkes and J. Finkle, 'Saipem says Shamoon variant crippled hundreds of computers', *Reuters*, 12-12-2018. https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA Consulted on 14-02-2019.

30 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', *Reuters*, 04-09-2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX Consulted on 11-02-2019.

31 A. Shalal, 'Germany concerned about possible 'sleeper' cyber sabotage', *Reuters*, 04-09-2018. https://www.reuters.com/article/us-germany-security/germany-concerned-about-possible-sleeper-cyber-sabotage-idUSKCN1LK1DX Consulted on 11-02-2019.

32 *General Intelligence and Security Service (AIVD)*, Jaarverslag 2018 [2018 Annual Report], April 2019.

33 *General Intelligence and Security Service (AIVD)*, Jaarverslag 2018 [2018 Annual Report], April 2019.

34 *General Intelligence and Security Service (AIVD)*, Jaarverslag 2018 [2018 Annual Report], April 2019.

35 Once again, the threat matrix is based on the actor typology in *'Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment'*, by M. de Bruijne, M. van Eeten, C. Hernandez Ganan and W. Pieters (TU Delft, 2017).

36 DNI, *Worldwide Threat Assessment of the U.S. Intelligence Community 2019* (2019), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

37 *Jaarverslag 2018* [Annual Report 2018], General Intelligence and Security Service (AIVD), April 2019.

38 ENISA, *ENISA Threat Landscape Report 2018* (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 .

39 *Jaarverantwoording politie 2018* [Police Annual Report 2018], May 2019.

40 Sophos, *Sophoslabs 2019 Threat Report* (2018), https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-2019-threat-report.pdf.

41 NCTV, *Cybersecuritybeeld Nederland 2018* [Cyber Security Assessment Netherlands 2018], June 2018, https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.

42 FireEye, *Facing Forward: Cyber Security in 2019 and Beyond* (2018), https://content.fireeye.com/predictions/rpt-security-predictions-2019.

43 I. Arghire, 'Supply Chain Attacks Nearly Doubled in 2018: Symantec', *SecurityWeek* 20-02-2019,https://www.securityweek.com/supply-chain-attacks-nearly-doubled-2018-symantec, consulted on 24-02-2019.

44 B. Barrett, 'How China's Elite Hackers Stole the World's Most Valuable Secrets', *WIRED* 20-12-2018, https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/, consulted on 24-02-2019.

45 Stilgherrian, 'At least nine global MSPs hit in APT10 attacks: ACSC', *ZDNet* 21-12-2018, https://www.zdnet.com/article/at-least-nine-global-msps-hit-in-apt10-attacks-acsc/, consulted on 24-02-2019.

46 M. Hirani, S. Jones and B. Read, 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', *FireEye Threat Research*, 09-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html, consulted on 24-02-2019.

47 *Jaarverslag 2018* [Annual Report 2018], General Intelligence and Security Service (AIVD), April 2019.

48 L. van Lonkhuyzen and V. Sondermeijer, '*MIVD verijdelde Russische cyberaanval op OPCW in Den Haag*' [MIVD thwarts Russian cyber attack on OPCW in The Hague], NRC.nl, 04-10-2018, https://www.nrc.nl/nieuws/2018/10/04/mivd-verijdelde-russische-cyberaanval-op-opcw-in-den-haag-a2186350, consulted on 24-02-2019.

49 A. Greenberg, *How Russian Spies Infiltrated Hotel Wi-Fi to Hack Victims Up Close*, 04-10-2018, https://www.wired.com/story/russian-spies-indictment-hotel-wi-fi-hacking/, consulted on 24-02-2019.

50 Central government (2018), https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/11/19/aanbiedingsbrief-bij- defensie-cyber-strategie/Kamerbrief+MinDef+aanbieding+Defensie+Cyber+Strategie.pdf.

51 G Myre, *The U.S. Pledges A Harder Line In Cyberspace — And Drops Some Hints*, 26-03-2019, https://www.npr.org/2019/03/26/705822275/the-u-s-pledges-a-harder-line-in-cyberspace-and-drops-some-hints?t=1553760003987, consulted on 28-03-2019.

52 NCTV, *Cybersecuritybeeld Nederland 2018* [Cyber Security Assessment Netherlands 2018], June 2018, https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf.

53 *Flink meer DDoS-aanvallen, 'vaak jongeren vanaf hun zolderkamer* [Substantial increase in DDoS attacks, 'often by young people from their bedrooms'], NOS.nl, 06-01-2019, https://nos.nl/artikel/2266370-flink-meer-ddos-aanvallen-vaak-jongeren-vanaf-hun-zolderkamer.html, consulted on 04-02-2019.

54 *Schade banken door phishing neemt explosief toe* [Explosive rise in losses incurred by banks due to phishing activities], NOS.nl, 27-03-2019, https://nos.nl/artikel/2277755-schade-banken-door-phishing-neemt-explosief-toe.html , consulted on 27-03-2019.

55 *Phishing weer groeiend probleem, oplichters steeds creatiever* [Phishing problem rises again, fraudsters becoming increasingly creative], NOS.nl, 25-11-2018, https://nos.nl/artikel/2260753-phishing-weer-groeiend-probleem-oplichters-steeds-creatiever.html, consulted on 11-02-2019.

56 *Jaarverantwoording politie 2018* [Police Annual Report 2018], May 2019.

57 *National Security Council cyber chief: Criminals are closing the gap with nation-state hackers*, 25-04-2019, https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/.

58 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's* [3.81 million euros in damage due to phishing attacks on internet banking services in 2018 - Less fraud involving bank cards and direct debit payments], 27-03-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, consulted on 27-03-2019.

59 *Banken waren opnieuw doelwit van ddos-aanval* [Banks targeted by another DDoS attack], Tweakers, 28-05-2018, https://tweakers.net/nieuws/139053/banken-waren-opnieuw-doelwit-van-ddos-aanval.html, consulted on 04-02-2019.

60 *DDoS-aanval belasting en douane* [DDoS attack on tax and customs authorities], NOS.nl, 10-05-2019, https://nos.nl/artikel/505247-ddos-aanval-belasting-en-douane.html, consulted on 04-02-2019.

61 *Kort problemen met website DigiD door DDoS-aanval* [Brief problems with DigiD website due to DDoS attack], NOS.nl, 31-07-2018, https://nos.nl/artikel/2244007-kort-problemen-met-website-digid-door-ddos-aanval.html, consulted on 04-02-2019.

62 *Opnieuw DDoS-aanval op website DigiD* [Another DDoS attack on the DigiD website], NOS.nl, 01-08-2018, https://nos.nl/artikel/2244113-opnieuw-ddos-aanval-op-website-digid.html , consulted on 04-02-2019.

63 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 23.

64 *Oorzaak computerstoring treinverkeersleiding gevonden* [Cause of rail traffic control computer failure identified], ProRail, 22-08-2018, https://prorail.nl/nieuws/oorzaak-computerstoring-treinverkeersleiding-gevonden, consulted on 24-02-2019.

65 *2019 Forcepoint Cybersecurity Predictions Report*, Forcepoint, 13-11-2018, https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf.

66 https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/

67 *Kaspersky Security Bulletin: THREAT PREDICTIONS FOR 2019*, Kaspersky Lab, 16-11-2018, https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878.

68 Ministry of Economic Affairs and Climate Policy, *Nederlandse digitaliseringsstrategie* [Dutch Digitisation Strategy], June 2018.

69 *Kabinet stopt EUR 165 miljoen in agenda digitale overheid* [Cabinet invests EUR 165 million in the digital-government agenda], Digitaleoverheid.nl, 17-08-2018, https://www.digitaleoverheid.nl/nieuws/kabinet-stopt-eur-165-miljoen-in-agenda-digitale-overheid/, consulted on 25-01-2019.

70 *VWS trekt zestig miljoen euro uit voor digitale zorg* [Ministry of Health, Welfare and Sport sets aside 60 million euros for digital care], Computable.nl, 19-9-2018, https://www.computable.nl/artikel/nieuws/overheid/6458649/250449/vws-trekt-zestig-miljoen-euro-uit-voor-digitale-zorg.html, consulted on 25-1-2019.

71 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 23.

72 *Resultaten self-assessment intersectorale afhankelijkheden* [Results of self-assessment into intersectoral dependencies], Netherlands Organisation for Applied Scientific Research and the Ministry of Justice and Security, 06-03-2019.
73 *Wat te doen als alles instort?* [What should I do if everything falls apart?], De Telegraaf, 25-09-2018.
74 Centre for European Policy Studies (CEPS), Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force (November 2018), p. 32.
75 Wouter van Noort, *Een voor een springen alle schermen op zwart* [One by one, the screens all went black], NRC, 06-10-2018.
76 Radiocommunications Agency Netherlands (AT), Verslag '*Opstap naar weerbaarheid in een digitale samenleving* [Report 'The road to resilience in a digital society'], 29-11-2018, https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2018/11/29/verslag-en-presentaties-opstap-naar-weerbaarheid-in-een-digitale-samenleving/Verslag+website+def.pdf, consulted on 28-01-2019.
77 *Wat te doen als alles instort?* [What should I do if everything falls apart?], De Telegraaf, 25-09-2018.
78 https://www.leidschdagblad.nl/cnt/dmf20190212_7504697/digitale-oorlog-minstens-zo-destructief?utm_source=google&utm_medium=organic.
79 https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.
80 *5G networks raise China espionage fears*, The Washington Times, 04-01-2019, https://www.washingtontimes.com/news/2019/jan/3/5g-networks-raise-china-espionage-fears/, consulted on 06-02-2019.
81 *G20: meer inzicht nodig in invloed digitale platforms op bedrijven en consumenten* [G20: greater insight required into the influence of digital platforms on businesses and consumers], Rijksoverheid.nl, 25-08-2018, https://www.rijksoverheid.nl/actueel/nieuws/2018/08/25/g20-meer-inzicht-nodig-in-invloed-digitale-platforms-op-bedrijven-en-consumenten, consulted on 06-02-2019. Kabinet wil meer inzicht in invloed van digitale platformen [Government wants greater insight into influence of digital platforms], Security.nl, 26-08-2018, https://www.security.nl/posting/574726/Kabinet+wil+meer+inzicht+in+invloed+van+digitale+platformen, consulted on 06-02-2019.
82 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 23-24.
83 *Het Analistennetwerk Nationale Veiligheid noemt Israël als derde land* [The National Security Analysts Network classifies Israel as a third country],
84 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 24.
85 *Welke deuren zet een topdeal met China open?* [What doors will a major deal with China open?], De Volkskrant, 16-10-2018, Chinese 'playbook' alarms FBI, Washington Post, 13-12-2018, Laurens Cerulus, China's ghost in Europe's telecom machine, Politico, 11-12-2017 (updated 28-01-2018).
86 *Europa overtuigen om geen Huawei te kopen 'topprioriteit' voor VS* [Convincing Europe not to do business with Huawei a 'top priority' to the US], Nu.nl, 05-02-2019, consulted on 06-02-2019.
87 *VS waarschuwt bondgenoten voor samenwerking met Huawei* [US warns allies against collaboration with Huawei], NOS, 11-03-2019, https://nos.nl/artikel/2275571-vs-waarschuwt-bondgenoten-voor-samenwerking-met-huawei.html.
88 Ministry of Economic Affairs and Climate Policy, *Nederlandse digitaliseringsstrategie* [Dutch Digitisation Strategy], June 2018, p. 34-36.
89 Joost Witteman, Erik Brouwer and Tom Smits, *Data zijn geen productiefactor, maar wel productiviteitsverhogend*, [Data is not a factor of production in itself, but it does boost productivity], in Economisch Statistische Berichten, Verplichte datadeling, Volume 103, 05-07-2018, p. 294-297.
90 NCTV, *Cyber Security Assessment Netherlands 4*, 2014.
91 *Duitse toezichthouder gaat dataverzameling Facebook aanpakken* [German supervisory body to tackle data collection by Facebook], Security.nl, 14-01-2019, https://www.security.nl/posting/594076/%22Duitse+toezichthouder+gaat+dataverzameling+Facebook+aanpakken%22, consulted on 05-02-2019. See also: Facebook gaf bedrijven toegang tot privéberichten gebruikers [Facebook granted businesses access to users' private messages], Security.nl, 19-12-2018, https://www.security.nl/posting/591518/%22Facebook+gaf+bedrijven+toegang+tot+priv%C3%A9berichten+gebruikers%22, consulted on 05-02-2019.
92 *New study: Google manipulates users into constant tracking*, Forbrukarrådet, 27-11-2018, https://www.forbrukerradet.no/forside/om-oss/, consulted on 05-02-2019. 50.000 Nederlanders tekenen petitie tegen locatie-opslag Google [50,000 Dutch people sign petition against Google's storage of location data], Security.nl, 22-01-2019, https://www.security.nl/posting/594944/50_000+Nederlanders+tekenen+petitie+tegen+locatie-opslag+Google, consulted on 05-02-2019.
93 '*Facebook riskeert in VS miljardenboete om privacyschendingen*' [Facebook risks multibillion-dollar fine for privacy violations], Nu.nl, 15-02-2019, https://www.nu.nl/internet/5744283/facebook-riskeert-in-vs-miljardenboete-om-privacyschendingen.html, consulted on 16-02-2019.

94 *Facebook staat toe advertenties te richten op vaccinatieweigeraars* [Facebook authorises targeted advertising to antivaccinationists], NOS.nl, 16-02-2019, https://nos.nl/artikel/2272187-facebook-staat-toe-advertenties-te-richten-op-vaccinatieweigeraars.html, consulted on 16-02-2019.
95 *Felle Britse kritiek op socialemediabedrijven* [Britain strongly criticises social-media companies], De Volkskrant, 18-02-2019.
96 NCTV, *Cybersecuritybeeld Nederland 2018* [Cyber Security Assessment Netherlands 2018], June 2018, https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf, consulted on 06-02-2019.
97 *GreyEnergy: Updated arsenal of one of the most dangerous threat actors*, ESET, 17-10-2018, https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ , consulted on 06-02-2019.
98 *Analysis of the Cyber Attack on the Ukrainian Power Grid*, sans.org, 18-03-2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, consulted on 06-02-2019.
99 *Cyber-Angriffe auf deutsche Energieversorger* [Cyber attack on German energy provider), bsi.bund.de, 13-06-2018, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html, consulted on 06-02-2019.
100 *GRIZZLY STEPPE - Russian Malicious Cyber Activity*, us-cert.gov, December 2016, https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity, consulted on 06-02-2019.
101 *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, us-cert.gov, 15-03-2018, https://www.us-cert.gov/ncas/alerts/TA18-074A, consulted on 06-02-2019.
102 *HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, citizenlab.ca, 18-09-2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, consulted on 04-03-2019.
103 *Inside the UAE's secret hacking team of American mercenaries*, Reuters.com, 30-01-2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/, consulted on 04-03-2019.
104 *Inside the UAE's secret hacking team of American mercenaries*, Reuters.com, 30-01-2019, https://www.reuters.com/investigates/special-report/usa-spying-raven/, consulted on 04-03-2019.
105 *UAE used cyber super-weapon to spy on iphones of foes*, Reuters.com, 30-01-2019, https://www.reuters.com/investigates/special-report/usa-spying-karma/, consulted on 04-03-2019.
106 *Jaarverslag AIVD 2017* [AIVD Annual Report 2017], aivd.nl, 06-03-2018, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2018/03/06/jaarverslag-aivd-2017/Jaarverslag+AIVD+2017.pdf, consulted on 04-02-2019.
107 *Joint report on publicly available hacking tools*, ncsc.gov.uk, 11-10-2018, https://www.ncsc.gov.uk/content/files/protected_files/article_files/Joint%20report%20on%20publicly%20available%20hacking%20tools%20%28NCSC%29.pdf, consulted on 04-02-2019.
108 *Gallmaker: New Attack Group Eschews Malware to Live off the Land*, Symantec.com, 10-10-2018, https://www.symantec.com/blogs/threat-intelligence/gallmaker-attack-group, consulted on 04-02-2019.
109 *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg.com, 04-10-2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, consulted on 07-03-2019.
110 *UK cyber security agency backs Apple, Amazon China hack denials*, Reuters.com, 05-10-2018, https://www.reuters.com/article/us-china-cyber-britain/uk-cyber-security-agency-backs-apple-amazon-china-hack-denials-idUSKCN1MF1DN, consulted on 07-03-2019.
111 *Statement from DHS Press Secretary on Recent Media Reports of Potential Supply Chain Compromise*, DHS.gov, 06-10-2018, https://www.dhs.gov/news/2018/10/06/statement-dhs-press-secretary-recent-media-reports-potential-supply-chain-compromise, consulted on 07-03-2019.
112 *Privégegevens van honderden Duitse politici, onder wie Merkel, op straat* [Personal data of hundreds of German policians – including Angela Merkel – leaked], DeMorgen.be, 04-01-2019, https://www.demorgen.be/buitenland/privegegevens-van-honderden-duitse-politici-onder-wie-merkel-op-straat-b1b2542b, consulted on 07-03-2019 .
113 *Hackerangriff auf Hunderte Politiker* [Hacker attack on hundreds of politicians], tagesschau.de, 04-01-2019, https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html, consulted on 07-03-2019.
114 *Festnahme eines Tatverdächtigen im Ermittlungsverfahren wegen des Verdachts des Ausspähens und der unberechtigten Veröffentlichung personenbezogener Daten* [Arrest of a suspect in preliminary investigation of spying and unauthorised publication of personal data], bka.de, 08-01-2019, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2019/Presse2019/190108_FestnahmeDatenausspaehung.html, consulted on 07-03-2019.
115 *Right country, wrong group? Researchers say it wasn't APT10 that hacked Norwegian software firm*, cyberscoop.com, 12-02-2019, https://www.cyberscoop.com/apt10-apt31-recorded-future-rapid7-china/, consulted on 04-02-2019.

116 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html, consulted on 04-02-2019.

117 *Olympic Destroyer is still alive*, securelist.com, 19-06-2018, https://securelist.com/olympic-destroyer-is-still-alive/86169/, consulted on 05-02-2019.

118 *Operation Sharpshooter*, mcafee.com 13-12-2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf, consulted on 05-02-2019.

119 *China link possible in cyber attack on Australian Parliament computer system*, abc.net.au, 08-02-2019, https://www.abc.net.au/news/2019-02-08/china-government-cyber-security-breach-parliament-hackers/10792938 consulted on 09-02-2019.

120 *With elections weeks away, someone "sophisticated" hacked Australia's politicians*, arstechnica.com, 18-02-2019, https://arstechnica.com/information-technology/2019/02/australian-political-parties-hacked-by-nation-state-attacker/ consulted on 06-02-2019.

121 https://www.wsj.com/articles/iran-blamed-for-cyberattack-on-australias-parliament-11550736796/

122 *Indictment of Iranian hackers by the Department of Justice of the United States of America*, US district court, 23-03-2018, https://www.justice.gov/usao-sdny/press-release/file/1045781/download, consulted on 26-02-2019

123 *Indictment of Iranian hackers by the Department of Justice of the United States of America*, https://www.justice.gov/opa/press-release/file/1114741/download, consulted on 26-02-2019.

124 *Indictment of North Korean hackers by the Department of Justice of the United States of America*, US district court, 08-06-2018, https://www.justice.gov/opa/press-release/file/1092091/download, consulted on 26-02-2019.

125 *Indictment of Russian hackers by the Department of Justice of the United States of America*, US district court, 03-07-2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election, consulted on 26-02-2019.

126 *Indictment of Russian hackers by the Department of Justice of the United States of America*, US district court, 03-10-2018, https://www.justice.gov/opa/page/file/1098481/download, consulted on 26-02-2019.

127 *Indictment of Chinese hackers by the Department of Justice of the United States of America*, US district court, 17-12-2018 https://www.justice.gov/opa/press-release/file/1121706/download, consulted on 27-02-2019.

128 *Canada identifies malicious cyber-activity by Russia*, Government of Canada, 04-10-2018, https://www.canada.ca/en/global-affairs/news/2018/10/canada-identifies-malicious-cyber-activity-by-russia.html, consulted on 26-02-2019.

129 Joint statement from Prime Minister May and Prime Minister Rutte, gov.uk, 04-10-2018, https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte, consulted on 27-02-2019.

130 *Indictment of Chinese hackers by the Department of Justice of the United States of America*, US district court, 17-12-2018 https://www.justice.gov/opa/press-release/file/1121706/download, consulted on 27-02-2019.

131 *UK and allies reveal global scale of Chinese cyber campaign*, UK government, gov.uk, 20-12-2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign, consulted on 27-02-2019.

132 *Cyber campaign attributed to China*, ncsc.govt.nz, 21-12-2018, https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/, consulted on 27-02-2019.

133 *Chinese cyber-enabled commercial intellectual property theft*, Ministry of Foreign Affairs of Australia, foreignminister.gov.au, 21-12-2018, https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx, consulted on 27-02-2019.

134 *Canada and Allies Identify China as Responsible for Cyber-Compromise*, cse.cst.gc.ca, 20-12-2018, https://cse-cst.gc.ca/en/media/media-2018-12-20 , consulted on 27-02-2019.

135 *Cyberattacks by a group based in China known as APT10*, Ministry of Foreign Affairs of Japan, 21-12-2018, https://www.mofa.go.jp/press/release/press4e_002281.html, consulted on 27-02-2019.

136 *Bolton confirms offensive cyber-operations conducted to protect midterms*, cyberscoop, 01-11-2018, https://www.cyberscoop.com/john-bolton-offensive-cyber-operations/, consulted on 28-02-2019.

137 *The pentagon has prepared a cyber attack against Russia*, publicintegrity.org, 02-11-2018, https://publicintegrity.org/national-security/military/the-pentagon-has-prepared-a-cyber-attack-against-russia/, consulted on 28-02-2019.

138 Ministerie van Justitie, *Voorzorgsmaatregel ten aanzien van gebruik Kaspersky antivirussoftware* [Precautionary measure in relation to Kaspersky antivirus software], 14-05-2018, https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregel-ten-aanzien-van-gebruik-kaspersky-antivirussoftware, consulted on 28-02-2019.

139 *Software and hardware of Huawei and ZTE is a security threat*, National Cyber Security Centre Czechia, govcert.cz, 17-12-2018, https://www.govcert.cz/en/info/events/2682-software-and-hardware-of-huawei-and-zte-is-a-security-threat/, consulted on 28-02-2019.

140 *H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019*, congress.gov, 13-08-2018, https://www.congress.gov/bill/115th-congress/house-bill/5515/text, consulted on 29-02-2019.
141 *Government Provides 5G Security Guidance To Australian Carriers*, minister.communications.gov.au, 23-08-2018, https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers, consulted on 29-02-2019.
142 *German officials sound China alarm as 5G auctions loom*, reuters.com, 13-11-2018, https://www.reuters.com/article/us-germany-china-5g-exclusive/exclusive-german-officials-raise-china-alarm-as-5g-auctions-loom-idUSKCN1NI1WC.
143 *Pence praises Poland's actions on Huawei as U.S. pressure mounts*, reuters.com, 13-02-2019, https://www.reuters.com/article/us-huawei-europe-poland/pence-praises-polands-actions-on-huawei-as-us-pressure-mounts-idUSKCN1Q22IX.
144 ENISA, *ENISA Threat Landscape Report 2018* (2019). https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 .
145 *Jaarverantwoording politie 2018* [Police Annual Report 2018], May 2019.
146 *Kamerbrief over phishing incident DigiD's via Mijnoverheid* [Letter to the Dutch Lower House of Parliament on the DigiD phishing incident via government portal MijnOverheid], 29-06-2018, phishing-incident-digids-via-mijnoverheid-22-juni-2018.pdf, consulted on 26-02-2019.
147 *FBI ziet toename van sim-swapping bij cryptodiefstal* [FBI observes increase in SIM swapping for cryptotheft], 07-03-2019, security.nl, https://www.security.nl/posting/600453/FBI+ziet+toename+van+sim-swapping+bij+cryptodiefstal, consulted on 08-03-2019.
148 *Aanvallen via ss7-protocol om 2fa-sms'jes te onderscheppen nemen toe* [Increase in SS7 protocol attacks to intercept 2FA text messages], tweakers.net, 01-02-2019, https://tweakers.net/nieuws/148636/aanvallen-via-ss7-protocol-om-2fa-smsjes-te-onderscheppen-nemen-toe.html, consulted on 08-03-2019.
149 *Internet Organised Crime Threat Assessment (IOCTA)*, Europol.europa.eu, 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment, consulted on 22-03-2019.
150 *Politie sluit grootste DDoS-website in Operation Power Off* [Police close largest DDoS website as part fo Operation Power Off], politie.nl, 25-04-2018, https://www.politie.nl/nieuws/2018/april/25/politie-sluit-grootste-ddos-website-in-operation-power-off.html consulted on 22-03-2019.
151 *World's biggest marketplace selling internet paralysing DDoS attacks taken down*, Europol.europa.eu, 25-04-2018, https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-biggest-marketplace-selling-internet-paralysing-ddos-attacks-taken-down, consulted on 22-03-2019.
152 *Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets*, Wegberg et al (USENIX, 2018).
153 M. McGuire, *Into the Web of Profit. An in-depth study of cybercrime, criminals and money*, April 2018.
154 *Jaarverantwoording politie 2018* [Police Annual Report 2018], May 2019.
155 *Duizenden jongeren 'verleid' tot hacken in campagne politie* [Thousands of youngsters 'enticed' to hack via police campaign, nos.nl, 14-02-2019, https://nos.nl/artikel/2271890-duizenden-jongeren-verleid-tot-hacken-in-campagne-politie.html, consulted on 21-02-2019.
156 *Hack_Right*, politie.nl, https://www.politie.nl/themas/hack_right.html?sid=fd8d5ado-1a02-4bb9-bof4-b34d9c787899, consulted on 26-02-2019 .
157 *Microsoft Security Intelligence Report 24*, https://www.microsoft.com/en-us/security/operations/security-intelligence-report, consulted on 26-03-2019.
158 Symantec Internet Security Threat Report 2019, https://www.symantec.com/security-center/threat-report, consulted on 04-03-2019.
159 Trend Micro 2018 Mobile Threat Landscape, https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape, consulted on 04-03-2019.
160 CrowdStrike Global Threat Report 2019, https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/, consulted on 26-03-2019.
161 *Inside Magecart: RiskIQ and Flashpoint Release Comprehensive Report on Cybercrime and the Assault on E-Commerce*, riskiq.com, 13-11-2018, https://www.riskiq.com/blog/external-threat-management/inside-magecart/, consulted on 07-03-2019.
162 *Symantec: duizenden webwinkels getroffen door formjacking* [Symantec: 'thousands of webshops hit by formjacking'], security.nl, 21-02-2019, https://www.security.nl/posting/598734/Symantec%3A+duizenden+webwinkels+getroffen+door+formjacking consulted on 07-03-2019.
163 *Symantec Internet Security Threat Report*, February 2019, https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf, consulted on 07-03-2019.
164 *Spam and Phishing in Q3 2018*, securelist.com, 06-11-2018, https://securelist.com/spam-and-phishing-in-q3-2018/88686/, consulted on 26-03-2019.

165 *Microsoft security intelligence report volume 24, January – December 2018*, February 2019, https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/, consulted on 26-03-2019.

166 *Phishing Attack Pretends to be a Office 365 Non-Delivery Email*, bleepingcomputer.com, 16-12-2018, https://www.bleepingcomputer.com/news/security/phishing-attack-pretends-to-be-a-office-365-non-delivery-email/, consulted on 26-03-2019.

167 *Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign*, fireeye.com, 19-11-2018, https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html, consulted on 26-03-2019.

168 *Indictment of Chinese hackers by the Department of Justice of the United States of America*, US district court, 17-12-2018, https://www.justice.gov/opa/press-release/file/1121706/download, consulted on 27-02-2019.

169 *Top phishing email attacks worldwide in 2018*, duocircle.com, November 2018, https://www.duocircle.com/phishing-protection/top-phishing-email-attacks-worldwide-in-2018, consulted on 26-03-2019.

170 *Global Threat Report 2019*, March 2019, https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/, consulted on 26-03-2019.

171 *3,81 miljoen euro schade door phishing bij internetbankieren in 2018 - Minder fraude met betaalpassen en automatische incasso's* [3.81 million euros in damage due to phishing attacks on internet banking services in 2018 - Less fraud involving bank cards and direct debit payments], 27-03-2019, https://www.nvb.nl/nieuws/3-81-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018-minder-fraude-met-betaalpassen-en-automatische-incasso-s/, consulted on 27-03-2019.

172 *Aanvallers wijzigen wereldwijd dns-instellingen domeinen* [Attackers change domain DNS settings around the world], security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen, consulted on 07-03-2019.

173 *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale*, FireEye.com, 09-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html, consulted on 07-03-2019.

174 *DNS Infrastructure Hijacking Campaign*, us-cert.gov, 11-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign, consulted on 07-03-2019.

175 *DNSpionage Campaign Targets Middle East*, talosintelligence.com, 27-11-2018, https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html, consulted on 07-03-2019.

176 *A Worldwide Hacking Spree Uses DNS Trickery to Nab Data*, wired.com, 11-01-2019, https://www.wired.com/story/iran-dns-hijacking/, consulted on 07-03-2019.

177 *ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet*, icann.org, 22-02-2019, https://www.icann.org/news/announcement-2019-02-22-en, consulted on 08-03-2019.

177 *Wet op de inlichtingen- en veiligheidsdiensten* [Intelligence and Security Services Act 2017], aivd.nl, https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten, consulted on 15-02-2019.

178 *BGP Hijack of Amazon DNS to Steal Crypto Currency*, dyn.com, 25-4-2018, https://dyn.com/blog/bgp-hijack-of-amazon-dns-to-steal-crypto-currency/, consulted on 26-03-2019.

179 *BGP/DNS Hijacks Target Payment Systems*, dyn.com, 03-08-2018, https://dyn.com/blog/bgp-dns-hijacks-target-payment-systems/, consulted on 26-03-2019.

180 *Fox-IT: Nederlandse bedrijven ook slachtoffer van SamSam-gijzelsoftware* [Dutch businesses also fall victim to SamSam ransom software], 02-12-2018, https://nos.nl/artikel/2261704-fox-it-nederlandse-bedrijven-ook-slachtoffer-van-samsam-gijzelsoftware.html, consulted on 22-03-2019.

181 *Microsoft Security Intelligence Report Volume 24*, microsoft.com, 28-02-2019, https://www.microsoft.com/security/blog/2019/02/28/microsoft-security-intelligence-report-volume-24-is-now-available/, consulted on 20-03-2019.

182 *For the exact criteria, see: Wbni voor digitale dienstverleners* [Network and Information Systems Security Act for digital service providers], https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners, consulted on 15-02-2019.

183 Source: NCSC, consulted on 26-02-2019.

184 *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor digitale dienstverleners* [Network and Information Systems Security Act (Wbni) for digital service providers], rijksoverheid.nl, 01-09-2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners, consulted on 15-02-2019.

185 *Nieuwe wet versterkt bestrijding computercriminaliteit* [New law boosts countermeasures against computer crime], rijksoverheid.nl, 28-02-2019, https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit, consulted on 05-03-2019.

186 *Cijfers datalekken 2018* [Data leak statistics 2018], autoriteitpersoonsgegevens.nl, 01-02-2019, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/cijfers-datalekken-2018, consulted on 26-02-2019.

187 *In 10 stappen voorbereid op de AVG* [Prepare for the GDPR in 10 easy steps], autoriteitpersoonsgegevens.nl, November 2017, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf, consulted on 15-02-2019.

188 *In 10 stappen voorbereid op de AVG* [Prepare for the GDPR in 10 easy steps], autoriteitpersoonsgegevens.nl, November 2017, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf, consulted on 15-02-2019.

189 *Wet op de inlichtingen- en veiligheidsdiensten 2017* [Intelligence and Security Services Act 2017], wetten.overheid.nl, https://wetten.overheid.nl/BWBR0039896/2018-05-01, consulted on 08-03-2019.

190 NCTV, *Cybersecuritybeeld Nederland 2018* [Cyber Security Assessment Netherlands 2018], June 2018, https://www.nctv.nl/binaries/CSBN2018_web_tcm31-332841.pdf, consulted on 07-02-2019.

191 *Oorzaak computerstoring treinverkeersleiding gevonden* [Cause of rail traffic control system failure identified], prorail.nl, 22-08-2018, https://www.prorail.nl/nieuws/oorzaak-computerstoring-treinverkeersleiding-gevonden, consulted on 07-03-2019.

192 *Brief van de minister van rechtsbescherming aan de Tweede Kamer (29279-455) m.b.t. Storing mobiele netwerk elektronische enkelband* [Letter to the Dutch Lower House of Parliament from the Minister for Legal Protection (29279-455) concerning the failure of the mobile network for electronic ankle bracelets], tk-storing-mobiele-netwerk-elektronische-enkelband.pdf, consulted on 07-03-2019.

193 *Meldelicht datalekken: facts & figures overzicht feiten en cijfers 1e helft 2018* [Data leak notification obligation: overview of facts and figures for the first half of 2018], autoriteitpersoonsgegevens.nl, 2018, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_halfjaarrapportage_q1_en_q2_2018_algemeen.pdf, consulted on 05-03-2019.

194 *Disparities found in levels of reporting across EU member states*, DLA Piper, dlapiper.com, 06-02-2019, https://www.dlapiper.com/en/netherlands/news/2019/02/dla-piper-gdpr-data-breach-survey/, consulted on 19-03-2019.

195 *Verkeerde Burgernetmail verzonden naar 145 BN-deelnemers* [Wrong Burgernet e-mail sent to 145 Burgernet participants], politie.nl, 10-07-2018, https://www.politie.nl/nieuws/2018/juli/10/04-verkeerde-burgernetmail-verzonden-naar-145-bn-deelnemers.html, consulted on 05-03-2019.

196 *DDoS-aanvallen treffen 15% meer websites in 2018* [DDoS attacks affect 15% more websites in 2018], SIDN, sidn.nl, 08-01-2019, https://www.sidn.nl/a/veilig-internet/ddos-aanvallen-treffen-15-meer-websites-in-2018, consulted on 12-03-2019.

197 *December piekmaand voor DDoS-aanvallen op webwinkels* [December peak month for DDoS attacks on webshops], NBIP, nbip.nl, 14-12-2018,https://www.nbip.nl/2019/01/14/december-piekmaand-ddos-webwinkels/, consulted on 12-03-2019.

198 *Rabobank en ABN AMRO zondag weer getroffen door DDoS-aanval* [Rabobank and ABN AMRO once again hit by DDoS attack on Sunday], 28-05-2018, https://www.nu.nl/internet/5286176/rabobank-en-abn-amro-zondag-weer-getroffen-ddos-aanval.html, consulted on 20-03-2019.

199 *Website DigiD was weer onbereikbaar door DDoS-aanval* [DigiD website once again inaccessible due to DDoS attack], 31-07-2018, https://www.nu.nl/internet/5391845/website-digid-was-weer-onbereikbaar-ddos-aanval.html, consulted on 20-03-2019.

200 *FBI en Nederlandse politie halen vijftien aanbieders DDoS-aanvallen offline* [FBi and Dutch police take 15 providers of DDoS attack services offline], 20-12-2018, https://www.nu.nl/internet/5643251/fbi-en-nederlandse-politie-halen-vijftien-aanbieders-ddos-aanvallen-offline.html, consulted on 20-03-2019.

201 Ministry of Economic Affairs and Climate Policy, *Nederlandse digitaliseringsstrategie* [Dutch Digitisation Strategy], June 2018.

202 https://nos.nl/artikel/2232061-rekenkamer-rijk-heeft-databeveiliging-niet-op-orde.html, consulted on 13-03-2019.

203 https://www.rekenkamer.nl/actueel/nieuws/2018/05/16/ministers-melden-te-weinig-wat-resultaten-zijn, consulted on 13-03-2019.

204 https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/documenten/rapporten/2018/05/16/staat-van-de-rijksverantwoording-2017, consulted on 13-03-2019.

205 https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde, consulted on 15-05-2019.

206 Netherlands Court of Audit, *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* [Digital dike strengthening: cyber security and critical water infrastructure], 28-03-2019.

207 Netherlands Court of Audit, *Digitale dijkverzwaring: cybersecurity en vitale waterwerken* [Digital dike strengthening: cyber security and critical water infrastructure], 28-03-2019.

208 https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-maart/index.jsp, consulted on 28-03-2019.

209 https://executive-people.nl/618901/ruim-op-de-nederlandse-organisaties-slachtoffer-van-phishing.html.

210 https://www.microsoft.com/securityinsights, consulted on 25-03-2019.

211 https://content.fireeye.com/m-trends/rpt-m-trends-2019, consulted on 13-03-2019.

212 CrowdStrike Global Threat Report 2019, https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/, consulted on 26-03-2019.
213 https://www.cpb.nl/publicatie/risicorapportage-cyberveiligheid-economie-2018.
214 https://www.ncsc.nl/actueel/nieuwsberichten/onderzoeksrapport-digitale-hygiene-nederland.html, consulted on 20-03-2019.
215 Radiocommunications Agency Netherlands, *De Staat van de Ether 2017* [The State of the Ether 2017], https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/onveilige-apparatuur-risico-voor-samenleving, consulted on 25-03-2019.
216 *Onderzoekers tonen Rowhammer-aanval om browser over te nemen op Android-toestel* [Researchers demonstrate Rowhammer attack to hack into browser on Android device], https://tweakers.net/nieuws/138207/onderzoekers-tonen-rowhammer-aanval-om-browser-over-te-nemen-op-android-toestel.html, consulted on 26-03-2019
217 *VUSec-onderzoekers weten ecc-geheugen aan te vallen met Rowhammer* [VUSec researchers successfully attack ECC memory with Rowhammer], https://tweakers.net/nieuws/146103/vusec-onderzoekers-weten-ecc-geheugen-aan-te-vallen-met-rowhammer.html, consulted on 26-03-2019
218 *Google researchers: Spectre blijft ons nog lang achtervolgen* [Spectre will haunt us long into the future], https://www.security.nl/posting/599154/Google-onderzoekers%3A+Spectre+blijft+ons+nog+lang+achtervolgen, consulted on 26-03-2019.
219 CA Insider Threat Report 2018. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf, consulted on 26-03-2019.
CompTIA 2018 Trends in Cybersecurity, https://www.comptia.org/resources/cybersecurity-trends-research, consulted on 26-03-2018, ,
World Economic Forum Global Risk Report 2018, http://reports.weforum.org/global-risks-2018/, consulted on 26-03-2019.
220 M. McGuire, *Into the Web of Profit. An in-depth study of cybercrime, criminals and money*, April 2018.
221 Netherlands Authority for Consumers and Markets, *5G en de Autoriteit Consument en Markt* [5G and the Netherlands Authority for Consumers and Markets], 12-12-2018.
222 European Centre for International Political Economy, *5G and National Security After Australia's Telecom Sector Security Review, Occasional paper No. 8/2018* (2018), p.4-5.
223 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 23.
224 Ryan Goosen, Anna Rontojannis, Stefan Deutscher (et al), *Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution*, 13-11-2018, https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx, consulted on 11-02-2019.
National Network for Safety and Security Analysts, Horizonscan Nationale Veiligheid 2018 [National Security Horizon Scan], October 2018, p. 23.
Celeste Fralick McAfee, *Artificial Intelligence in Cybersecurity Is Vulnerable*, 15-01-2019, https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/, consulted on 11-02-2019.
Artificial Intelligence and Cybersecurity: Attacking and Defending, Tripwire, 10-12-2018, https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/, consulted on 11-02-2019.
Tara Seals, *Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad*., 03-10-2018, https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/, consulted on 11-02-2019.
Scot Finnie, *AI in cybersecurity: what works and what doesn't*, 15-08-2018, https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html, consulted on 11-02-2019.
225 Craig S. Smith, Alexa and Siri Can Hear *This Hidden Command. You Can't.*, New York Times, 10-05-2018, https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html, consulted on 11-02-1029.
226 *BlackRock shelves unexplainable AI liquidity models*, Risk.net, 12-11-2018, https://www.risk.net/asset-management/6119616/blackrock-shelves-unexplainable-ai-liquidity-models.
227 Kees Verhoeven, *Investeer 25 miljoen in kunstmatige intelligentie* [Invest €25 million into artificial intelligence], D66, 20-09-2018, https://d66.nl/investeer-in-kunstmatige-intelligentie/.
228 Ryan Goosen, Anna Rontojannis, Stefan Deutscher (et al), *Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution*, 13-11-2018, https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx, consulted on 11-02-2019.
Celeste Fralick McAfee, *Artificial Intelligence in Cybersecurity Is Vulnerable*, 15-01-2019, https://www.scmagazine.com/home/opinion/artifical-intelligence-in-cybersecurity-is-vulnerable/, consulted on 11-02-2019.
Artificial Intelligence and Cybersecurity: Attacking and Defending, Tripwire, 10-12-2018, https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/, consulted on 11-02-2019.
Tara Seals, *Artificial Intelligence: A Cybersecurity Tool for Good, and Sometimes Bad*., 03-10-2018, https://threatpost.com/artificial-intelligence-a-cybersecurity-tool-for-good-and-sometimes-bad/137831/, consulted on 11-02-2019.
Scot Finnie, *AI in cybersecurity: what works and what doesn't*, 15-08-2018, https://www.csoonline.com/article/3295596/security/ai-in-cybersecurity-what-works-and-what-doesnt.html, consulted on 11-02-2019.

229 National Network for Safety and Security Analysts, *Horizonscan Nationale Veiligheid 2018* [National Security Horizon Scan], October 2018, p. 13-18.
230 Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force* (November 2018), p. 10-12, 66.
231 *2019 Forcepoint Cybersecurity Predictions Report*, Forcepoint, 13-11-2018, https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf, consulted on 29-11-2018.
232 Centre for European Policy Studies (CEPS), *Strengthening the EU's Cyber Defence Capabilities. Report of a CEPS Task Force* (November 2018), p. 10-12, 66; Digitale oorlog minstens zo destructief [Digital war at least equally as destructive], Leidsch Dagblad, 13-02-2019.
233 *Digitale oorlog minstens zo destructief* [Digital war at least equally as destructive], Leidsch Dagblad, 13-02-2019.
234 Ministry of Economic Affairs and Climate Policy, *Nederlandse digitaliseringsstrategie* [Dutch Digitisation Strategy], June 2018, p. 13-14.
235 *De technologische Koude Oorlog* [The Technological Cold War], De Groene Amsterdammer, 23-01-2019.
236 *Europa overtuigen om geen Huawei te kopen 'topprioriteit' voor VS* [Convincing Europe not to do business with Huawei a 'top priority' to the US], Nu.nl, 05-02-2019, consulted on 06-02-2019; Minister VS waarschuwt voor Huawei bij begin Europese toer [US minister issues warning against Huawei at the start of European tour], NOS.nl, 11-02-2019, https://nos.nl/artikel/2271562-minister-vs-waarschuwt-voor-huawei-bij-begin-europese-toer.html, consulted on 12-02-2019.
237 *Revitalizing privacy and trust in a data-driven world. Key findings from The Global State of Information Security®* Survey 2018., PWC, 28-03-2018, https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf, consulted on 15-02-2019.
238 *Cybersecurity predictions for 2019*, CSO Online, 20-11-2018, https://www.csoonline.com/article/3322221/security/9-cyber-security-predictions-for-2019.html; Prospects for cybersecurity in 2019, Oxford Analytica, 23-11-2018.
239 Ministry of Economic Affairs and Climate Policy, *Nederlandse digitaliseringsstrategie* [Dutch Digitisation Strategy], June 2018.
240 *Roadmap Digitaal Veilige Hard- en Software* [Digitally Secure Hardware and Software Roadmap], Ministry of Economic Affairs and Climate Policy and Ministry of Justice and Security, April 2018, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software/Roadmap+Digitaal+Veilige+Hard-+en+Software.pdf.
241 *Het DigiNotarincident. Waarom digitale veiligheid de bestuurstafel te weinig bereikt* [The DigiNotar incident: Why cyber security isn't discussed enough in the boardroom], Dutch Safety Board, June 2012, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwjR4t2-5L3gAhUQU1AKHVkgB-QFjACegQICBAC&url=https%3A%2F%2Fwww.onderzoeksraad.nl%2Fnl%2Fmedia%2Fattachment%2F2018%2F7%2F10%2Frapport_diginotar_nl_web_def_20062012.pdf&usg=AOvVaw3M1PhT7xZArFoOgZmyboNB.
242 *KPN erkent fouten bij hack, gaat versneld investeren in IT-systemen* [KPN recognises errors leading to hack, will accelerate investment in IT systems], Het Financiële Dagblad, 14-02-2012; KPN: hack gevolg van achterstallig onderhoud [KPN: 'Hack caused by poor maintenance'], De Volkskrant, 14-02-2012.
243 John Snow, *Top 5 most notorious cyberattacks*, Kaspersky Lab, 06-11-2018, https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/, consulted on 18-02-2019.
244 *The WannaCry attack is a wake-up call*, Financial Times, 14-05-2017, https://www.ft.com/content/f6cd3e38-388a-11e7-821a-6027b8a20f23, consulted on 18-02-219; *Wake-up call voor bedrijven in strijd tegen cybercrime* [Wake-up call for businesses in the fight against cyber crime], Computable.nl, 07-08-2017, https://www.bnr.nl/nieuws/tech/10327239/wake-up-call-voor-bedrijven-in-strijd-tegen-cybercrime, consulted on 18-02-2109; *Maersk moest 45.000 pc's herinstalleren wegen NotPetya* [Maersk forced to reinstall 45,000 PCs due to NotPetya], Security.nl, 25-01-2018; *Brancheorganisatie voor ict-beveiligers ziet het licht* [Sector organisation for ICT security firms founded], Computable.nl, 14-03-2018.
245 The Dutch Data Processing and Cybersecurity Notification Obligation Act (*Wet gegevensverwerking en meldplicht cybersecurity*, applicable until 15 November 2018) and the Network and Information Systems Security Act (*Wet beveiliging netwerken en informatiesystemen*, applicable from 15 November 2018 onwards).
246 See https://www.ncsc.nl/actueel/leidraad-coordinated-vulnerability-disclosure.html, consulted on 08-03-2019.

Publication
National Coordinator for Security and Counterterrorism (NCTV)
PO Box 20301, 2500 EH The Hague
Turfmarkt 147, 2511 DP The Hague,
The Netherlands
+31 (0)70 751 5050

More information
www.nctv.nl
csbn@nctv.minjenv.nl
@nctv_nl

June 2019