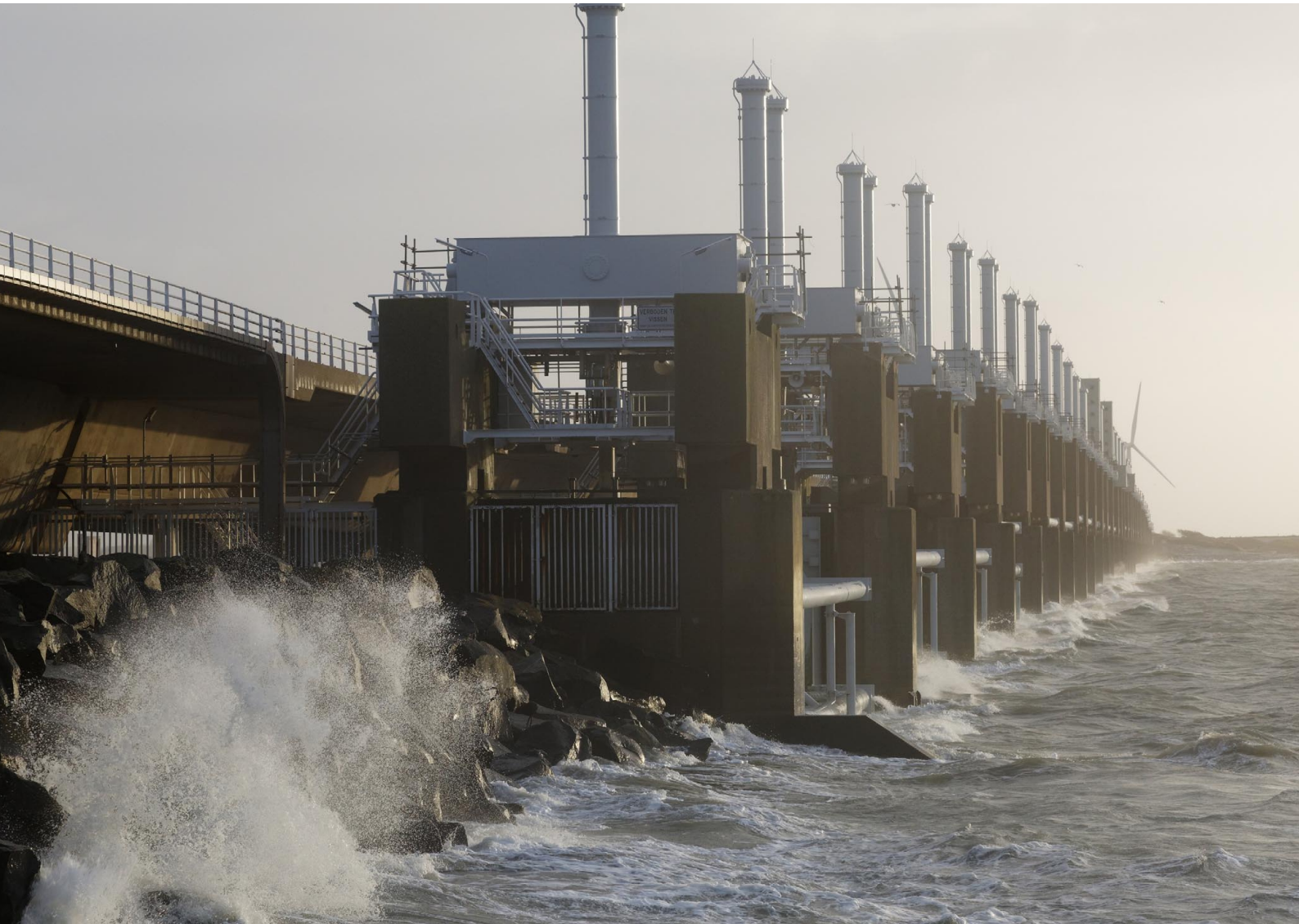
National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Cyber Security Assessment Netherlands

CSAN 2020



Cyber Security Assessment Netherlands

CSAN 2020

Publication details

The Cyber Security Assessment Netherlands (CSAN) 2020 provides an overview of the cyber threats facing this country and the interests that could be harmed. It also discusses cyber risks and cyber resilience, with an accent on national security. The CSAN is drawn up every year by the National Coordinator for Security and Counterterrorism (NCTV).

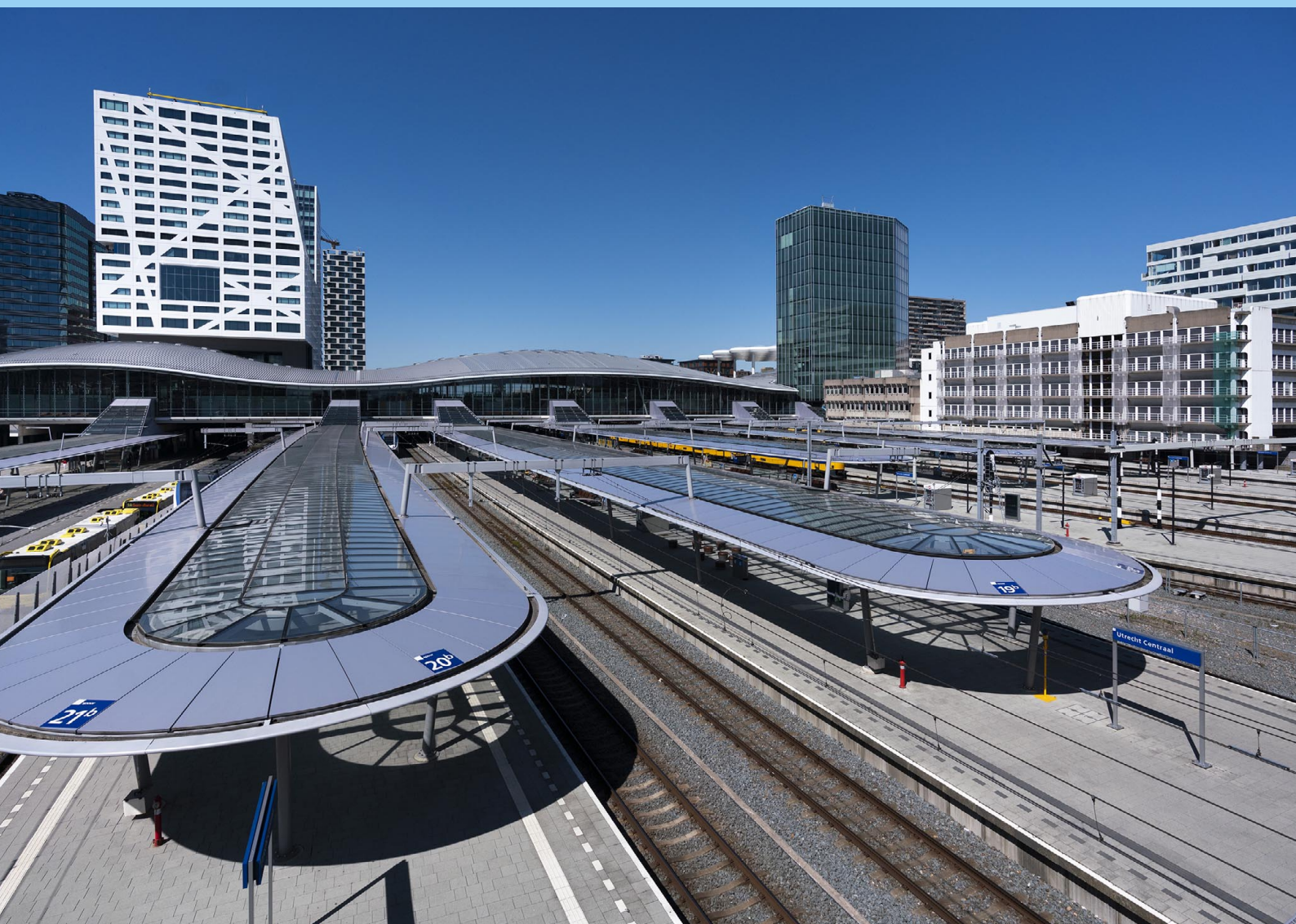
The NCTV protects the Netherlands from threats that could disrupt Dutch society. Together with its partners in the government, research community and business sector, the NCTV works to ensure that the Netherlands' vital infrastructure is and remains secure. The NCTV is the central-government body responsible for counterterrorism, cybersecurity, national security, crisis management and state threats. Together with its partners in the security sector, the NCTV works to keep the Netherlands a safe and stable country. Its focus is on preventing and minimising social disruption.

The National Cyber Security Centre (NCSC) is the central information hub and centre of expertise for cybersecurity in the Netherlands. The NCSC helps to boost society's cyber resilience, specifically within central government and 'critical providers'.

The CSAN is drafted jointly by the NCTV and the NCSC, which are grateful for the information, insights and expertise provided by government agencies, organisations associated with critical processes, researchers and other parties.

Table of Contents

Cyber risks intertwined with other risks



Cyber incidents can paralyse a society

Like coronavirus, cyber incidents can strike at the very heart of our society and paralyse it, perhaps for an extended period of time. The Netherlands is highly dependent on digital services, processes and systems, which are growing ever more closely intertwined with physical processes, activities and devices. Collectively, all these things are part of a greater whole: the global digital domain. While the digital domain offers many opportunities, it also heightens our vulnerability to human error, technical failures and the actions of malicious parties. All over the world, a variety of actors exploit the digital domain to carry out cyber attacks. It is also a potential battleground for interstate conflicts. Not all countries and organisations have ensured that their cyber resilience is up to par, and their failure to take the necessary action can have an impact on others. Countries and organisations that do take their resilience seriously can still encounter problems as a result of cyber incidents that affect other parties. Boosting cyber resilience is the most important tool for managing risks in the digital domain. It is definitely not just an issue for technical experts. It is also – or perhaps even primarily – an issue of governance and risk management for public administrators and leaders of organisations.

Cyber risks have not diminished

A 'cyber risk' is defined as the chance that a cyber incident could occur and the impact it would have on various interests, in light of the current level of cyber resilience. The cyber risks facing the Netherlands have not diminished during the period under review and remain fundamentally the same. From a national-security perspective, the main risks involve sabotage and espionage on the part of state actors, and preparations to that end. The concept of a cyber risk also encompasses the large-scale breakdown of services, processes or systems. In addition, there is the risk of cyber attacks carried out by criminal actors seeking economic gain. Extortion with the help of ransomware is a proven method in this connection. It is possible that criminals increasingly have the intention and capacity to target control systems used by critical processes. Ransomware, data theft and digital manipulation by criminals mainly affect the organisation targeted. Yet other services, processes, systems and organisations that are dependent on or in some way connected to that target can also be impacted, possibly in ways that affect society as a whole.

Cyber threat is here to stay

The term 'cyber threat' refers to the possibility of a cyber incident or a series of simultaneous or successive cyber incidents. An 'incident' can be either a cyber attack or a breakdown caused by human error or a technical issue.

As in 2019, it can be concluded that the cyber threat is permanent in nature and that cyber incidents can cause harm that leads to social disruption. Although the Netherlands has not yet experienced social disruption as a result of a cyber incident, the possibility cannot be ruled out. The criminal cyber attacks on the municipality of Lochem and Maastricht University show how serious the repercussions of such incidents can be for organisations, their staff and the general public. The failure of systems has also had social consequences. For example, a

malfunction at KPN caused the emergency number 112 to go down, with the result that the police and ambulance services could not be reached for a time.

Digital security is a prerequisite for a functioning society

Digital security means that digital services, processes and the underlying systems can function smoothly and without interruption. Digital security is inextricably linked to national security. This is especially true in the case of critical processes and the (global) digital domain[1], which is *the* digital foundation of our society. At the same time, this domain can be exploited to carry out cyber attacks, and it is a potential battleground for interstate conflicts. As their name suggests, critical processes are essential to society; they are also a potential target for certain actors (primarily state actors) during or in preparation for conflicts. The digital domain and critical processes are closely intertwined: certain critical processes, for example, help to shape the digital domain, including 'internet and data services'. Others, such as 'national transport and distribution of electricity', provide the prerequisites that make it possible. Conversely, critical processes are themselves almost entirely digitalised, and thus dependent on the digital domain. Another key issue is the digital security of other socially important organisations, services and processes. These include, for example, not only globally prominent knowledge-intensive companies but also ostensibly less important organisations or processes: cyber risks do not stand in isolation, and vulnerabilities that affect one party could well have an impact on other parties.

Cyber resilience not yet up to par everywhere

Cyber resilience is a complex concept. In essence, it refers to the ability to adequately manage cyber risks. To be resilient, organisations must be capable of preventing cyber incidents or minimising their impact on a daily basis. Parties must work together to boost digital resilience. Public administrators must feel a sense of responsibility when it comes to managing cyber risks.

However, cyber resilience of this kind is not yet evident everywhere and, as a result, certain parties can be particularly vulnerable to cyber incidents. This is especially true when insufficient basic measures have been taken to erect barriers to cyber attacks and to limit damage and facilitate recovery when incidents do occur. At the same time, resilience to cyber incidents remains a thorny issue. Digital services and processes are interconnected. Systems consist of a variety of components (both hardware and software), and they are connected to an array of other systems. There are unsafe products and services on the market. In cyberspace, users – inadvertently – conduct themselves in an unsafe manner. All this introduces potential vulnerabilities that not only open the door to cyber attacks, but can also lead to system failures.

There is not yet a complete and clear sense of the degree of cyber resilience of critical processes and associated systems. Supervisory authorities for providers of critical processes describe a varied picture. Some parties have things sufficiently under control; others do not. At some ministries and central government bodies, information security is still not as it should be.

Cyber risks are intertwined with other risks

The cyber risks facing a country, economic sector or individual party are intertwined with each other and with other types of risks. Digital services, processes and systems are part of a larger whole; the global digital domain. The 2008 financial crisis and the 2020 COVID-19 pandemic show that certain events can rapidly have a global impact on other domains and strike at the heart of society and the economy. This is also true for cyber incidents. This is especially true when incidents occur on a large scale at the same time as, in conjunction with, or in succession to other incidents. A combination of a large-scale cyber incident and the COVID-19 pandemic would have major consequences, for example. Thanks to digitalisation, commercial, educational and social activities that would otherwise have been halted by the pandemic can continue, at least in part. The flip side of this is the unprecedented burden that this situation is placing on the digital domain. A large-scale digital breakdown could cause more societal harm than it otherwise might without the added factor of the pandemic. Geopolitical developments, such as trade embargoes, also affect cyber risks.

If a given country or organisation is not sufficiently resilient, there could be repercussions for other countries and organisations. Even when countries and organisations are resilient, they can still run into problems as a result of cyber incidents primarily affecting other parties. The vulnerabilities in Citrix ADC and Gateway servers published in late 2019 are a good illustration of this phenomenon. These vulnerabilities created a global risk that such flaws could be exploited by attackers. In the Netherlands, hundreds of organisations (possibly in excess of 3,700), including providers of critical processes, are thought to have been affected. A major power cut or a malfunction at a national telecom provider could quickly bring digital processes to a standstill. In addition, it is not always easy for manufacturers, employees and consumers to safely conduct certain activities in cyberspace, as there are many dangers lurking, including malicious websites.

1 The digital domain is the complex environment that has arisen from the interaction between people, software and services on the internet, supported by physical information and communication technology (ICT) in the form of devices and connected networks. A synonym for the term 'digital domain' is 'cyberspace'.

Boosting resilience: the most important tool for managing cyber risks

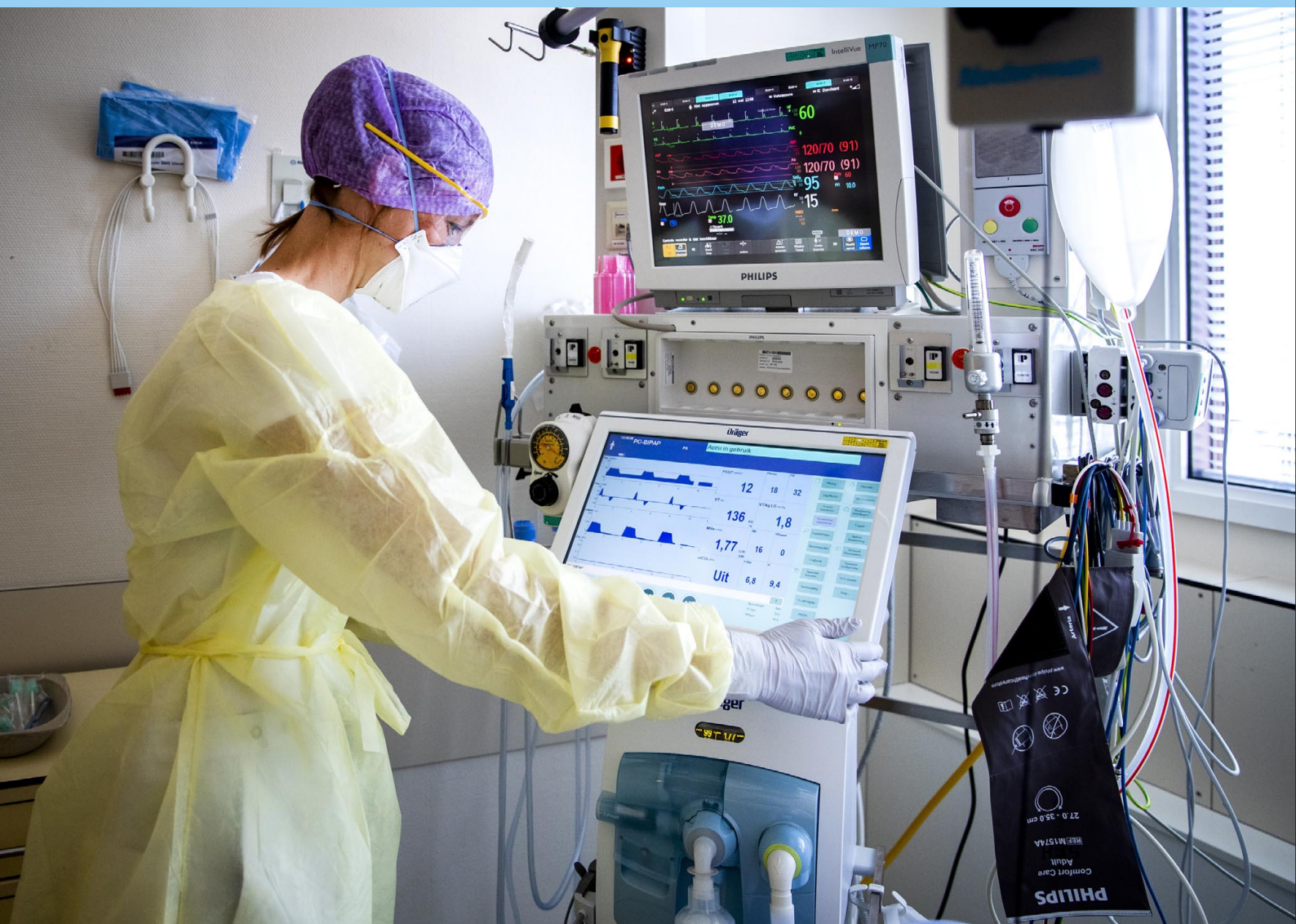
Boosting cyber resilience remains the most important tool for adequately managing cyber risks. This can reduce both the chance that a cyber incident could occur and its potential impact if it does. Cyber resilience can be increased with the help of technical, procedural or organisational measures. Other ways of heightening resilience are through legislation, grant policy, training and education (to equip people with online safety skills), information campaigns, partnerships, and the establishment of standards for the digitalisation of services and processes and for system design.

There are a number of reasons why cybersecurity does not come about automatically. In global terms, many parties play a role in making and keeping the digital domain safe. Cyber risks, especially for the digital domain as a whole, are sometimes underestimated. Often, individuals do not feel 'incentivised' to contribute to the security of the whole. This can give rise to vulnerabilities. Obviously, the Dutch government and other Dutch parties have limited scope for influencing global digital security. Plus, it is difficult to fully grasp the risks to the entire digital domain and their impact on society. This makes it difficult to assess the risks and to determine whether or not to take measures to manage them. In addition, it is not clear in advance which parties have the incentives, capabilities and willingness to limit risks.

Boosting cyber resilience is definitely not only the job of technical experts. It is also – or perhaps even primarily – an issue of governance and risk management for heads of organisations, countries and groups of countries.

Back to Table of Contents

Threats, interests and resilience determine the risk



1 Introduction

Purpose and main questions

The Cyber Security Assessment Netherlands (CSAN) 2020 provides an overview of the cyber threats facing this country and the interests that could be harmed. It also discusses cyber risks and resilience, with an accent on national security.

The main questions that CSAN 2020 seeks to answer are:

- In the period between 1 January 2019 and February 2020, what noteworthy developments were there in terms of: a) cyber incidents, b) cyber resilience and c) interests that were (or could be) affected by such incidents?
- What broader developments are expected to affect cybersecurity in the years ahead?
- What cyber threats can harm national security? Who or what is the source of these threats? And who or what do they target?
- What interests can be affected by cyber incidents? What impact can such incidents have? And to what extent do the parties in question take account of this when assessing these interests?
- How resilient is the Netherlands to cyber threats?

Terminology

The analysis presented in the CSAN is primarily centred on three key concepts: *threat*, *interest* and *resilience* (see below). Taken together they determine the cyber risk. If, for example, the cyber threat rises while the level of resilience remains the same, the outcome is a greater overall risk, i.e. a greater chance or impact of cyber incidents. When there are more interests in play, for example because the Netherlands has digitalised more processes, this could lead to a greater risk, assuming that resilience and threat levels remain the same. This is because the impact of cyber incidents can increase due to greater dependence. A party's willingness to boost its resilience relates in part to its view of the cyber risk and other interests. This is a matter of governance and/or risk management.

Key concepts

Threat: a cyber incident or a combination of simultaneous or consecutive cyber incidents that could potentially occur. In the CSAN the focus is primarily on threats that may harm national security interests.
Interest: values, social gains, and tangible and intangible assets that may be damaged if a cyber incident occurs, and the importance that society or a party attaches to protecting them. In the CSAN the focus is on national security interests.
Resilience: the ability to prevent cyber incidents and, when cyber incidents do occur, to detect them, mitigate the damage and repair the damage more easily.
Cyber risk: the chance that a cyber incident could occur and the impact it would have, in light of the current level of cyber resilience.
Cyber incident: all events or activities that adversely affect the availability, integrity or confidentiality of information systems and process control systems, the data processed and stored thereon, and the services and processes dependent on them. An incident can either be a cyber attack (i.e. a malicious act by a cyber actor) or a breakdown caused by human error or a technical problem.
Digital domain: a complex environment resulting from the interaction of people, software and services on the internet, supported by worldwide distributed physical information and communications technology devices and connected networks.[II] A synonym for 'digital domain' is 'cyberspace'.
Cybersecurity: the full spectrum of measures designed to prevent damage through the disruption, failure or misuse of ICT systems and to repair such damage when it does occur.

II Definition of 'cyberspace' given in ISO/IEC standard 27032:2012 (E).

Scope

Digitalisation is the source of many opportunities; it also lends itself to various types of misuse. As stated above, the CSAN does not deal with the opportunities presented by digitalisation. Nor does it seek to address every possible form of misuse, as evidenced by the key concepts defined above. For example, terrorist propaganda falls outside the scope of the assessment. The same applies to certain forms of cybercrime. The CSAN does, however, focus on crime that uses ICT as a weapon to attack other ICT (aka computer-focused crime). The fact that certain other forms of misuse lie outside the scope of this report does not mean that they are unimportant, however.

Back to Table of Contents

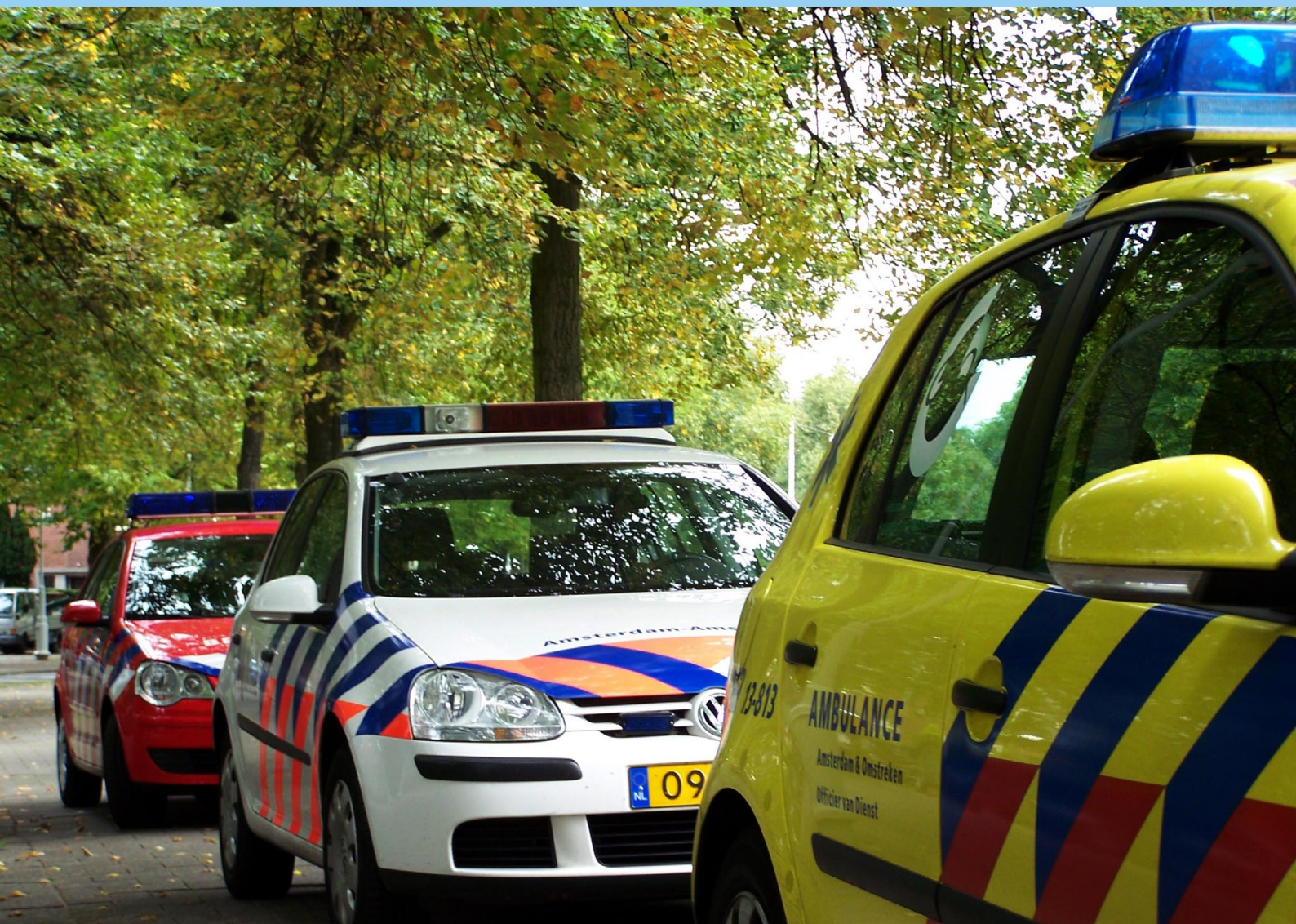
Background

CSAN 2020 is based on the insights and expertise of government agencies, organisations involved in critical processes, research institutions and other parties. The authors of the report also relied on public sources. CSAN 2020 was drawn up by the NCTV and the NCSC. The NCTV commissioned the Netherlands Organisation for Applied Scientific Research (TNO) to ask partners of the NCTV and the NCSC in December 2019 for online input on the chapter 'The year in review'. TNO also drafted the chapter 'Threat scenarios' under the editorial supervision of the NCTV. Monitoring cyber incidents, threats, interests and resilience is an ongoing process, with the CSAN as one of the annual results. Areas that have changed little, if at all, since previous editions of the CSAN are described in brief, or in some cases omitted entirely.

Structure

As its title suggests, chapter 2 presents an overview of the year: a look back on notable developments between January 2019 and February 2020. There is also a brief discussion of how some actors have attempted to exploit the COVID-19 pandemic to further their aims. Chapter 3 offers a preview of broader developments that could affect cybersecurity. Chapter 4 describes and explains the threat to national security in greater detail. Chapter 5 deals with the interests that can be affected by cyber incidents, the impact such incidents can have and the extent to which relevant parties can take this into account when weighing up these interests. The Netherlands' resilience to cyber threats is the subject of chapter 6. Chapter 7 describes three scenarios that collectively form a narrative that sheds further light on specific cyber incidents and their possible consequences. You can use these scenarios to determine what the findings of this CSAN might mean for you or your organisation. This chapter is new as of this year. The appendices explain the abbreviations and key terms and set out the sources and reference material used.

Cyber incidents revealed possible impact and level of dependence



2 The year in review

In 2019 and early 2020 there were no cases of social disruption as a result of cyber attacks or malfunction. Despite that, criminal cyber attacks on the municipality of Lochem and Maastricht University laid bare the potential impact of cyber incidents. Digital attacks were also observed, mostly carried out by state actors, for purposes of espionage, sabotage and information operations. There were also incidents involving the use of ransomware by criminals as a means of extortion. Systems failures had social consequences. For example, a malfunction at KPN caused the emergency telephone number 112 to go down, with the result that the police and ambulance services, for example, could not be reached for a time.

The *modi operandi* and the techniques used have largely remained the same. The use of ransomware by criminal extortionists and the active exploitation of vulnerabilities by both state actors and criminals was noteworthy, however. As in previous years, malicious actors are always looking for weak links in supply chains as a springboard to attacking attractive targets. Vulnerabilities in Pulse Secure and Fortigate virtual private network (VPN) software and in Citrix ADC and Gateway servers made it plain that such flaws can have a major impact.

Cyber attacks mostly perpetrated by state and criminal actors

As in previous years, cyber attacks were observed all over the world, carried out by both state actors and criminals.

Tensions between powers reverberate in cyberspace

Geopolitical developments have repercussions for the digital domain, and they can have an impact on the Netherlands, either directly or indirectly.[1] These days, conflicts increasingly play out in a grey zone between war and peace and on a variety of fronts. More and more, competition for global or regional dominance is taking place in non-military arenas, including cyberspace. A cyber attack can cause serious harm, in the political, military and economic spheres.[2]

AIVD and MIVD: the Netherlands is being targeted for digital espionage

Countries use espionage to achieve their political, military, economic and/or ideological goals. Research by the General Intelligence and Security Service (AIVD) shows that more and more countries are engaged in political and/or economic espionage. State actors continue to be highly successful in compromising systems, including government systems, both inside and outside the Netherlands. This continues to occur despite the investments that public institutions have made in cyber resilience.[3] In 2019 the Netherlands' Defence Intelligence and Security Service (MIVD) also identified various cyber espionage activities against the Netherlands, other Western countries and the interests of our alliances.[4]

The intelligence obtained through political espionage is used by states as a source of advance knowledge to prepare for future political or social developments. This intelligence can also be used to influence decision-making or elections or to hold sway over members of the diaspora. For example, intelligence may be gathered in order to play countries off against each other, so as to undermine unity and international cooperation within NATO or the EU.[5]

The Netherlands is a target of economic espionage. The Dutch economy is highly developed, innovative and internationally

oriented. Espionage activities may be aimed at improving one's own country's economic development or obtaining knowledge in the case of countries facing sanctions.[6]

AIVD and MIVD: digital sabotage is one of the biggest cyber threats

The AIVD and MIVD regard the possibility of digital disruption and the sabotage of critical infrastructure as one of the biggest cyber threats to the Netherlands and its allies.[7] Multiple states have demonstrated that they are both willing and able to commit digital sabotage in order to achieve their geopolitical goals. For some time now, the AIVD has noted that some of these states are making preparations to facilitate digital sabotage in the future. These preparations consist of infiltrating ICT systems associated with critical infrastructure and other sectors. In 2019 the MIVD also identified various preparatory activities for sabotage targeting Western countries and the interests of alliances to which the Netherlands belongs.[8] Currently, these states do not have the intention to engage in acts of digital sabotage against the Netherlands. However, this could change, depending on geopolitical developments.[9]

State actors are conducting information operations

A number of countries are using information operations as a tool in hybrid conflicts. These kinds of operations are used to sow division over issues that are sensitive in certain countries or alliances. Social polarisation and the splintering of the political landscape in a large number of countries create the conditions for this kind of interference. A 2019 investigation by the MIVD brought to light intelligence operations targeting the Netherlands, other Western countries and the interests of our alliances.[10]

Cyber attacks are an attractive business model for criminals

Over the past year, criminals have carried out multiple cyber attacks for the purpose of extortion, information theft and CEO fraud.[III] They consider this an appealing business model.[11] Extortion involving ransomware is a proven method in this regard (see 'Ransomware used for extortion').

Top echelon of cybercriminals may be working together in new ways

The police have observed a possibly new form of interaction between various groups within the top echelon of cybercriminals. Previously, these groups worked fairly autonomously, taking care of many stages of their operations themselves. Now it seems specific groups are cooperating. Both the police and a number of security firms find it plausible that some actors within the top echelon of cybercriminals are trafficking in access to commercial networks after compromising them and determining their value.[12]

State actor combines espionage and cybercrime

In 2019 a state-allied hackers collective was found to be engaged in both espionage and financially motivated operations.[13] Criminals often use the same (public) resources as state actors, and vice versa. In the past, state-allied actors from a different country also engaged in financially motivated attacks.

Modi operandi and tools of choice have largely remained the same

Ransomware used for extortion

It is increasingly common for criminal actors to use ransomware to force victims to pay them to unlock their systems. These actors mainly target organisations that are in a position to pay large sums of money[14] and/or those for which the continuation of operations and valuable, unique data play a key role. This method usually entails an extensive exploration of the network in question. This enables the actor to estimate the value of the data and the damage to the victim and to ensure that the ransomware is installed to maximum effect. On the basis of these insights, the amounts demanded can vary from a few tens of thousands to millions of euros.[15] There seems to be an increase in ransomware attacks in which data is not only encrypted but also copied. If the organisation refused to pay, the criminals would sometimes publish the data.[16]

In early February 2020 cybersecurity experts published articles about a new type of ransomware, known as EKANS, which targets industrial control systems (ICS) and is believed to have been developed by criminals. These systems are used, for example, for drinking water and energy supply systems. The method of attack is relatively simple, but it would seem that this ransomware was developed specifically to attack ICS. The victims of EKANS are thought to include the state oil company of Bahrain and various manufacturing firms. EKANS may be the first ransomware focused on ICS that was designed by a criminal actor.[17]

III CEO fraud is a form of business email compromise (BEC), which involves attempting to induce a company employee to transfer money into an account in the hands of a criminal.

Ransomware causes financial losses around the world

In March 2019 it emerged that the Norwegian energy and aluminium concern Hydro had been infected with LockerGoga ransomware.[18] Hydro, which also has plants in the Netherlands, was forced to halt production at various locations in Europe and the United States and, where possible, to switch to manual operations.[19] Recovery efforts took a considerable amount of time, and the concern's financial losses for the first half of 2019 alone are estimated at between €55 and €66 million.[20]

In the Netherlands the NCSC, together with both Dutch and international partners, launched an investigation in March 2019 into LockerGoga ransomware. It emerged from this investigation that the actors were using multiple ransomware variants, including MegaCortex, Ryuk and Maze. It also transpired that there may be a considerable amount of time (i.e. months) between the initial infiltration of a system and the deployment of the ransomware. It is believed that the attackers use this time to collect information about the organisation so as to calculate a 'customised' ransom. However, other motives, such as espionage or sabotage, cannot be ruled out. Wherever possible, potential victims are notified by the authorities so they can take measures to prevent further harm. As of mid-2019 the number of victims in the Netherlands was limited. There were no known victims in the critical infrastructure sector or central government.

Generic malware used to mount ransomware attacks

Emotet and Trickbot are generic malware variants that have been associated with ransomware attacks.[21] They have been transformed into multifunctional attack platforms that can be used, for example, to drop in additional types of malware, such as ransomware. The Dutch police have observed that the deployment of ransomware can be the final step in a cyber attack. It is quite possible that other activities could have occurred during the span of time between the initial infection and the placement of the ransomware. These activities can include copying information or securing access to the network at a later time.[22] In many cases Emotet is used as a springboard to installing Trickbot.[23] Trickbot is the name of a family of malware that can facilitate additional functionalities by way of discrete modules, for example the ability to track keystrokes and mouse movements.

Ransomware attack on Maastricht University

On 23 December 2019, Maastricht University was the victim of a ransomware attack. The attacker gained access to the university's network after staff members had opened a link in a phishing email two months before. After gaining access to the system, the attacker compromised multiple servers and explored the network in order to broaden access to the network. The attacker succeeded in obtaining administrator rights over university servers because two of the servers had not installed essential security updates from May 2017.[24]
On 23 December 2019 the attacker rolled out Clop ransomware on a segment of the servers. Files were encrypted on at least 267 servers. As a result, emails, research data and computers were rendered inaccessible, and a number of websites were blocked. And because back-up servers were also affected, the recovery operation was complex. The university decided to pay €197,000 in ransom to the (presumably Russian) criminals in order to gain access to the encrypted files.[25] The University reported the hack to the police.
According to an investigation into the ransomware attack, this '[...] occurred due to a combination of several missed security updates, limited segmentation within the network, a failure to follow up on various alarm signals and human error'.[26]

Misuse of legitimate tools and generic services

One of the key findings of CSAN 2019 is that advanced attacks can be carried out with readily available technology.[27] Freely accessible technology (for applications like ICT management) and generic services (e.g. public cloud or email services) are used in cyber attacks. IBM has observed an increase in the use of legitimate technology instead of malware: over half of the cyber attacks (57%) used ordinary management applications like PowerShell and PsExec.[28] An analysis by the security firm Positive Technologies on the techniques that 29 recent attackers used in their campaigns revealed that over half of them deployed legitimate, publicly available penetration-test and system-management tools.[29] A known example of misuse of legitimate tools is Cobalt Strike.[30] The use of legitimate tools and generic services hampers both detection and attribution.[31]

Cyber attack on the municipality of Lochem via Remote Desktop Protocol (RDP)

A cyber attack on the municipality of Lochem in early June 2019 exploited a vulnerability in a Remote Desktop Protocol (RDP). RDP is used to manage computers remotely. The hackers behind the Lochem incident used brute-force attacks on the RDP port in order to gain access to a server used to enable remote working. After logging into the server the attacker(s) installed various applications which afforded them a glimpse into the network and its users. Ransomware was also deployed, encrypting a number of files. Following the attack it was decided to reconfigure the computer systems. As a result, certain municipal services, such as submitting a passport application or change of address or registering a birth, were not available for period of time. The financial losses due to the attack amounted to €200,000.[32]

Malicious actors seek to exploit current situation

Active misuse of various vulnerabilities

In 2019 and early 2020, both state and criminal actors were observed to actively misuse various vulnerabilities.[33] The AIVD and MIVD confirm that state actors have exploited vulnerabilities in Fortigate and Pulse Secure VPN software. In this context, the AIVD and MIVD advised various companies and other organisations about what measures to take.[34] Malicious actors were quick to misuse vulnerabilities in Citrix ADC and Citrix Gateway servers after the publication of an exploit on 9 January 2020.[35] The AIVD and MIVD confirm that a state actor exploited the published vulnerability in Citrix servers in preparation for cyber espionage.[36] Criminals took advantage of the vulnerabilities in Citrix servers to infect organisations with ransomware.[37]

Actors seek to take advantage of COVID-19 pandemic

Shortly after the outbreak of the COVID-19 pandemic, there were indications that actors were opportunistically taking advantage of the situation to carry out 'theme-based' cyber attacks. For example, hospitals, research institutions and the World Health Organisation (WHO) were all victims of cyber attacks.[38] But the healthcare sector was not the only target; government agencies[39] and ordinary members of the public[40] also had to deal with a variety of cyber attacks.[41]

Altering DNS settings as an attack technique

Incidents that occurred during the period covered by this report suggest that there is (renewed) interest in altering Domain Name System (DNS) settings[IV] (aka a DNS hijack[42]) as an attack technique. By changing an organisation's DNS settings, for example by hacking into a registrar, malicious parties can temporarily divert and intercept incoming network traffic. This technique can be used for various ends, including espionage. DNS attacks can have considerable impact on the integrity of the internet.[43]

Increase in phishing via text message

For years, phishing has been a popular way for cybercriminals and other malicious actors to carry out attacks, and this past year, too, it was the most common method of attack (sometimes as a first step in a more complex process).[44] Incidents show that criminals are branching out into a new form of phishing using text messages (referred to as 'smishing') or WhatsApp. They are also exploiting the increasing use of technology that enables private individuals to send payment requests via messaging apps.[45] It cannot be ruled out that this technique is being used for purposes other than fraud, such as taking over accounts as a first step in a wider attack. Other actors could use this technique as well.

Misuse of Dutch ICT infrastructure

Dutch ICT infrastructure is also misused by state actors to carry out cyber attacks on other countries. The Netherlands is attractive in this regard due to its high-quality digital infrastructure and the relative ease of renting ICT capacity. This form of misuse can harm the Netherlands' international image and adversely affect the interests of alliances to which it belongs and the integrity of Dutch ICT infrastructure.[46]

As in previous years, Dutch ICT infrastructure is being misused for various types of cybercrime, including the facilitation of cyber attacks.[47] Dutch servers are also misused for botnet spam. Of all the servers used by cybercriminals around the world for spamming via botnets, approximately 6.3% are in the Netherlands.[48]

More large-scale DDoS attacks

In 2019 the Dutch Internet Providers Management Organisation (NBIP) registered '919 DDoS [distributed denial of service] attacks. There were 938 for the whole of 2018. The maximum size of a DDoS attack was 124 Gbps, compared to 68 Gbps in 2018 and 36 Gbps in 2017. This means that the maximum size was almost twice what it was in 2018. In 2019 there were 29 attacks that lasted for longer than four hours, compared to 22 in all of 2018. So these types of attacks are also on the rise.' The NBIP notes 'a trend whereby more large-scale DDoS attacks are being used to render a particular service inaccessible.'[49] Experts consulted on the matter indicated that the feared leap in technical complexity did not occur.[50] The Netherlands Bureau for Economic Policy Analysis (CPB) has stated that the Netherlands is still at risk of DDoS attacks and that the potential financial impact could be substantial.[51]

IV DNS is the network protocol that is used on the internet to translate domain names into IP addresses and vice versa.

Actors hit a variety of targets

Supply chain misused by compromised ICT products

Actors are focusing more and more on the weak link in chains on which the intended target is dependent. That can be a simpler approach than mounting a direct attack on the organisation in question.[52] During the period under review, attacks on much used products in order to gain access to the intended target stood out. For example, in early 2019 a cyber attack was discovered in which the software update programme ASUS Live Update was misused in order to install a backdoor via a malicious update.[53] In October the anti-virus software company Avast announced that an actor had succeeded in infiltrating their internal network.[54] State-allied actors were believed to have been involved in both attacks.[55] It is suspected that the actor behind this recent attack on Avast was seeking to compromise CCleaner as a preliminary step to attacking other targets, as had previously been done in 2017.[56] Such access can be misused for digital espionage and sabotage. The AIVD has warned of new risks of cyber espionage as a result of inadequate security at suppliers, given that the production process, having been fragmented by globalisation, now extends across national borders.[57]

Various sectors and organisations, including critical sectors, have been targeted

According to a study by Ponemon in the UK, the US, Germany, Mexico, Australia, Japan and elsewhere, at least 90% of the organisations with process control systems studied, including those in the healthcare, transport and utilities sectors, were the victim of a successful cyber attack.[58] Other sources report attacks on the energy, nuclear, oil and chemical sectors.[59] Dragos has also noted an increase in both the frequency and complexity of cyber attacks on critical infrastructure.[60]

In the past, state actors have repeatedly demonstrated that they possess both the intention and the capacity to carry out cyber attacks on critical infrastructure or on suppliers of systems (including ICS)[V] used in it. A 2019 cyber attack on an energy supplier in the Middle East probably used a destructive type of malware that made it possible to re-write hard discs in order to render computers unusable.[61] Previously, it transpired that a state actor was also targeting the ICS supply chain, possibly with a view to committing sabotage.[62] The AIVD has determined that state actors are embedding themselves in ICT systems of various organisations, including those associated with critical infrastructure.[63]

Multiple espionage campaigns have been observed targeting organisations from various sectors. Research by the AIVD and MIVD has revealed that several leading economic sectors in the Netherlands have fallen victim to cyber espionage, particularly the high-tech, energy, maritime and life sciences & health sectors. Other targets include suppliers of government ministries (including the Ministry of Defence), critical sectors, and various other organisations, such as telecom providers, universities and other educational institutions, research institutions, think tanks, biotechnology firms, startups and the wider business community, which are hacked in an effort to obtain personal information and other forms of data.[64] Three Dutch universities and an institution of higher professional education were targeted by state-sponsored hackers in late 2019 and early 2020, who sought to steal academic knowledge such as books and other teaching material.[65] In February 2020 a research group at VU University was briefly the victim of a cyber attack in which the attackers managed to gain extensive rights for one of the servers that contained research findings.[66] Outside of the Netherlands, a number of attacks on European embassies attracted attention.[67] The AIVD has reported that ministries, intelligence and security services, political parties, sociocultural organisations and other entities have all been the target of political espionage.[68]

In addition to the financial sector, the industrial sector, municipalities and educational institutions have also been the target of cybercriminals in the Netherlands. In the US, France and Germany, such attacks on municipal institutions and hospitals have led to serious disruption to public services.[69]

A variety of vulnerabilities with potentially major consequences

As in previous years, during the period under review a variety of vulnerabilities with potentially major consequences for many organisations came to public attention. A vulnerability is a characteristic which enables an attacker to carry out a cyber attack or which can lead to a system failure. It may be a characteristic of a digital service, process or system, of a specific organisation, or indeed of society as a whole.

Vulnerabilities in hardware with (potentially) major consequences announced

The past year witnessed a further growth in the number of hardware vulnerabilities. This year, too, a certain type of attack (i.e. a transient execution attack) led to changes to all Intel processors and all popular operating systems. SSDs[VII] with hardware encryption contain such serious vulnerabilities that the encryption has no value whatsoever. Even the Dynamic Random Access Memory (DRAM) chips that have recently arrived on the market proved still to have known vulnerabilities. This DRAM vulnerability is especially troubling because no solution has yet been developed for it, and it will remain present for years. There are currently no alternatives.[70]

V Industrial control systems (ICS) are measuring and regulatory systems, designed to guide, for example, industrial processes or the management systems of buildings.

VI A solid-state drive (SSD) is a specific medium for storing digital data. SSDs are mainly found in systems where a hard disk would traditionally have been used.

Dutch organisations were vulnerable for months through VPN servers

In August 2019 a security researcher warned that serious security leaks in VPN servers from both Fortigate and Pulse Secure were being actively misused.[71] Although there were updates available for both vulnerabilities, as of August there were still numerous vulnerable systems online. For example, according to the media, various Dutch organisations still had not installed the two available patches for vulnerabilities in Pulse Secure in August, including two subdivisions of the Ministry of Justice and Security.[72] The Fortigate vulnerabilities enable a malicious party to carry out attacks that could lead to denial of service, the manipulation of data and access to sensitive data. The last two of these risks also apply to the Pulse Secure vulnerabilities. In September 2019, further reports appeared in the media when it emerged that various Dutch organisations were still vulnerable. [73]

Vulnerabilities in Citrix servers expose many organisations to misuse

On 17 December 2019, Citrix announced that vulnerabilities had been discovered in Citrix ADC and Citrix Gateway (previously known as Netscaler). By exploiting these vulnerabilities, a malicious party can, in certain situations, gain access to the local network and local systems.[74] The published announcement also contained a temporary solution. Citrix advised all users of the systems in question to take mitigating measures. According to Citrix, the reason for the announcement was that three different security researchers had reported this critical vulnerability within the span of two days. This increased the chance that the security leak would become known before a solution was available. In addition, one of the three security firms planned to announce the vulnerability, come what may, on 23 December 2019. According to Citrix there was thus no possibility to keep the leak quiet for several weeks in order to develop a patch.[75] On 24 December 2019 the NCSC issued a High/High security recommendation[VII] about these vulnerabilities.[76]

On 8 January 2020 security researchers announced that actors were actively looking for vulnerable Citrix ADC and Citrix Gateway servers.[77] Shortly after that, exploits were announced to misuse these vulnerabilities. At that point the Netherlands had hundreds of vulnerable Citrix servers according to researchers.[78] After the exploits were announced, various organisations were attacked[79] and compromised.[80] In order to prevent misuse to the greatest possible extent, the NCSC has monitored the situation continuously, issued recommendations and conducted technical research.

On 20 January 2020 the first patches were issued by Citrix. These offered a solution for around 50% of the vulnerable Citrix systems in the Netherlands. The remaining necessary patches were ready on 24 January.[81] In the period between the publication of the exploits and the implementation of the patches, organisations were potentially vulnerable to misuse.

Citrix was criticised for its response. Due to the publicity about the vulnerability and what some characterised as a less than adequate solution, both researchers and malicious parties were able to determine exactly what the vulnerability was and develop an exploit.[82]

VII The security recommendations issued by the NCSC are plotted on two 'axes': the chance that the vulnerability will be exploited and the severity of the resultant damage if it is. These possibilities are each ranked as low, medium or high.

Vulnerabilities as a result of production and supply chain dependencies

Because organisations make use of products and services from other parties, a single incident can have repercussions throughout the entire chain.[83] The Scientific Council for Government Policy (WRR) has, for example, pointed out the vulnerabilities that have arisen as a result of complex, transnational production and supply chains and the use of generic hardware and software.[84] For its part the National Security Agency (NSA) has warned about the risks associated with the use of cloud services. While such services can improve an organisation's security, they can also introduce risks that must be taken into account.[85]

System failure with ramifications for digital and physical networks

Unavailability 112 illustrates chain dependence

The unavailability of the national emergency numbers on 24 June 2019 is a good illustration of chain dependence of ICT networks and the impact of service disruption. That day, due to a malfunction in KPN's telephone network, the national emergency number 112 and the national police number 0900 8844 could not be reached for several hours. Other organisations, including hospitals, were difficult or impossible to reach as a result of this breakdown. With 112 out of service, it was more difficult for those in need to contact emergency services.[86] The existing emergency plans were ill-suited to a situation in which both 112 and 0900-8844 were simultaneously unreachable.[87] It was reported that KPN's back-up facilities did not work either.[88]

Malfunctions associated with major technology companies can cause chain effects

In 2019 reports appeared in the media about a number of system failures suffered by global technology companies, such as Cloudflare, Amazon Web Services (AWS) and Google Cloud. Those failures not only had global consequences for many other organisations; in some instances, they also impacted other major technology companies. For example, according to the media, an outage at Cloudflare, which is actually meant to prevent malfunctions and delays (among other things), on 24 June 2019[VIII] affected 16 million apps and websites around the world, including in the Netherlands. This problem was caused by a network configuration error at a local provider in the US city of Pittsburgh which was mistakenly replicated by Verizon, an international provider. This concatenation of errors is thought to have led not only to the above-mentioned outage at Cloudflare, but also to similar problems at Amazon and Facebook. Causes of malfunctions mentioned in the media include network congestion, a software error, a DDoS attack, a failure at another party and a power cut. According to the media, a backup generator failed during a power cut at AWS.[89]

Malfunctions at Dutch organisations illustrate dependence on ICT

In 2019 various system failures at Dutch organisation made the news. There were both nationwide and regional malfunctions at telecom providers, some of which affected not only their own customers but also those customers' customers. For example, a problem at Tele2 meant that government agencies, municipalities, the judiciary and the Netherlands Vehicle Authority (RDW) were difficult or impossible to reach and that people with an electronic ankle tag could not be tracked. ICT failures at multiple hospitals were also covered in the news. As a result, operations had to be cancelled, and patients were referred to different hospitals.[90] The Dutch Safety Board (OVV) has concluded that hospitals' awareness of the risks posed by an ICT failure has not kept pace with these hospitals' increased dependence on ICT.[91]

The various facets of resilience

Examples of doubts surrounding resilience

A good illustration of the kind of doubts that can arise with regard to cyber resilience is the case of serious vulnerabilities in the VPN servers of Fortigate and Pulse Secure. In August 2019 it emerged that these vulnerabilities could still be found in numerous systems, despite the availability of patches and warnings about misuse. The case of vulnerabilities in Citrix ADC and Gateway servers is also instructive: in early January 2020 certain organisations had not yet taken the recommended mitigating measures, even after an exploit was made available.[92] Despite the availability of security updates and the publicity in the Netherlands, vulnerable Citrix ADC and Gateway servers could still be found at 150 companies in the Netherlands as of 7 February, according to the media.[93] According to the Dutch Safety Board, ill-advised choices in the design and management of the ICT infrastructure and in the preparation for a possible ICT breakdown, contributed to the protracted ICT breakdown at the hospitals studied.[94] The head of the AIVD pointed out that improvements must be made to our resilience to the invisible threat posed by state and criminal actors.[95] The Radiocommunications Agency determined that the digital security of internet-of-things devices is generally not at an acceptable level. Seventeen of the 22 devices studied scored between 'mediocre' and 'very poor' when it came to basic security and privacy.[96] In May 2019 and May 2020 the Netherlands Court of Audit stated that information security at the ministries and the central government organisations studied was still not up to par. [97]

VIII There are no indications that this disruption is connected to the previously mentioned malfunction in the Netherlands at KPN.

Perception that privacy legislation poses obstacles

A number of experts consulted indicated that privacy legislation seems to have a negative effect on cooperation, information-sharing and investigation practices, if only because it is unclear to some parties how to deal with the General Data Protection Regulation (GDPR). 'In areas where the importance of cooperation and information-sharing has grown in recent years, it would seem that the new legislation has thrown up new obstacles.'[98] There are organisations that believe, for example that the GDPR does not offer a basis for processing or sharing information with partners, particularly those outside the EU.

Criticism of the government's response towards the business community

A number of experts consulted criticised the government's sharp response towards the business community for not having their security measures in order following the VPN (Pulse) vulnerability, when the government itself was found to be vulnerable. According to them the government's criticism put the cybersecurity cooperation between the public and private sector under strain.[99] This criticism 'from the government' focused on the fact that organisations were vulnerable for months because they had not installed the available patches, even though both the opportunities for and several instances of misuse were known (see 'Dutch organisations were vulnerable for months through VPN servers').

WRR believes that the Netherlands is insufficiently prepared for cyber incidents

The WRR finds it noteworthy that virtually all of the measures and ambitions of the government and other key parties are aimed at *preventing* cyber incidents. Preparations for the effects of disruption, on the other hand, are given little attention. Whereas it is largely clear what can and should be done in the case of a physical disaster, such as a dike breach, the full implications of disruption with a cyber component are largely unknown and uncertain. Moreover, the government has insufficient resources to take action, in part because a great deal of infrastructure is in the hands of private parties, often from outside the Netherlands.[100]

Criminal investigations

The police conducted various investigations into cybercrime, including into actors involved in carrying out or facilitating cyber attacks. For example, in 2019 the Dutch police turned their attention to a bulletproof hoster[IX] which led to the takedown of a botnet and the arrest of two suspects. With the arrest of a Dutch national on suspicion of developing and selling malware, the police stopped the spread of the popular Rubella virus. In February 2019 a group of cybercriminals were caught red-handed sending phishing emails from a hotel room in Soest and stealing victims' telephone login details for online banking. In 2019 various police units arrested individuals on suspicion of hacking social media accounts. With the support of Europol a number of countries put an end to the activities of the international criminal GozNym network, which used GozNym malware. This malware was employed to steal an estimated €100 million from over 41,000 victims.[101] In connection with an international investigation operation in January 2020, the police arrested a Dutch national on suspicion of offering around 12 billion login names and stolen passwords.[102]

Preventive partnerships

Various preventive partnerships have been formed or strengthened.[X] Such partnerships enable the police to put up barriers against cyber attacks or their facilitation. For example, the police work with other parties in projects like 'NoMoreRansom', 'NoMoreDDoS', 'NoMorePhishing', 'Hack_Right' and in operations to reduce helpdesk fraud.[103] In addition, the Network and Information System (Security) Act provides for four sector-based computer crisis teams: one for healthcare (Z-CERT), one for municipalities (Information Security Service, IBD), one for water authorities (CERT Water Management) and one for education and research (SURFcert). This makes it possible for the parties involved to engage in more intensive information-sharing about cyber attacks and to work with the NCSC in the framework of a nationwide system.[104] In 2019 the participating parties in the National Response Network (NRN) signed a partnership agreement for the purpose of pooling the knowledge and capabilities of those involved and, by doing so, further enhancing the response to these kinds of incidents.[105]

Weighing up competing interests and concerns about dependence on foreign parties

Examples involving the trade-offs between digital security and other interests

Parties need to weigh up the interest of digital security against other interests. This means that cybersecurity is a complex trade-off between optimal service and a safe government.[106] Educational institutions see a dilemma between open, accessible education and knowledge institutions, on the one hand, and digital security, on the other.[107] There is a tension between the use of encryption as a security tool and the need for intelligence and security agencies to access information in connection with their work. For example, both the US and the UK have pressured Facebook not to roll out end-to-end encryption.[108]

Concerns remain about dependence on foreign parties

Previous CSANs concluded that the continuity of core social processes is greatly dependent on major foreign providers of digital facilities. The WRR has since echoed this conclusion. State actors

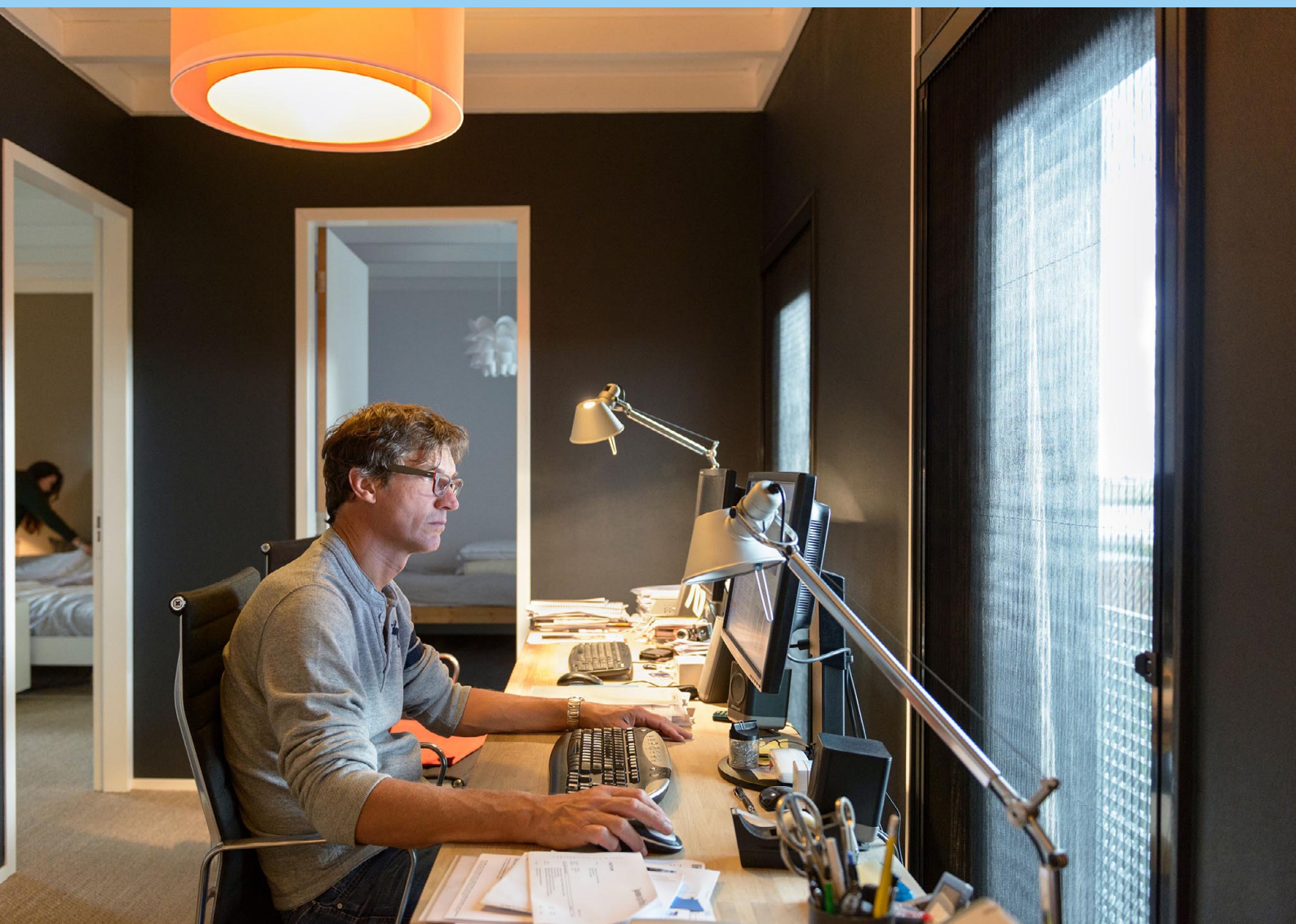
IX A bulletproof hoster offers servers for criminal purposes and protects them from investigative agencies.

X This overview is not meant to be exhaustive. It is merely a list of a few examples.

are now targeting these facilities, and the cooperation of those providers is necessary when incidents occur. National governments may lack sufficient powers to compel them to cooperate.[109] That dependence was evident in the Citrix case. According to researchers, the vulnerabilities in that case put 80,000 organisations in 158 countries at risk. In the Netherlands over 3,700 organisations were reportedly affected.[110] One cybersecurity firm stated that caution is advised in light of the sheer variety of products and services and the large amount of data they generate, given that this kind of bundling can lead to a greater failure if it occurs.[111] The Network of Analysts for National Security highlighted the lack of good alternatives when breakdowns occur in the products or services of major technology companies.[112] A number of experts have noted the greater focus on digital sovereignty and dependence on foreign systems for our core infrastructure.[113] News reports regularly express concerns about Huawei in relation to the rollout of 5G, partly in light of geopolitical tensions between the US and China.[114]

Back to Table of Contents

Geopolitical tensions increase the digital threat



3 Looking ahead

The progressive digitalisation of our world will affect both the threat and our level of resilience and magnify the importance of digital security. Mounting geopolitical tensions will increase the digital threat posed by state actors. Techniques and technologies which have long been the subject of discussion, such as artificial intelligence, will be implemented more widely in the years ahead. This has both positive and negative implications for digital security. In the years to come, digital security will also be influenced by the interaction between technology and other developments. For instance, the further transition to a data-driven economy, with the associated concerns about privacy and digital security, will only increase the importance of digital security. The COVID-19 pandemic has led to a further increase in the use of digital services and the digital domain. This can stimulate further digitalisation, which in turn increases the importance of digital security.

Issues raised in CSAN 2019 are still relevant

The 'Looking ahead' section of CSAN 2019 already dealt with the advent of artificial intelligence and the repercussions for digital security. It also pointed out that geopolitical developments would further magnify the threat posed by state actors. The fundamental misalignment of interests between countries and differences of opinion about international norms and values aggravate this threat. It is unclear if the incentives for boosting resilience are keeping pace with the threat and the interests at stake. There seems to be a rise in geopolitical tensions over technology and dominance. CSAN 2019 also noted that digitalisation is leading to an expansion of the attack surface and a shift in actors' focus to other and new valuable targets. System failures will have a greater impact on society due to more advanced digitalisation and the ensuing far-reaching dependence on digital processes and systems.[115]

Further implementation of technology affects digital security

The years ahead will mainly be characterised by the further implementation of techniques and technologies which have been discussed for some time. One example of this is artificial intelligence.[116] Our society will also be increasingly shaped by the policies of major technology and social media companies. These wide-ranging social developments will also have repercussions for digital security, both positive and negative, which will be explored further below.

Spread of autonomous systems leading to greater digital vulnerability

In addition to its positive aspects, the spread of autonomous systems, such as self-driving cars and the wide variety of internet-of-things products, also has consequences for digital security.[117] For example, IoT devices are regularly found to have vulnerabilities that cannot be (fully) rectified by patches.[118] In addition, the failure of autonomous systems can lead to accidents (e.g. in the case of self-driving cars) or, in the worst-case scenario, to social disruption. The increased prevalence of autonomous systems also increases the attack surface for malicious parties: actors have a growing number of methods at their disposal to mount a cyber

attack. Finally, the large number of devices observing the world around us and recording the associated data, such as smart cameras, are attractive for the purpose of espionage.

Smart algorithms have both positive and negative effects on digital security

The trend whereby systems are becoming increasingly capable of independent learning, understanding and reasoning has continued in the period under review.[119] This has implications for digital security. Smart algorithms are partly public and offer new opportunities to link to a variety of data sources. These kinds of linkages can lead to the misuse of personal data. Because users are often unaware of what is being done with their data, it is difficult to defend against the actions of malicious parties. On the other hand, smart systems can also be employed to defend against cyber attacks and can play a role in prevention, protection, detection and response.

The emergence of large, interlinked networks poses a challenge to resilience

In the digitalised world, interconnected networks of data, services and systems are becoming ever more extensive.[120] From the point of view of resilience, the main question is how these networks can be organised in a secure way. In the current situation it is often unclear how networks and their component parts are controlled. As a result of connected clouds, bits of data are invisibly connected to each other, making it difficult to supervise, let alone manage, that data. Data management will become even more challenging in light of the possibility that users and managers might lose insight into and a grasp of their own digital ecosystem. On the other hand, such services are being professionalised by these providers. Ideally, with time, insight into data management and 'security by design' will increase.

Dependence on foreign technology makes us vulnerable

Rapid digitalisation has created a dependence on technology which comes from outside the Netherlands and lies beyond the control of the Dutch authorities.[121] Dependence on technology offers opportunities, but it also makes us vulnerable to system failures and to the actions of malicious parties, especially foreign parties that are assertively pursuing their own geopolitical agenda. In the worst-case scenario, incidents can lead to social disruption. When they occur, system failures make it clear how dependent society has become on these services, without good alternatives. The dependence on external technology and the vulnerabilities this entails is increasing all the time due to further transformation in the direction of a data-driven economy (see 'Social developments increase importance of digital security').

Digital security is affected by other developments

The interaction between technology and other developments has implications for digital security.

Geopolitical tensions resonate on global IT market

Geopolitical developments are expected to affect the digital domain in the coming years, with countries attempting to influence emerging internet standards. Security interests will play a greater role in the choices that are made in relation to ICT infrastructure. With the rise in geopolitical tensions and mistrust of hardware/software, producers and service providers, the number of trusted products and suppliers per country or region may decrease. This could lead to a fragmentation of ICT markets on the basis of geopolitical considerations[122] as countries pursue greater digital sovereignty.[123]

This makes digital security an interest that countries will increasingly prioritise. Countries both near and far will try to gain a better grasp of ICT infrastructure for reasons of security. In this light, it is conceivable that Europe could find itself caught between the two main power blocs: China and the US. With the implementation of new technology and the high degree of penetration of ICT and networks, risk assessments will look different from before. Security interests will play a more prominent role.

Social developments increase importance of digital security

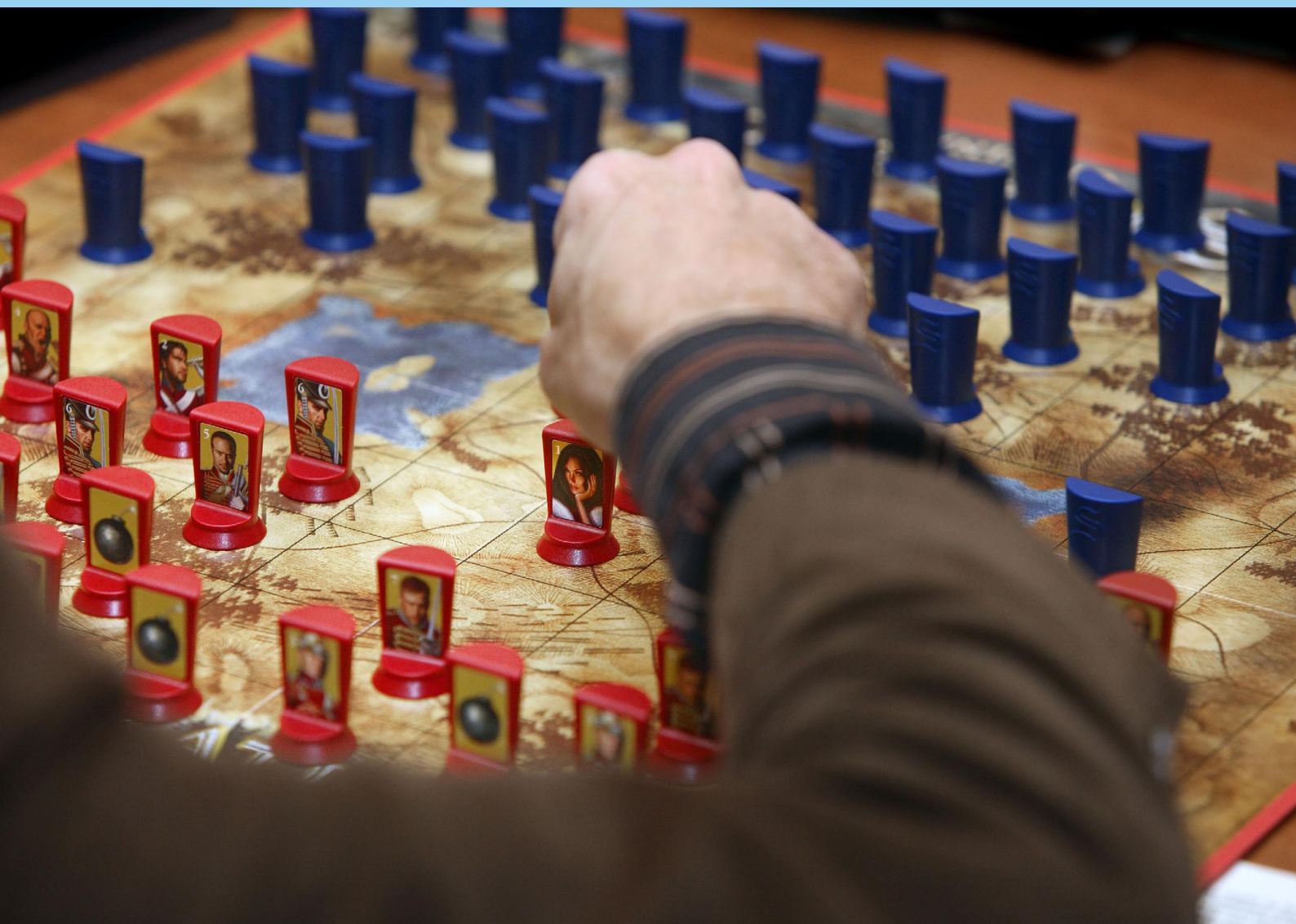
Another social development that increases the importance of digital security is the further transformation towards a data-driven economy, with all the associated concerns about privacy and digital security.[124] In a digitalised economy, people and machines become increasingly complementary. New technologies form the basis for the 'fourth industrial revolution' in which autonomous systems in production chains are closely connected and function in a data-driven manner. In the data-driven economy, deep, extensive and complex dependencies are arising due to the increasing use of platforms originating from major political powers. This is also giving leading technology companies and their products ever more access to critical processes. In this way they are carving out positions of power within national economies. On the other hand, countries may be trying to gain a better grip on their own infrastructure (see above).

A recent development is the social impact of the COVID-19 pandemic. Thanks to digitalisation, commercial, educational and social activities that would otherwise have been halted have been able to continue, at least in part. The downside of the current situation, in which many people are working from home, leisure activities are also primarily occurring at home, and many services are now being provided digitally, is that the digital domain is under unprecedented pressure. With the advent of the '1.5 metre society', social continuity will depend more than ever on the digital

domain. The current situation shows the crucial importance of digital security. More than in the past, a major breakdown can lead to social disruption. The increased use of the digital domain also creates more opportunities for malicious parties. For example, criminals were quick to capitalise on this increased usage, and the new situation also offers opportunities for state actors, for example in the realm of espionage.

Back to Table of Contents

Organisations also targeted to serve as springboard to other organisations.



4 Threat

As in 2019, it can be concluded that the cyber threat is permanent in nature and that cyber incidents can cause harm that leads to social disruption. Espionage, sabotage and preparations for sabotage, and malfunctions of digital services, processes and systems, pose a particular threat to national security. The threat of malicious activities (cyber attacks) is posed primarily by state actors. Cybercriminals, e.g. criminal extortionists, also pose a threat. If the threat manifests itself primarily against the digital domain and Dutch critical processes, the impact on national security may be significant. Cyber incidents targeting other sectors, parties and processes that are crucial to (Dutch) society may also have a significant impact. The digital domain, the global supply chain, critical processes and other organisations may be targeted to serve as springboards to other targets. Dependency on products or services from countries with an offensive cyber programme against the Netherlands is a risk-enhancing factor.

The incidents described in chapter 2, 'The year in review' (hereafter 'review'), give an idea of the direction in which the threat may be developing. State actors are using information operations for geopolitical purposes. One state actor has been found to be carrying out complex attacks on a broad target group. The loss of system integrity or data integrity may also have far-reaching consequences for national security. The possible scope and consequences of such a loss of integrity are unclear.

Threat posed primarily by state and criminal actors

Main focus of state actors – besides espionage and sabotage – is on information operations

State actors are primarily involved in espionage and sabotage (see 'Espionage, sabotage and system failures are threat to national security'). They also carry out information operations and, by doing so, adversely affect the integrity and confidentiality of systems and information.[125] There is no reason whatsoever to believe that they will cease these activities. States can use information as a weapon to promote their own image (propaganda) or to influence others by sowing doubt, fear or indecision. The practice of using untrue, inaccurate or misleading information for this purpose is known as disinformation. Propaganda and disinformation do not by definition have a cyber component as referred to in the CSAN. This is, however, the case for hack-and-leak operations, whereby authentic information obtained by way of a digital attack is leaked at a specific moment.[126] Often, when information is leaked, it is framed in a certain way, placed in a context that may not necessarily be accurate, but that makes its effect more harmful. Hack-and-leak campaigns are carried out against businesses, politicians and government bodies.[127] Influencing operations, which are a type of information operation, often also have a digital component, since they adversely affect the integrity or confidentiality of information.

Threat posed by cybercriminals is undiminished

In addition to the threat posed by state actors, that posed by cybercriminals to the confidentiality, integrity and availability of digital services, processes and systems is also undiminished.[128] Globally operating sophisticated cybercrime groups remain active, with targets including the financial sector. The Cobalt group, for example, attempts to bring the internal networks of banks under its control, in order to subsequently siphon off large sums of money by manipulating cash machines, bank account databases or

SWIFT transactions.[129] Criminal service providers who, by offering the necessary tools, enable a range of actors to carry out cyber attacks (cybercrime-as-a-service) also continue to pose a threat.

Increased threat of extortion

The review revealed an increase in the threat of extortion by cybercriminals in connection with data confidentiality breaches or interference with availability. These cybercriminals use ransomware to attack organisations which they believe are in a position to pay significant sums of money and/or for which the continuation of operations and valuable unique data play a key role. It has emerged that organisations do indeed pay ransoms. In some cases the criminals threaten to disclose their copied data if they do not. This threat is sometimes carried out.[130] Cybercriminals are likely to continue using this method for as long as it remains an attractive revenue model.

The threat posed by cybercriminals against industrial control systems (ICS) may be increasing further. The review mentions new ransomware called EKANS, which targets ICS and which is probably the work of criminal hackers.[131] It is possible that cybercriminals increasingly have the intention and capacity to attack critical infrastructure for financial gain.[132] After all, ICS are an attractive target because their availability is essential to organisations' ability to function. This increases organisations' willingness to pay a ransom in the event of a ransomware attack. Attacks on ICS can have a disruptive effect, for example if the electricity network is affected. To date, most known digital attacks targeting ICS have been carried out by state actors.[133] Moreover, it cannot be ruled out that state actors are deliberately trying to make attacks seem criminally motivated to make them harder to attribute. Their actual objective may be espionage or sabotage. As noted in the review, there is also the possibility of the activities of state and criminal actors being intertwined or of state and criminal actors working together.

Threat posed by other categories of actors is small

The threat posed by ideologically motivated actors (hacktivists and terrorists) and personally motivated actors (insiders, cyber vandals and script kiddies) is relatively small. For several years now, no substantial attacks by these categories of actors against the Netherlands or Dutch interests have been observed. There is no reason to assume this will change in the coming years. Polarisation in society on issues including the policy on nitrogen pollution and the rollout of 5G may, however, lead to an increase in the number of cyber attacks by hacktivists or physical attacks with digital consequences, such as the recent arson attacks on mobile phone and internet masts. Such attacks may cause service failures that render telephone networks and the emergency number (112) unavailable.[134]

Espionage, sabotage and system failures are threat to national security

Threat of digital espionage and sabotage by state actors is undiminished

As already noted in the review, tensions between powers are also spilling over into the digital domain. An increasing number of state actors are actively involved in political, economic or military espionage and sabotage or preparations for sabotage.[135]

Digital espionage adversely affects system confidentiality. A noteworthy international example of a digital espionage campaign during the period under review is the large-scale misuse of serious vulnerabilities in iOS and Android software including a zero-day vulnerability affecting Android software.[136] These vulnerabilities were exploited to carry out complex attacks on a wide range of targets. As far as is known no previous cases have been observed of state actors using such complex tools to conduct such a *broad* attack. The assumption had been that actors would make targeted and limited use of such tools in order to avoid discovery and get maximum benefit from their knowledge of a vulnerability.

Digital sabotage adversely affects system availability and seems primarily intended to influence decision-making in the affected country at times of conflict or crisis.[137] Threatening to digitally bring a country's critical processes to a standstill, or actually doing so, can give a state actor power over another state. Whether or not this threat manifests itself depends on geopolitical conflicts, since tensions between powers can be followed up in the digital domain.

Threat posed by system failures remains relevant

System failures categorised as non-malicious threats have a potentially significant impact on society. The increasing connectivity and complexity of digital services, processes and systems mean it is likely that the Netherlands will experience system failures more frequently. In the review, several examples of malfunctions are given to illustrate chain dependency in ICT networks.[138]

Speed with which vulnerabilities are misused increases threat

It is clear from the review that criminal and state actors misuse vulnerabilities. They are capable of fast and large-scale strikes when an exploit becomes available.[139] Their intention and capacity to react fast to vulnerabilities increase the threat.

Loss of integrity of digital services, processes and systems: scope and consequences unclear

The scope of intentional or unintentional loss of integrity of digital services, processes and systems, and the consequences this would have are unclear, but the potential impact of such a loss is thought to be significant.[140] Members of the public, businesses and organisations must be able to rely on this integrity, but the main aim of state and criminal actors' activities is sometimes to damage

the integrity of data or data processing.[141] It is apparent from the review that actors are showing renewed interest in tampering with Domain Name System (DNS) settings. By changing organisations' settings, actors can divert or intercept incoming network and email traffic. Large-scale compromising of DNS servers can have a significant impact on the integrity of internet traffic and damage trust in the digital domain.[142]

The manipulation of information can have major consequences and poses a particular risk in sectors where information is regularly updated, such as the financial sector. Cyber incidents can cause financial data to be destroyed, encrypted or manipulated, while at the same time transactions continue to go ahead in the wider financial system which can no longer be processed correctly. This can jeopardise the stability of the financial system, with potentially serious economic consequences. In this scenario a cyber incident can mean an operational disruption resulting in a crisis with a major impact on society. However, a crisis of this kind does not occur out of nowhere, but is a consequence of a combination of specific factors and a loss of trust in the system.[143]

Threat against primary targets and springboard targets

If the threat were to manifest itself against the digital domain and Dutch critical processes, the impact on national security could be significant. Nevertheless, there are also other sectors, parties and processes that are crucial to the proper functioning of Dutch society. Examples include globally prominent knowledge-intensive businesses (in leading economic sectors), the defence industry, lower tiers of government, semi-public institutions and hospitals.

The threat against these targets exists because actors have the intention and the capacity to carry out cyber attacks and make use of the opportunities available to do so, such as vulnerabilities. The review shows that many types of organisation have been the target of attacks. The focus of state actors' political espionage activities can vary by country and by type of espionage. The leading economic sectors in the Netherlands are an obvious target for economic espionage, while central government is an obvious target for political espionage. Critical processes are a popular target for sabotage by state actors. Financially strong organisations are favoured as targets by cybercriminals.

In addition to the 'primary' targets listed above, attackers also focus their attention on parties that can serve as springboards to other targets.[144] The digital domain, the often global supply chains and concentrations of personal data provide ideal conditions. Possible springboard targets include hardware and software suppliers, critical processes like those at telecom companies, and organisations that gather and process personal data, including medical data or personnel data, on a large scale. When selecting these secondary targets, actors actively look for weak links in supply chains to serve as springboards to attractive or more attractive targets. This means that even apparently unattractive sectors or organisations may be of interest to attackers.

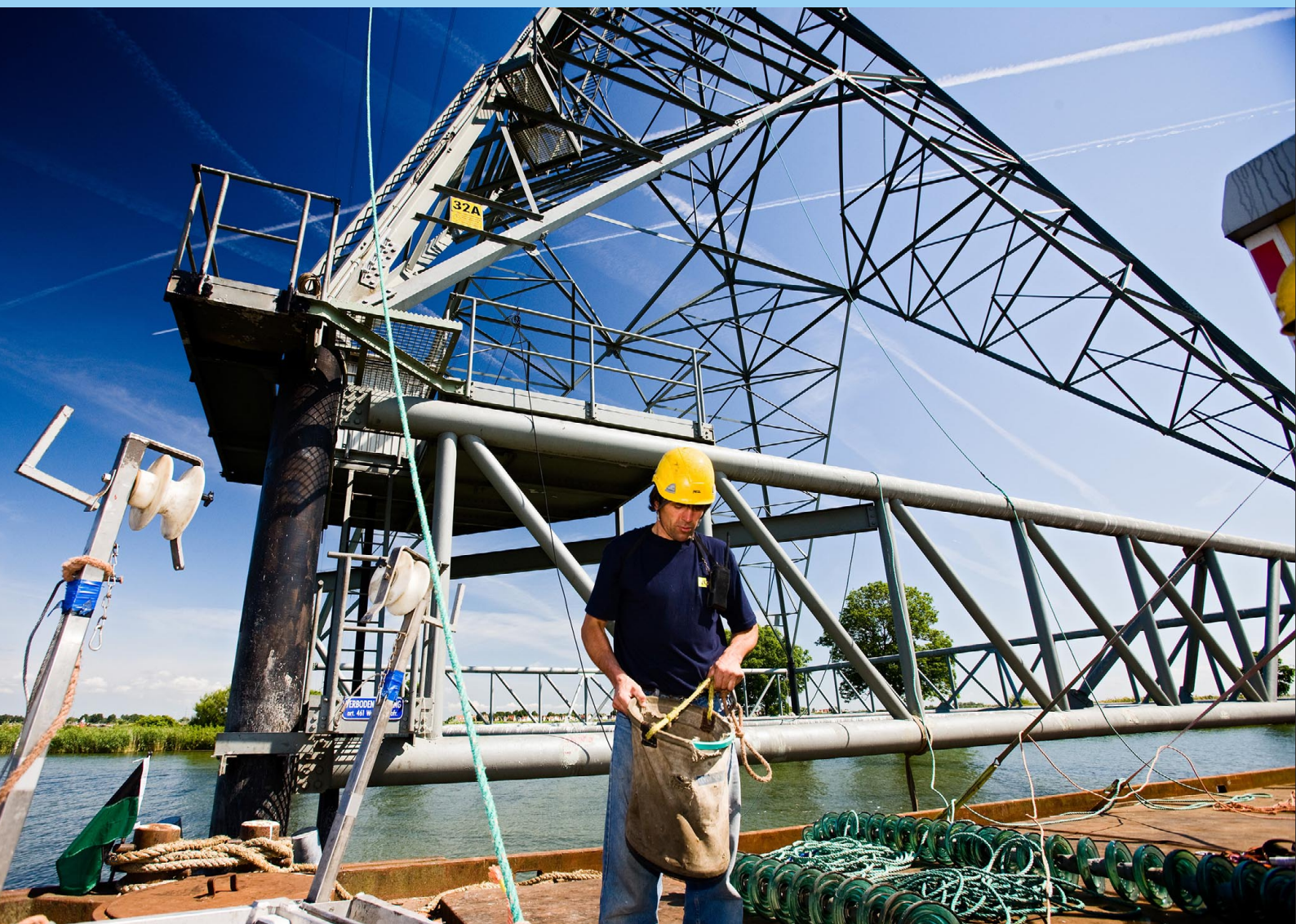
There is also a threat because a system failure at one of these secondary targets, for example due to a technical issue or a failure caused by human error, can have knock-on effects at other organisations.

Dependency on countries with an offensive cyber programme is a risk-enhancing factor

Dependency on ICT products or services from countries found to have an offensive cyber programme targeting the Netherlands is a risk-enhancing factor. In 2019 there were once again concerns about the downside of dependency on a limited number of providers from a limited number of countries. It cannot be assumed that these suppliers take account of Dutch interests.[145] This dependency is a risk factor for digital espionage, sabotage and other threats. Countries use other methods besides cyber attacks in their attempts to achieve their long-term objectives. The deployment of economic means and the creation of strategic and technological dependency are a part of their power politics. If a country achieves dominance in a particular field of technology, it ultimately sets the technological standards for the future. This also increases the dependency of the rest of the world on that country. Foreign investments or takeovers in the Netherlands can also result in full or partial loss of control over critical processes. This jeopardises the continuity of critical processes and creates the risk of knowledge and sensitive or confidential data being leaked. Fragmentation and the dispersal of parts of the production process across national borders can also be a risk factor.[146] Countries can impose requirements on foreign companies and force them to comply with laws on for example supervision or cooperation with the government. The General Intelligence and Security Service (AIVD) therefore considers it undesirable for the Netherlands to be dependent on businesses in countries with offensive cyber programmes that target Dutch interests for critical processes or the exchange of sensitive data.[147]

Back to Table of Contents

Digital security not a given



5 Interests

Digital security is a prerequisite for a functional society. This applies especially to the security of the digital domain and critical processes, where incidents can result in social disruption. There are various reasons that digital security is not a given. Cyber risks are often underestimated. Despite the potentially significant impact of cyber incidents, the risk is hard to get on the agenda. This is not helped by the fact that creating a complete overview of investments in digital security is a complex task.

Digital security is a prerequisite for a functional society

Digital security is inextricably linked to national security. This applies in particular to the global digital domain, which forms the digital foundation of our society, and to critical processes, which are crucial to our society and economy. The digital domain and critical processes are closely linked. Certain critical processes help shape the digital domain, including 'internet and data services'. Others, such as 'national transport and distribution of electricity' help establish the necessary conditions. Critical processes are almost entirely dependent on digital services, processes and underlying systems, and thus on the digital domain.

The digital security of other organisations, services and processes that are crucial to society is also important, as is that of sectors which may seem less relevant to national security (see chapter 4, 'Threat'). There is a risk to the organisations, services and processes themselves, but attackers may also use them as a springboard to other targets. In addition, attacks on seemingly less significant organisations, services and processes may have knock-on effects elsewhere.

Digital security is not a given

Although digital security is inextricably linked to the national security of the Netherlands, it is not a given – neither for the country as a whole, nor for individual parties.

Dutch influence on global digital security is limited

In global terms, many parties play a role in making and keeping the digital domain safe. Obviously, the scope for the Dutch government and other Dutch parties to exercise any influence on this is limited. The digital domain is not confined by national borders. A relatively small group of suppliers of hardware, software, digital services and platforms from a limited number of countries play a crucial role, but they do not have full control over the digital domain. Ultimately, the digital domain and digital security are shaped by many different organisations and countries. However, different countries and businesses have different norms and values when it comes to human rights, privacy and digital security for example. This is evident, for example, from the different statutory requirements they place on businesses. Furthermore, some countries have an offensive cyber programme that targets the Netherlands.

Incentives are not always sufficient to prompt contribution to broader digital security

Without the right incentives, it cannot be assumed that parties will take into account the broader digital security interests of others and of society as a whole when weighing up interests. The possible 'externalities' or 'third party effects' of decision-making are discussed in economic literature in particular. These effects may create perverse incentives and/or undesirable outcomes for society.[148] For example, if a web hosting company were to give relatively little attention to security, its prices would most likely be lower than those of competitors who invest more in security. A customer, for example the owner of an online shop, might draw the same conclusion. The customer may not be aware of the risks or may decide that a cyber incident would cause very little direct harm to their business. In this scenario the adverse effects on others are not taken into account. Externalities can also be

positive. An internet service provider which invests heavily in cybersecurity and actively removes systems that are part of a botnet is contributing not only its own customers' security but also to that of potential victims of the botnet. The provider and its customers cover the costs, while the benefits are also reaped by others.
The government and the national authorities also balance digital security interests against other interests. After all, capacity and funding that is invested in digital security cannot be used elsewhere. Sometimes economic and foreign interests must also be considered.

Weighing up threats, interests and resilience in connection with 5G networks

The question of the relative weight that should be accorded to threats, interests and resilience has been addressed explicitly at national level in connection with the further rollout of 5G networks. The critical parts of telecom providers' networks were identified and the importance of their availability, confidentiality and integrity was determined. An assessment was made of the threat against these networks and the measures already in place. In the final decision the economic importance of 5G and diplomatic relations with other countries were also taken into account. One consequence of the decision is that extra stringent requirements will be put in place for providers of products and services used in critical parts of the telecom network.[149]

Large tech companies do not automatically take into account Dutch interests

The Netherlands is dependent in a broad sense on a relatively small number of suppliers of hardware, software, digital services and platforms, from a limited number of countries. These suppliers do not automatically take the Netherlands' national security into account. Some countries may potentially even be using these companies in their offensive cyber programmes against other countries. In addition, many technology companies gather large amounts of data and offer their products and services worldwide, making them attractive targets for cyber actors. Via these businesses, cyber incidents can cause a global chain reaction.

Payment of ransomware demands: individual versus public interest

An example of a situation in which the interests of an individual organisation clash with the public interest is that in which an organisation pays a ransom in order to regain access to encrypted files following a ransomware attack. It is in the victim's interest to restart their own services and operations as soon as possible. From a public perspective it is important not to sustain a criminal revenue model that will claim new victims. Maastricht University was the victim of a ransomware attack and paid a ransom of €197,000 (30 bitcoins).[150] A study by Sophos claims that one third of targeted companies pay a ransom. Payment can make it easier to restore data and may seem like the cheaper option to the organisation in question. For example, the restoration of encrypted data following a ransomware attack on the American city of Baltimore cost $5.3 million, while the ransom demand was only for $76,000. After payment of a ransom, however, organisations still need to invest in cybersecurity in order to prevent future attacks, meaning the difference in costs is smaller than it seems.[151] Cybersecurity insurance companies are prepared to cover the ransom if an insured party is targeted, sometimes despite it being possible to restore data in other ways.[152] One Dutch insurer, however, maintains that the payment of ransoms is only a fall-back option and that ultimately the organisation itself decides whether or not to pay.[153] The police and the National Cyber Security Centre (NCSC) advise against paying ransoms, because this sustains a criminal revenue model. Police investigations revealed that the money paid is used partly to carry out new attacks.[154] Furthermore, criminals may specifically target businesses with cybersecurity insurance or a strong financial position, as they are more likely to pay. It is also by no means certain that encrypted data will be made available again after payment,[155] as experiences with NotPetya have shown in the past. Files may also have been copied before being encrypted and may be used to continue to extort money from the victim after the ransom is paid.[156]

Cyber incidents can occur on a large scale, simultaneously or consecutively

Cyber incidents can manifest themselves in various ways and may occur in conjunction with incidents of a completely different nature. This is due to the strong – often international – interconnectedness between digital services, processes and systems and the use of generic hardware and software (or hardware and software components). A consequence of this is that cyber incidents can set off an unexpected chain reaction, the effects of which may jeopardise the proper functioning of parts of society.[157] Those effects can be amplified further if trust is undermined, for example through disinformation. Often it is not immediately clear what has caused an incident:[158] human error, for example incorrect routing, a software bug or a cyber attack.

Difficult to gain complete sense of risks to digital domain as a whole and their impact on society

It is difficult to gain a complete sense of the risks of cyber incidents to the digital domain as a whole and of the impact of those risks on society. These risks are known as 'systemic cyber risks'[XII] – as opposed to risks to separate domains and components – and cannot usually be identified until they occur. With this kind of risk a range of factors, connections and dependencies need to be taken into account. Individually or in combination, these can result in a chain reaction with often unexpected and complex consequences.[159] This makes it difficult to assess the risks and to determine whether or not to take measures to manage these risks. In addition, it is not clear in advance what parties have the incentives, capabilities and willingness to limit the risks.

Consequences of disclosure or non-disclosure of vulnerabilities not always entirely apparent

There are advantages and disadvantages to disclosing vulnerabilities. Vulnerabilities – both those that have and those that have not yet been disclosed – can be misused, thus posing a risk to the security of the digital domain. The consequences of disclosure are not always entirely apparent. For most disclosed vulnerabilities a sufficient patch or other mitigating measures already exist, but this is not always the case. Even if patches or measures exist, they are not always implemented immediately; actors, on the other hand, are capable of misusing vulnerabilities very quickly. There are various researchers and businesses who permanently work to detect vulnerabilities in hardware and software. Big companies are prepared to pay large sums of money to find out about previously unknown vulnerabilities. At the start of 2020 the HackerOne bug bounty platform claimed to have a base of 600,000 ethical hackers. Together they earned $40 million worldwide in 12 months.[160] It is now common practice to observe a 90-day waiting period between reporting a vulnerability to a company and disclosing it to the rest of the world. This gives organisations time to develop a patch. However, not every organisation manages to find a solution within that period, for example because this is not seen as a priority. It is also possible that input from other companies is needed find a solution. This may cause information about the vulnerability to be leaked, creating opportunities for misuse, or it may take longer than 90 days for all the organisations involved to be able to introduce a patch at the same time. Finally, organisations may know about vulnerabilities and decide not to share that knowledge unless another party raises the alarm.

The considerations on whether or not to disclose vulnerabilities give rise to various questions with regard to digital security. Can researchers/research groups and organisations sufficiently gauge the consequences of disclosing or not disclosing a vulnerability in a specific case to enable them to properly weigh up the conflicting interests involved? Do they in all cases consider the legal boundaries of coordinated vulnerability disclosure (CVD)? Is it always legitimate to disclose the vulnerability if a business has not made a patch available within 90 days? Is disclosure still desirable in the case of a fundamental vulnerability in millions of devices for which no patch is available? May a business decide itself not to make a patch available on the premise that the impact of any misuse will be minimal or in the hope that the vulnerability in question will not be disclosed?

Cyber risks appear to be underestimated

Despite the serious cyber risks that have been present for many years, cyber resilience is not yet everywhere as it should be. Cyber risks appear to be underestimated.

Cyber incidents: major consequences, but difficult to get on the agenda

In order to take considered decisions, parties must be aware of the cyber risks. The Scientific Council for Government Policy (WRR) notes that the absence of truly disruptive cyber incidents makes it difficult to get this kind of disruption on the agenda, let alone to get across – and bring about broad recognition of – its urgency. However, the WRR believes it is unwise to downplay incidents and dismiss disruptive scenarios as unrealistic.[161] The head of the AIVD points out that people struggle to grasp the invisible threat of, for example, espionage.[162] The Dutch Safety Board (OVV) notes that awareness of the risk of ICT failures in hospitals has not increased at the same rate as the sector's dependency on ICT.[163] Incidents like the ransomware attack on Maastricht University have, however, boosted awareness and may lead similar organisations to take additional measures.[164] Some experts have observed that the WRR report has led to more importance being attached to digital security in the Netherlands.[165]

Incomplete overview of costs and benefits of investing in digital security

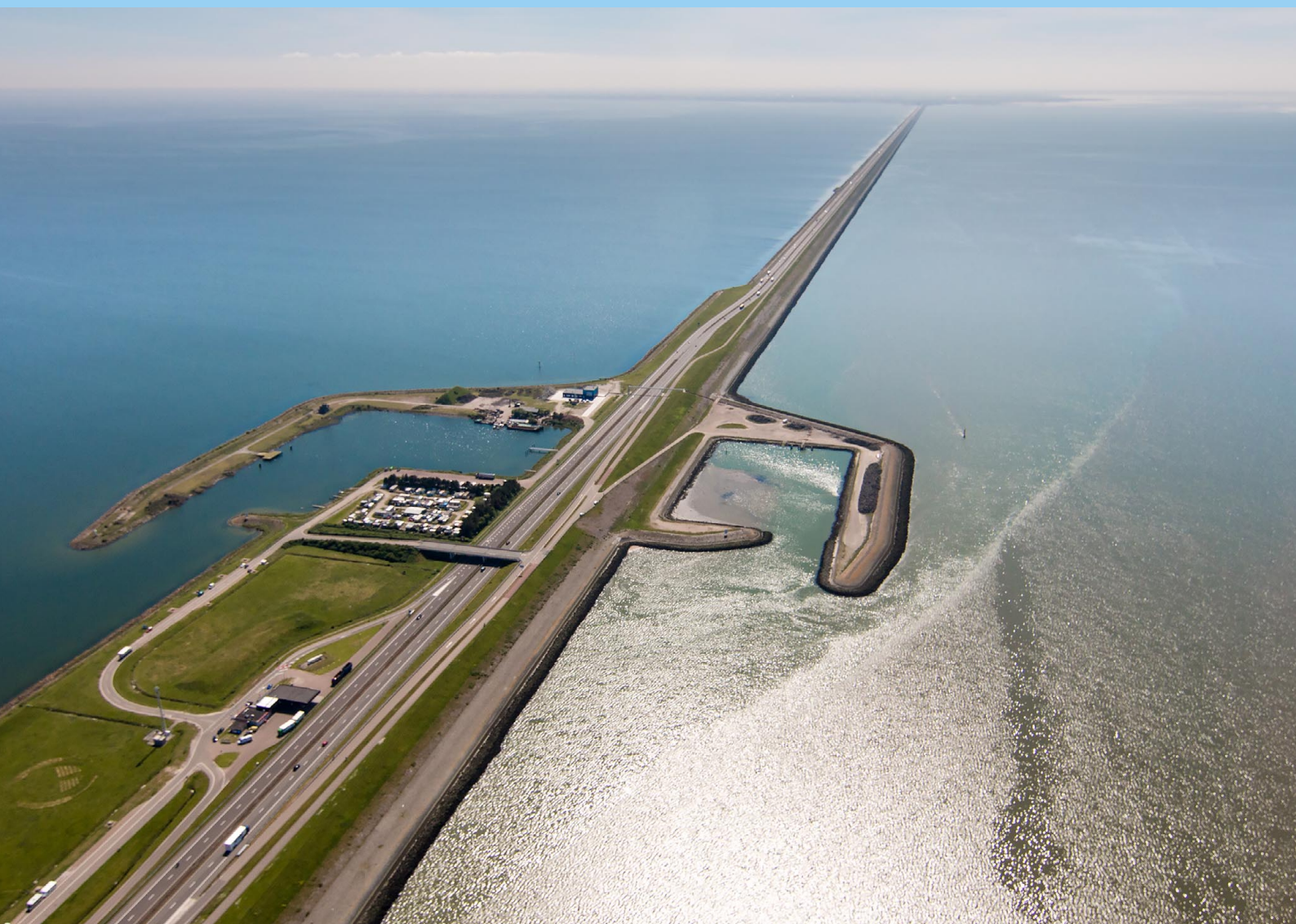
Ideally, decisions should be based at least in part on a complete overview of the risks, capacities and costs of increasing resilience, but this is a complex task. According to the Netherlands Bureau for Economic Policy Analysis (CPB) organisations have an incomplete overview of the costs and benefits[XII] of investments in digital security and face various uncertainties. This can lead to the level of investment being either too high or too low. The first reason for organisations' having an incomplete overview is that the available advice and guidance on the optimum level of investment and on which measures are necessary is inconsistent. The second reason is that information is lacking on the scale of cyber risks and the financial consequences. This is due to: 1) some attacks going unnoticed, 2) organisations not always wanting to reveal that an attack has taken place and 3) organisations sometimes being unable to assess the long-term effects of an attack.[166] The third reason is that some of the adverse effects (the externalities mentioned above) of inadequate cybersecurity are suffered by third parties[167]. In academic literature – particularly economic literature – mention is also made of an 'information problem' with regard to decision-making on cybersecurity.[168]

Back to Table of Contents

XI In the literature, systemic cyber risks are usually linked to the financial system and the financial markets. This focus is partly due to the lessons learned in the financial crisis, which started in the US and spread inexorably across the globe.

XII Benefits in this context should be understood as the positive effects of the measures to increase resilience. The measures are aimed at preventing cyber incidents and, if they do occur, discovering them quickly and ensuring any damage can be mitigated and more easily repaired.

Cyber resilience not yet evident everywhere



6 Resilience

Cyber resilience is not yet evident everywhere and, as a result, certain parties can be particularly vulnerable to cyber incidents. This is especially true when basic measures have not been taken to erect barriers to cyber attacks and to limit damage and facilitate recovery when incidents do occur.

Although basic measures increase organisations' digital resilience, this remains a thorny issue. Digital services and processes are interconnected. Systems consist of a variety of components (both hardware and software), and they are connected to an array of other systems. There are unsafe products and services on the market and users – inadvertently – conduct themselves in an unsafe manner. All this introduces potential sources of technical failure or human error and vulnerabilities which open up opportunities for malicious actors who deliberately misuse the digital domain to carry out attacks.

It is essential to national security that critical processes can function without disruption. There is not yet a complete and clear sense of the degree of cyber resilience of critical processes and associated systems. Supervisory authorities for the providers of critical processes describe a varied picture. Some parties have their digital security sufficiently under control; others do not. According to the Netherlands Court of Audit, information security at the ministries and other central government bodies assessed is still not as it should be.

Lack of resilience due to absence of basic measures

The vast majority of cyber attacks are carried out using simple methods. These methods remain effective because basic measures have not been implemented everywhere. Basic measures can also prevent more sophisticated attacks.

Organisations are not equipped to deal with phishing

It is a complex task for organisations (and individuals) to protect themselves against phishing. In the period under review, phishing was once again the most frequently used method for carrying out an attack or the first step of an attack.[169] However, by implementing basic measures, barriers to cyber attacks can be erected or further damage can be prevented. In order to reduce the effectiveness of phishing, more and more organisations have launched campaigns to make their employees more aware of the risks. The government has also launched an awareness campaign. Research has shown that awareness has increased: in phishing simulations click-through rates have fallen.[170] In 2018 Google reported, that thanks to the use of security keys (physical USB-based devices), none of their 85,000 employees was successfully phished. The security keys meant it was no longer relevant whether or not a user clicked a link.[171] The use of security keys is not (yet) regarded as a basic measure, but shows that it is possible to greatly reduce the success rate of phishing.

Permanent alertness to phishing is vital. People are clicking on dubious links less often, but it still happens and, what is more, attackers are adapting their methods. Phishing is traditionally done via email, but the review shows that cybercriminals also use SMS phishing (smishing). Increasingly, attackers are also successfully gathering sensitive information from social media and using it to target a specific person (spear phishing).[172] This makes the phishing attempt harder for the victim to spot.

Organisations do not always timely protect themselves against vulnerabilities

Organisations do not always manage to install all security updates in time. Research shows that less than half of vulnerabilities are patched within 90 days.[173] Systems sometimes remain vulnerable for years, because security updates have not been installed. Many successful cyber attacks make use of vulnerabilities that have been known and for which a patch has been available for years.[174]

Since organisations are insufficiently protected against vulnerabilities, misuse of known vulnerabilities in hardware and software is still a successful method of attack. It is also a method that is easy to use. A study by IBM showed that the popularity of scanning tools is also growing. Scanning tools allow actors to search for vulnerable systems easily and on a large scale. As soon as a vulnerability is found the system is penetrated and compromised.[175]

Fast detection can limit damage, but response is generally too slow

Early detection of attacks is a basic measure. The sooner attacks are detected, the better. However, for many organisations this remains a complex task. Research shows that in 2019 the average detection time was 56 days.[176] This is in stark contrast to the amount of time an attacker needs to achieve their goal – only a few hours.[177] The review notes that actors exploit vulnerabilities soon after their disclosure.[178] Fast detection can also limit damage in circumstances where the attacker is not relying on quick results, such as espionage.

Lack of measures facilitates successful attacks

The approach of criminal actors is becoming increasingly sophisticated and state actors are deploying their sophisticated attack capacities more widely. Although protection against these methods is more complex, basic measures can still make a difference. Organisations do not always put these basic measures in place, making them extra susceptible. The ransomware attack on Maastricht University is an example of a sophisticated attack where basic measures would probably have reduced the impact. Criminals spent two months exploring the university network and rendering backups unusable before encrypting the files. Various basic measures, such as dealing with reports of phishing correctly, installing security updates, segmenting the network, monitoring and detection, and making offline back-ups, had not been implemented properly.[179] A combination of basic measures, such as network segmentation and good monitoring and detection can also reduce the impact in the event of zero-day vulnerabilities being abused by, for example, state actors.

Basic level of resilience not achieved for various reasons

The experts consulted[XIII] indicated that '[…] many organisations and partners in the supply chain (industries, suppliers) do not meet [the basic level of cybersecurity], or [that] improvements are lagging behind, especially in light of the continually developing threats'. They noted that awareness within organisations has improved and that this has led to more measures being taken. They also noted improvements in terms of investment in cybersecurity at various organisations.[180]

Expert consultation

An expert consultation highlighted various reasons that the basic level of cybersecurity is not met:

- *'Organisations appear to have taken insufficient precautions against known vulnerabilities. [….]*
- *Available security updates are not implemented or are implemented too late. [….]*
- *Errors in I(C)T architecture with a lack of proper zoning, meaning the impact of vulnerabilities is greater than necessary.*
- *Misconfiguration of devices, including IoT devices, ICT systems and cloud services, unintentionally making them accessible to external parties.*
- *Continued use of weak authentication methods.*
- *Lack of in-house knowledge and expertise on information security and the organisation's key systems and processes.*
- *Poor online safety habits and cyber hygiene on the part of employees, as a result of which they are easily manipulated with the help of ever improving social engineering techniques (phishing, misuse of social media), thus making the organisations they work for susceptible.*
- *Idea of cybersecurity measures as a cost rather than a potential business enabler.*
- *Reactive approach to cybersecurity (mainly among smaller organisations) as this seems the most (cost) efficient. Investments in cybersecurity are not made until after a cyber attack or cyber incident occurs. [….]'.* [181]

Digital resilience is a thorny issue

Although basic measures increase organisations' digital resilience, this remains a thorny issue. Digital services, processes and systems are linked to each other and to physical processes, activities and devices. There are unsafe products and services on the market and users – inadvertently– conduct themselves in an unsafe manner. All this introduces potential sources of technical failure or human error and vulnerabilities which open up opportunities for malicious actors who deliberately misuse the digital domain to carry out attacks. This reduces digital security overall, while weak points are difficult for a single party or even a country to exercise any influence over.

Negative effects of interconnectedness, complexity and connectivity

Creating resilient digital infrastructure is a challenge. Digital services and processes are interconnected. Systems consist of a variety of components (both hardware and software), and they are

XIII See chapter 1.

connected to an array of other systems. The review highlights vulnerabilities caused by supply chain dependency and malfunctions with digital and physical knock-on effects. Attackers are well aware of the opportunities for compromising supply chains, generic services, widely used products and more.[182]

Non-secure products and services are the Achilles heel of digital security

Digital products and services that are not secure are still a fundamental cause of cyber incidents. They make it easier for attackers to carry out successful attacks. A lack of security can, for example, be caused by suppliers providing insecure configurations as standard. In 2019 there was an increase in the misuse of poorly configured cloud applications, in the shape of publicly accessibly cloud storage, unsecured databases and unprotected backup servers.[183] A lack of security can also be the result of suppliers failing to make security updates available, security updates being difficult to install or update mechanisms being compromised.

No complete and clear sense of resilience of critical processes (yet)

It is essential to national security that critical processes can function without disruption. A relatively new aspect is the supervision of (primarily) providers of critical processes[XIV] under the Network and Information Systems (Security) Act (WBNI) by supervisory authorities appointed in accordance with that act. The policy response to CSAN 2019 stated that the Security and Justice Inspectorate is responsible, together with other government inspectorates, for providing a coherent assessment of the way these tasks are performed and ensuring that knowledge and expertise are shared between inspectorates.[184] The publication of the first overarching assessment is expected in 2021.

There is not yet a complete and clear sense of the degree of cyber resilience of critical processes and associated systems. Gaining a complete sense of this and of the degree to which measures are effective and efficient, is a complex task. Reliable methods and techniques for measuring resilience in order to assess the risks to national security are still under development. Supervisory activities relating to cybersecurity in the context of the WBNI are relatively new to some supervisory authorities. However, the first effects of better insight among supervisory authorities into digital resilience of providers of critical processes are already becoming visible.[XV]

Supervisory authorities for providers of critical processes describe a varied picture. The resilience of the organisations in question varies. Some parties have things sufficiently under control; others do not. Supervisory authorities have, on the one hand, observed a clear focus on the continuity of processes and systems and the implementation of associated measures. On the other hand, they take the view that there is still a lot to be gained in terms of detection, response and recovery. Not all organisations are giving basic measures with regard to authorisations and security updates the attention they deserve. This signals a lack of maturity when it comes to resilience against cyber threats.

Assessments by the Court of Audit also show that resilience falls short of what is required. In 2019, the Court of Audit revealed shortcomings in the digital protection of key flood defences in the Netherlands.[185] In 2020 the Court of Audit was highly critical with regard to border control, another critical process. The cybersecurity of the Royal Military and Border Police's border control processes at Amsterdam Schiphol Airport was found to be lacking and not future-proof. Security tests on ICT systems are rarely if ever carried out and systems are operational without it having been established that they meet the security requirements. Furthermore, systems are not linked to the detection capacities of a security operations centre, creating the risk that cyber attacks are not detected in time or at all. A successful attack could make carrying out border controls practically impossible, with all the concomitant consequences. The assessment also showed that it was possible, by employing sophisticated means, to manipulate travellers' details. This could allow travellers for whom an alert has been issued to cross the border unnoticed.[186]

Information security at ministries and central government bodies is not as it should be

In May 2020 the Court of Audit noted that ministries and other central government bodies are now more aware of the importance of information security and that efforts have been made in this regard across central government. Information security is as it should be at six of the 16 ministries and bodies assessed[187], up from three the previous year.[188] At nine other ministries and central government bodies this was not yet the case and at one ministry there was one deficiency. The Court of Audit noted that the level of security varies between ministries and pointed out that ministries are dependent on each other when information – confidential or otherwise – is exchanged. This chain is only as strong as its weakest link.[189]

As in previous years, the Court of Audit made a number of critical observations regarding ICT management and maintenance. Management relates to whether systems are working properly and whether the number of malfunctions is low. IT management was found to be lacking. Good management involves ensuring that

XIV The Network and Information Systems (Security) Act (WBNI) distinguishes various categories of provider. Providers of critical processes do not all fall into the same category, but for the sake of convenience they will be referred to here as a single category, namely 'providers of critical processes'.

XV Idem.

only authorised parties can access systems, that users don't have more rights than necessary and that updates are tested before they are rolled out. Maintenance is about ensuring systems are up-to-date and future-proof. The Court of Audit found that at six of the 11 ministries assessed sufficient knowledge is present about the state of the ICT systems, the cost of their continued operation and the size of the risk of malfunctions. Its findings regarding the other ministries were less positive.[190]

Back to Table of Contents

What if your organisation is hit by a ransomware attack?

7 Threat scenarios

The previous chapters address digital threats, digital resilience and the interests that can be in jeopardy when cyber incidents occur. But what does this mean for your organisation?

To help answer this question, this chapter describes three related scenarios. They set out various ways ransomware is used. In 2019, ransomware was frequently employed by various actors. This chapter can help you think about whether the scenarios could occur at your organisation, what precautions have already been taken and what you could do if your organisation ever found itself in a similar situation. Staff members who may have a role to play in the event of a major incident should consider to what extent they are prepared and what they would do if these scenarios became a reality. For further guidance on preparations to limit damage and facilitate recovery, please refer to the National Crisis Plan for Digital Incidents. [191]

This is the first edition of the CSAN to include threat scenarios. These scenarios were developed by the Netherlands Organisation for Applied Scientific Research (TNO) at the request of the National Coordinator for Security and Counterterrorism (NCTV).

Scenario 1a: large-scale ransomware attack via supply chain

Descriptions of events

Via spear phishing, cybercriminals have gained access to Vendorizon's[XVI] customer database. Vendorizon is a global player, selling software packages – including a widely used administrative software package – and management solutions from a range of suppliers to public and private organisations in various sectors. The attackers are in a position to make a malicious security update for the administrative software package available to organisations who have bought this software via Vendorizon. As soon as a user installs the security update, the attackers gain access to their network and ransomware is installed and activated.

Since the update originates from a trusted source and is presented as a patch for a critical vulnerability in the software, many organisations install it immediately. As a result the ransomware spreads in a short space of time to hundreds of organisations in various sectors, including in the Netherlands. Rumours about a major ransomware attack spread quickly via the media. Initially the cause is thought to lie with the software producer. It soon emerges that only organisations that bought the software from Vendorizon have been affected – via the malicious security update. Other Verizon customers put all security updates on hold as a precaution.[XVII] This means that after the first day the ransomware does not spread any further.

Interpretation

Spear phishing remains attractive to cybercriminals as a means to gain access to an organisation's network.[192] Other tools are then used to broaden the scope of the attack.

The review shows that attacks carried out via chain partners pose a significant threat. It is important to note that interdependencies between parties can take various forms. There does not necessarily need to be a direct technical link. Functional dependencies can

XVI Any resemblance to an actual company is purely coincidental and unintended.

XVII In normal circumstances, installing updates as soon as possible increases resilience, but if a supply chain partner has been compromised, this is not always the case.

also provide a way in for malicious actors. A chain partner may have information or access to sensitive information about vulnerabilities at an organisation, for example due to outsourcing.

Cybercriminals are increasingly able to conceal ransomware in seemingly reliable software. In this scenario the attackers use trusted channels, making their attack even harder to detect than via phishing or spear phishing.

This scenario also shows that it is necessary to balance the importance of installing patches as soon as possible to safeguard the system's digital security against the impact malicious patches can have on continuity of operations. An organisation may – sensibly – decide to install a security update from a trusted partner as soon as possible and still run into difficulties if it turns out the partner has been compromised. This highlights the importance of exchanging information (e.g. indicators of compromise (IoCs)[193] with partners in the supply chain.

Key questions for the reader

1. Do you have a good overview of the hardware and software your organisation uses and do your suppliers provide the latest information about vulnerabilities and updates?
2. What agreements have been made with partners in your supply chain about exchanging relevant cybersecurity information (such as IoCs), technical details and incident response information?[194]
3. Has your organisation considered the possible risks it faces as a result of interactions with clients, suppliers and other service providers, and taken measures to mitigate the risks created by these interdependencies?
4. Does your organisation have existing contacts within relevant government organisations, including the police, where it could report a cyber incident, ask for assistance and/or lodge a criminal complaint if a cyber incident were to occur

Scenario 1b: the importance of basic measures in limiting the impact of ransomware attacks

Description of events

A large number of organisations have been hit by a ransomware attack carried out via a malicious security update for an administrative software package. It is unclear how many organisations have been affected, because, while some organisations have been open and transparent about the attack, others have been less forthcoming. It follows that there may also be organisations that have been affected but have chosen not to publicise this at all.

From the information provided by organisations that have been open, it is clear that the attackers are demanding substantial ransom payments in exchange for access to files. A few of the organisations are able to recover their systems themselves, by using their backups. Others call in the help of an external party to manually reinstall and reconfigure all the affected devices from the backup. This can take anything from a few days to two weeks, depending on the organisation. However, there are a considerable number of organisations who do not have a backup or whose backup is unusable because it is connected to a compromised part of the network. They see no option but to pay the ransom since the alternative is to accept the loss of all the affected data.

Some of the organisations affected have cybersecurity insurance and submit a claim. There are also rumours circulating on social media that, despite having a backup, some organisations are planning to pay the ransom because they have concluded that this is more cost efficient. After all, for many organisations reinstalling computers and clearing systems is a major, and therefore costly, operation. Organisations that pay the ransom are heavily criticised in public discussions of the incident. A heated debate ensues on the options for fining organisations that pay the ransom, given the increased risk of ransomware attacks.

Interpretation

The review discusses ransomware attacks.[195] The acceptability of paying ransom is a question that arises in this connection. It is often pointed out that this involves balancing, on the one hand, the organisation's interest in continuing its operations and, on the other hand, society's interest in undermining the business model for this type of crime. In practice, many organisations have no real choice, because if they do not have a backup or their backups have also been affected, paying the ransom is the only way to recover their files. This shows once again how important it is to have basic measures in place. What can be done to ensure organisations have realistic options to consider?

Another aspect that is highlighted in this scenario is the degree of openness about this kind of attack and its effect on the organisation in question. Although openness about a successful cyber attack can initially damage an organisation's reputation, daring to be vulnerable and transparent and thus allowing other parties to benefit from the lessons learned can earn public plaudits.

A further aspect is whether or not to lodge a criminal complaint with the police. This can lead to the perpetrators being tracked down and held responsible for the crimes, and prevent them from claiming more victims.

Key questions for the reader

1. Does your organisation have a procedure in place for making backups? And does it regularly test whether these backups work?
2. Has your organisation taken other measures, such as compartmentalising networks, to stop malware spreading as easily?
3. If your organisation were to be affected by ransomware, would you know what to do?
4. In the event of a successful attack, would your organisation share and/or publicise information about the attack and the lessons learned and/or lodge a criminal complaint? If so, why? If not, why not?

Scenario 1c: problem solved! Or not...?

Description of events

A few months after high tech company zMART-Veder[XVIII] was hit by ransomware, the business is once again in the news following a cyber attack. Under pressure from several anonymous messages on social media (claiming that innovative technology has been stolen) zMART-Veder reports a data breach relating to a large amount of confidential commercial information on innovative technologies. The company's stock price plummets. A digital forensics company is brought in and announces that there are indications that the data breach can be linked to an advanced persistent threat (APT) group affiliated to a state actor in Asia. The forensics company suspects that a group of professional cybercriminals, specialised in obtaining access via phishing attacks, has sold its access to several organisations' systems to this state actor. This took place at the same period as the ransomware attack.[196]

Also in the same period, traces of preparations for a cyber attack were discovered in energy supplier Current Streams'[XIX] IT network. If carried out, the attacks could lead to large-scale disruption to the supply of energy by the company. Current Streams was among the organisations whose systems were hit by ransomware several months ago. The effects of the ransomware attack were limited to its office software. The traces that have now been found show that the attackers also gained access to the company's operational technology. They display characteristics of the modi operandi used by an APT group known for its sabotage (disrupting critical infrastructure) and manipulation (influencing democratic processes) activities. This APT group is closely affiliated to a country in the Middle East that has been in the news a lot in the past year in connection with various geopolitical disputes with the United States and the European Union.

Interpretation

Once organisations have recovered following a ransomware attack and the dust seems to have settled, it is understandable that they feel like the attack is over. This applies particularly if an organisation was one of a large number to be hit by the same ransomware as this creates the impression that they were not targeted specifically but were merely unlucky. Cybercriminals are increasingly specialising in certain parts of an attack, in order to improve their business model. In the example in this scenario a group has gained access to the victims' operational networks via sophisticated ransomware. As a result, they are able to not only encrypt files, but also obtain login details and possibly other valuable information. This allows them to make more money – in addition to demanding a ransom – by selling this data to other actors (an APT group in this scenario).

The line between criminal and state activities appears to be blurring and, as a result, attacks consisting of several, sometimes coordinated, steps are occurring more frequently. So it is important to remain alert, even after an attack seems to be over. What else has been done to the systems? Has confidential information been copied? Have criminals found other ways to make money out of the attack, for example by selling their access to another malicious party? Did other parties embed themselves in the system some time ago?

Key questions for the reader

1. Why might a state actor be interested in your organisation? Could your organisation be an attractive springboard, for example to one of your customers or another party in your supply chain?
2. What measures has your organisation put in place to monitor ICT infrastructure and detect suspicious activity?
3. What information held by your organisation do you regard as your 'crown jewels'? What additional protection measures are in place to stop this information being compromised?
4. Have your organisation's cybersecurity professionals been trained to recognise possibly complex cyber attacks?

Back to Table of Contents

XVIII Any resemblance to an actual company is purely coincidental and unintended.

XIX Any resemblance to an actual company is purely coincidental and unintended.

Appendices

Appendix 1
Abbreviations and glossary

Actor	An individual or group of individuals who carry out or intend to carry out a cyber attack. Examples include a) states/state-related actors, b) criminals, c) terrorists, d) hacktivists, e) cyber vandals and script kiddies, and f) insiders.
AIVD	General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*).
AP	Dutch Data Protection Authority (*Autoriteit Persoonsgevens*)
Attack	See 'cyber attack'.
Authentication	Establishing the identity of a user, computer or application.
Availability	The certainty that users can access data or a digital system or use digital services or processes whenever they wish or are supposed to be able to. Planned system maintenance is not relevant in this regard.
Basic measures	Activities aimed at achieving the minimum physical, procedural, behavioural and technical guarantees necessary to ensure that cyber incidents can be prevented and that, when they do occur, they can be discovered and the damage can be mitigated and more easily repaired. Another term for this is 'cyber hygiene'. An example of a basic measure is making online and offline back-ups.
Bitcoin	A type of digital currency. See 'cryptocurrency'.
Botnet	A collection of infected systems that can be controlled remotely from a central location. Botnets provide the infrastructure for many forms of internet crime.
Cloud service	ICT infrastructure provided as a service online.
Confidentiality	The certainty that data and/or digital services, processes or systems are only accessible to authorised persons or software.
Criminal/Criminal actor	Actor who carries out attacks for economic or financial gain.
Critical processes	Processes that are so essential to Dutch society that their failure or disruption would lead to serious social disruption and pose a threat to national security. These processes constitute the critical infrastructure in the Netherlands. Examples of critical processes include the availability of electricity, internet access, drinking water and financial transactions. In the Netherlands 28 processes have been formally designated as critical.[197]
Cryptocurrency	Umbrella term for digital currencies that use cryptographic calculations as an authenticity feature and for transactions.

CVD	Coordinated vulnerability disclosure. The practice of coordinating reports of discovered security leaks. Agreements are made for this purpose, usually to the effect that the notifying party will not share the discovery with third parties until the leak has been repaired, and that the affected party will not take legal action against the notifying party. This was previously known as 'responsible disclosure'.
Cyber	Relating to digital information and systems connected to internet.
Cyber attack	Malicious act by a cyber actor aimed at using digital resources to adversely affect the availability, integrity or confidentiality of information systems and process control systems, the data processed and stored thereon and the services and processes dependent on them.
Cybercrime	A distinction can be made between cybercrime in a narrow sense (computer-focused crime) and cybercrime in a broad sense (computer-assisted crime and computer-enabled crime). • Computer-focused crime: attacks targeting ICT systems carried out using ICT resources. For example: hacking, DDoS attacks and ransomware. • Computer-assisted crime: Crime that was previously committed via analogue means, but is now committed mostly via digital means. For example: CEO fraud. • Computer-enabled crime: analogue crime that can only occur in the physical world, but of which elements of the modus operandi are ICT-supported. For example, drugs can be trafficked online, but they can only be smuggled or consumed in the physical world. Increasingly, all forms of crime are becoming computer-enabled to some extent. All types of cybercrime can be sophisticated or less sophisticated in nature. The CSAN addresses only *computer-focused* cybercrime.
Cybercrime-as-a-service	The online provision of extensive cybercrime services, whereby almost every step related to committing and concealing cybercrime can be bought or sold. The CSAN focuses on the provision of services relating to cyber attacks.
Cyber incident	All events or activities that adversely affect the availability, integrity or confidentiality of information systems and process control systems, the data processed and stored thereon, and the services and processes dependent on them. Umbrella term for cyber attacks and system failures.
Cyber risk (risk of cyber incidents)	The chance that a cyber incident could occur and the impact it would have, in light of the current level of cyber resilience.
Cybersecurity	The full spectrum of measures designed to prevent damage through the disruption, failure or misuse of ICT systems and to repair such damage when it does occur. This damage may consist of adverse effects on the availability, integrity or confidentiality of information systems and information services, and the data stored thereon.
Cyberspace	See 'digital domain'.
Cyber vandal	See 'script kiddie'.
Data manipulation	Intentional alteration of data; violation of data integrity.
Data theft	Loss of data confidentiality through the copying or removal of data.
DDoS	Distributed Denial of Service. A type of attack in which a specific service (e.g a website) is made unavailable by overwhelming it with an excessive amount of network traffic from a large number of different sources.
Digital attack	See 'cyber attack'.

Digital domain	A complex environment resulting from the interaction of people, software and services on the internet, supported by worldwide distributed physical information and communications technology devices and connected networks.[XX] The terms 'digital space' and 'cyberspace' are also used.
Digital security	The ability of information systems and process control systems, the data processed and stored thereon and the services and products dependent on them to function smoothly. The CSAN's focus is on digital security in the digital domain, critical processes and other sectors, digital services and processes that are crucial to the smooth functioning of (Dutch) society.
Digital space	See 'digital domain'.
DNS	Domain Name System. The system that links internet domain names to IP addresses and vice versa. For example, the web address www.ncsc.nl is linked to the IP address 159.46.193.36. A DNS record also specifies how emails to the domain should be handled.
DoS	Denial of service. An attack which makes a particular service (e.g. a website) unavailable to its normal users. When a DoS attack is carried out on a website, it usually takes the form of a DDoS attack.
Encryption	The process of putting information into code, rendering it inaccessible to unauthorised parties.
Espionage	Loss of data confidentiality through the copying or removal of data.
Exploit	Software, data or a sequence of commands that takes advantage of a vulnerability in software or hardware in order to cause unintended behaviour.
Exploit kit	Tool that enables its user to launch an attack by selecting ready-made exploits and the desired consequences and infection method.
Hacker/hacking	The most commonly used definition of hacker, and the one used in this document, is: an individual who attempts to break into ICT systems with malicious intent. Originally, the term was used to refer to an individual who used technology (including software) in an unconventional manner, usually in order to circumvent limitations or achieve unanticipated effects.
Hacktivist	Portmanteau word combining 'hacker' and 'activist'. An ideologically motivated actor who carries out digital attacks of an activist nature.
ICS	Industrial control systems. See 'process control systems'.
Impact	The damage to interests when a cyber incident occurs. The CSAN focuses on the impact on national security in general and specifically on the impact on the digital domain, critical processes and other digital services and processes that are crucial to the smooth functioning of (Dutch) society.
Incident	See 'cyber incident'.
Industrial control systems	See 'process control systems'.
Insider	An internal actor with inside access to systems or networks who poses a threat and is motivated by revenge, monetary gain or ideology. An insider may also be engaged or instructed by someone outside the organisation.

XX Definition of 'cyberspace' given in ISO/IEC standard 27032:2012 (E).

Integrity	1. Of data: the accuracy and completeness of data and data processing. 2. Of persons: their trustworthiness. 3. Of digital services, processes or systems: their proper functioning.
Interests	Values, social gains, and tangible and intangible assets that may be damaged if a cyber incident occurs, and the importance that society or a party attaches to protecting them. The CSAN focuses on national security interests.
IoT	Internet of Things. A network of smart devices, sensors and other objects, often connected to the internet, that gather data about their surroundings, exchange that data and, on the basis of that data, take autonomous or semi-autonomous decisions or actions that affect their surroundings.
IP	Internal Protocol. Set of rules that assigns addresses to internet traffic so as to ensure it reaches its intended destination.
Leak	Loss of confidentiality resulting from natural, technical or human failure.
Malfunction	See 'system failure'.
Malware	Contraction of the words 'malicious software'. 'Malware' is a generic term for viruses, worms, trojans and more.
MIVD	Netherlands Defence Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*).
MO	See 'modus operandi'.
Modus operandi	The method an actor uses or can use to carry out a cyber attack. Examples include combining tools to carry out an attack and deploying tools either indiscriminately (scatter-shot MO) or in a targeted manner. The focus here is on the actor's method. The term tool relates to the tool/toolbox itself.
National security	National security is at stake when one or more national security interests are seriously threatened. National security relates to all intentional and unintentional risks and threats which could cause social disruption in the Netherlands, from floods to terrorism and from a pandemic to a cyber attack.
National security interests	The six national security interests are: • Territorial security: the ability of the Netherlands and its EU and NATO allies to function without disruption as independent states in a broad sense; or territorial integrity in a narrow sense. • Physical security: the ability of people in the Netherlands and their surroundings to go about their business without disruption. • Economic security: the Netherlands' ability to function without disruption as an effective and efficient economy. • Ecological security: the continued existence of the natural environment in and around the Netherlands. • Social and political stability: the continued existence of a social climate in which individuals can live their lives without disruption and groups of people can live together successfully, without disruption, within the framework of democracy, the rule of law and shared values. • International legal order: the proper functioning of the international system of norms and agreements aimed at promoting international peace and security.
Party	Umbrella term for an organisation, business, government body or member of the public.
Phishing	Umbrella term for digital activities aimed at tricking people into revealing personal details. This data can be misused to gain access to systems.

Process control system	General terms for various types of system that manage physical processes, such SCADA, DCSs and PLCs. These systems can open and close sluices or turn wind turbines on and off, for instance. Process control systems are also known as industrial control systems.
Ransomware	Type of malware that blocks systems or the data on those systems and only grants access again once a ransom payment is made.
Resilience	The ability to prevent cyber incidents and, when cyber incidents do occur, to discover them, mitigate the damage and repair the damage more easily. This can be done with the help of technical, procedural or organisational measures. Other ways of increasing resilience are through legislation, grant policy, training (to inform users about online safety), information campaigns, partnerships between various parties, and agreed standards for the digitalisation of services and processes and for system design.
Sabotage	Intentional, long-term interference with the availability of – or, in extreme cases, destruction of – digital services, processes or systems.
Script kiddie	Actor with limited knowledge who uses tools designed and developed by others to carry out cyber attacks, uncover vulnerabilities or test themselves.
Social disruption	Disruptive effects on society that may occur if one or more of the six national security interests are jeopardised. (See also 'national security interests').
Spam	Unwanted email, usually of a commercial nature.
Spear phishing	A variant of phishing whereby one person or a limited group of people are targeted after being selected based on their level of access. The aim of spear phishing is to achieve the best possible result without attracting too much attention.
State actor	States that carry out cyber attacks on other countries, organisations or individuals do so with primarily geopolitical motives. Their objectives are to acquire strategic information (espionage), influence public opinion or democratic processes (manipulation) or disrupt or even destroy critical systems (disruption and sabotage).
State-affiliated actor	Actor affiliated to a state actor.
Supply chain	An ecosystem of service providers who supply hardware, software, networks or services which are used by other parties for their own networks and/or service provision. This includes cloud providers for instance.
System failure	A situation in which the availability or integrity of information systems and process control systems, the data processed and stored thereon and the services and products dependent on them is adversely affected, regardless of the cause. This term does not cover cyber attacks. The CSAN's focus is on failures that could cause a chain reaction within the digital domain, critical processes and other processes that are crucial to the smooth functioning of (Dutch) society.
System manipulation	Undermining the integrity of digital services, processes or systems.
Target	The digital service, organisation, process or system on which an actor carries out a cyber attack.
Terrorist	Ideologically motivated actor who attempts to achieve social change, instil fear into certain population groups, or influence political decision-making, by using violence against people or causing disruptive damage.

Threat	A cyber incident or a combination of simultaneous or consecutive cyber incidents that could potentially occur. In the CSAN the focus is primarily on threats that may damage national security interests.
Tool	The software, hardware and method(s) of attack that an actor uses or can use to carry out a cyber attack. Examples include ransomware and DDoS attacks. The focus here is on the tool/toolbox itself. The term modus operandi relates to the actor's use of the tools.
Two-factor authentication	A method of establishing someone's identity, which requires two independent forms of proof of identity.
Vulnerability	A characteristic that enables an attacker to carry out a cyber attack or that can lead to a failure. This may be a characteristic of a digital service, process or system, of a specific organisation, or indeed of society as a whole.
Zero-day vulnerability	A vulnerability for which a patch is not yet available, because the developer of the vulnerable software has had no time (i.e. zero days) to repair the vulnerability.

Back to Table of Contents

Appendix 2 Sources and references

1 'Cyber Security Assessment Netherlands 2019', NCTV, 12-06-2019.
2 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID: De Militaire Inlichtingen- en Veiligheidsdienst beschermt wat ons dierbaar is', MIVD 2019 Public Annual Report, April 2020.
3 AIVD 2019 Annual Report, April 2020.
4 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020.
5 AIVD 2019 Annual Report, April 2020.
6 AIVD 2019 Annual Report, April 2020, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2020/04/29/jaarverslag-2019/Jaarverslag+2019+webversie.pdf; 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020.
7 AIVD 2019 Annual Report, April 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020.
8 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020.
9 AIVD 2019 Annual Report, April 2020.
10 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020.
11 2019 Annual Report, Dutch Police, 13-1-2020.
12 'A Guide to LockerGoga, the Ransomware Crippling Industrial Firms', *Wired*, 25-03-2019, https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/, consulted on 16-01-2020.
13 'Threat Research. APT41: A Dual Espionage and Cyber Crime Operation', FireEye, 07-08-2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html.
14 2019 Annual Report, Dutch Police, 13-01-2020; 'Results of online expert consultation for CSAN 2020', TNO, 15-01-2020; 'Internet Organised Crime Threat Assessment' (IOCTA) 2019, Europol, 09-10-2019, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019; *NCSC Magazine*, issue no. 1, NCSC, 01-12-2019, https://magazines.ncsc.nl/ncscmagazine/2019/01; 'Targeted Ransomware: Proliferating Menace Threatens Organizations', Symantec, 18-07-2019, https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat.
15 2019 Annual Report, Dutch Police, 13-01-2020; 'Travelex being held to ransom by hackers', BBC, 7-1-2020, https://www.bbc.com/news/business-51017852.
16 'Maze Ransomware Gang Dumps Purported Victim List', Bank Infosecurity, 17-12-2019, https://www.bankinfosecurity.com/blogs/maze-ransomware-gang-dumps-purported-victim-list-p-2839, consulted on 22-01-2020; 'Allied Universal Breached by Maze Ransomware, Stolen Data Leaked', Bleeping Computer, 21-11-2019, https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked, consulted on 22-01-2020; 'Ransomware Hackers Have Started Leaking City Of Pensacola Data', *Forbes*, 31-12-2019, https://www.forbes.com/sites/leemathews/2020/12/31/ransomware-hackers-have-started-leaking-city-of-pensacola-data/#14b3872f994b, consulted on 22-01-2020; 'Nemty Ransomware to Start Leaking Non-Paying Victim's Data', Bleeping Computer, 13-01-2010, https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data, consulted on 22-01-2020; 'Sodinokibi Ransomware Publishes Stolen Data for the First Time', Bleeping Computer, 11-01-2020, https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-publishes-stolen-data-for-the-first-time, consulted on 16-01-2020.
17 'Mysterious New Ransomware Targets Industrial Control Systems', *Wired*, 03-02-2020, https://www.wired.com/story/ekans-ransomware-industrial-control-systems; 'EKANS Ransomware and ICS Operations', Dragos, 03-02-2020, https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations.

18 'Hydro subject to cyber attack', Hydro, 19-03-2019, https://www.hydro.com/en-NL/media/news/2019/hydro-subject-to-cyber-attack, consulted on 02-01-2020.
19 'Big Norwegian Aluminum Producer Suffers Extensive Cyber Attack', Bloomberg, 19-03-2019, https://www.bloomberg.com/news/articles/2019-03-19/hydro-says-victim-of-extensive-cyber-attack-impacting-operations-jtfgz6td, consulted on 02-01-2020.
20 'Third quarter 2019: Ramping up production in Brazil, declining market prices', Hydro, 23-10-2019, https://www.hydro.com/en-DE/media/news/2019/third-quarter-2019-ramping-up-production-in-brazil-declining-market-prices, consulted on 02-01-2020.
21 Annual report 2019, Dutch Police, 13-01-2020; 'Ryuk ransomware targeting organisations globally', NCSC-UK, 21-06-2019, https://www.ncsc.gov.uk/news/ryuk-advisory, consulted on 17-01-2020; 'Severe Ransomware Attacks Against Swiss SMEs', GovCERT.ch, 09-05-2019, https://www.govcert.ch/blog/36/severe-ransomware-attacks-against-swiss-smes, consulted on 17-01-2020; 'BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen', BSI, 24-04-2019, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/BSI_warnt_vor_Ransomware-Angriffen-240419.html, consulted on 17-01-2020.
22 2019 Annual Report, Dutch Police, 13-01-2020.
23 'A One-Two Punch of Emotet, TrickBot, & Ryuk Stealing & Ransoming Data', Cybereason, 02-04-2019, https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data, consulted on 27-01-2020.
24 'UM Cyber Attack Symposium – Lessons learnt', Maastricht University, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt, consulted on 12-02-2020; 'Servers Universiteit Maastricht misten belangrijke update uit 2017', Security.nl, 06-02-2020, https://www.security.nl/posting/642659/Servers+Universiteit+Maastricht+misten+belangrijke+update+uit+2017.
25 'UM Cyber Attack Symposium – Lessons learnt', Maastricht University, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt, consulted on 12-02-2020; Letter to parliament on cybersecurity in education, Ministry of Education, Culture and Science, 14-02-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.
26 Letter to parliament on cybersecurity in education, Ministry of Education, Culture and Science, 14-02-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.
27 'Cyber Security Assessment Netherlands 2019', NCTV, 12-06-2019.
28 'IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit', IBM, 26-02-2019, https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Cryptojacking-for-Profit, consulted on 17-01-2020.
29 'Hack at all cost: putting a price on APT attacks', Positive Technologies, 14-08-2019, https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report, consulted on 27-01-2020.
30 'Identifying Cobalt Strike team servers in the wild', Fox-IT, 26-02-2019, https://blog.fox-it.com/2019/02/26/identifying-cobalt-strike-team-servers-in-the-wild, consulted on 28-01-2020.
31 '8 Legit Tools and Utilities That Cybercriminals Commonly Misuse', Dark Reading, 18-07-2019, https://www.darkreading.com/attacks-breaches/8-legit-tools-and-utilities-that-cybercriminals-commonly-misuse/d/d-id/1335254, consulted on 27-01-2020; AIVD 2018 Annual Report, April 2019.
32 'RDP-aanval kostte gemeente Lochem zo'n 200.000 euro', Security.nl, 26-09-2019, https://www.security.nl/posting/625572/RDP-aanval+kostte+gemeente+Lochem+zo%27n+200_000+euro, consulted on 10-01-2020; 'Lochem legt computers dag plat na hack', Lochems Nieuws, 12-06-2019, https://www.lochemsnieuws.nl/2019/06/12/lochem-legt-computers-dag-plat-na-hack, consulted on 28-01-2020.
33 'A Chinese APT is now going after Pulse Secure and Fortinet VPN servers', ethhack, 05-09-2019, https://ethhack.com/2019/09/a-chinese-apt-is-now-going-after-pulse-secure-and-fortinet-vpn-servers, consulted on 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a consulted on 17-02-2020; 'VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers', ZDNet, 06-01-2020, https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers, consulted on 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a, consulted on 17-02-2020; 'Cybercriminals are Focusing on Vulnerable Edge Services', Fortinet, 19-11-2020, https://www.fortinet.com/blog/industry-

trends/cybercriminals-target-entire-digital-footprint.html, consulted on 17-02-2020; 'Criminelen verspreiden ransomware via Citrix-kwetsbaarheid', Security.nl, 24-1-2020, https://www.security.nl/posting/640914/Criminelen+verspreiden+ransomware+via+Citrix-kwetsbaarheid.

34 'Analyse van de gelopen risico's door de kwetsbaarheden in de virtual private network (VPN) software van het bedrijf Pulse Secure', House of Representatives, 11-02-2020, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z02670&did=2020D05619

35 'Na de hack zou de Citrix-crisis aan Lochem voorbij gaan. Fout gedacht', NRC, 22-01-2020, https://www.nrc.nl/nieuws/2020/01/22/na-de-hack-zou-de-citrix-crisis-lochem-nu-niet-raken-fout-gedacht-a3987772, consulted on 20-02-2020.

36 Information from the AIVD and MIVD.

37 'Criminelen verspreiden ransomware via Citrix-kwetsbaarheid', Security.nl, 24-1-2020, https://www.security.nl/posting/640914/Criminelen+verspreiden+ransomware+via+Citrix-kwetsbaarheid.

38 'Microsoft is Alerting Hospitals Vulnerable to Ransomware Attacks', Bleeping Computer, 01-04-2020, https://www.bleepingcomputer.com/news/security/microsoft-is-alerting-hospitals-vulnerable-to-ransomware-attacks, consulted on 29-04-2020; 'FBI: groot aantal ziekenhuizen besmet met malware', Security.nl, 31-03-2020, https://www.security.nl/posting/650102/FBI%3A+groot+aantal+ziekenhuizen+besmet+met+malware, consulted on 29-04-2020; 'Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic', Bleeping Computer, 26-03-2020, https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic, consulted on 29-04-2020; 'Overheid waarschuwt ziekenhuizen voor cyberaanval', *De Tijd*, 25-03-2020, https://www.tijd.be/ondernemen/algemeen/Overheid-waarschuwt-ziekenhuizen-voor-cyberaanval/10216656, consulted on 29-04-2020; 'En pleine crise du coronavirus, les hôpitaux de Paris victimes d'une cyberattaque', *L'Express*, 23-03-2020, https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html, consulted on 29-04-2020; 'Hackers linked to Iran target WHO staff emails during coronavirus', Reuters, 02-04-2020, https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC, consulted on 29-04-2020.

39 'WHO Chief Impersonated in Phishing to Deliver HawkEye Malware', Bleeping Computer, 19-03-2020, https://www.bleepingcomputer.com/news/security/who-chief-impersonated-in-phishing-to-deliver-hawkeye-malware, consulted on 29-04-2020; 'Netwalker Ransomware Infecting Users via Coronavirus Phishing', Bleeping Computer, 21-03-2020, https://www.bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing, consulted on 29-04-2020; 'HHS.gov Open Redirect Used by Coronavirus Phishing to Spread Malware', Bleeping Computer, 23-03-2020, https://www.bleepingcomputer.com/news/security/hhsgov-open-redirect-used-by-coronavirus-phishing-to-spread-malware, consulted on 29-04-2020.

40 'Klanten Rabobank weer doelwit van phishingmail over corona', Security.nl, 26-03-2020, https://www.security.nl/posting/649516/Klanten+Rabobank+weer+doelwit+van+phishingmail+over+corona, consulted on 29-04-2020.

41 'Hackers are messing with routers' DNS settings as telework surges around the world', Cyberscoop, 25-03-2020, https://www.cyberscoop.com/dns-hijacking-covid-19-oski-bitdefender-telework, consulted on 29-04-2020; 'Hackers Hijack Routers' DNS to Spread Malicious COVID-19 Apps', Bleeping Computer, 23-03-2020, https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps, consulted on 29-04-2020; 'Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book', MalwareBytes, 18-03-2020, https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book, consulted on 29-04-2020; 'Security researcher Marco Ramilli analyzed a new Coronavirus (COVID-19)-themed attack gathering evidence of the alleged involvement of an APT group', Security Affairs, 19-03-2020, https://securityaffairs.co/wordpress/99977/apt/apt27-abusing-covid-19.html, consulted on 29-04-2020.

42 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen, consulted on 17-01-2020; 'DNS Attacks Grow More Frequent and Costly', *Infosecurity Magazine*, 18-06-2019, https://www.infosecurity-magazine.com/news/dns-attacks-grow-more-frequent, consulted on 17-01-2020; 'Worst DNS attacks and how to mitigate them', Network World, 18-07-2019, https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html consulted on 17-01-2020; 'Ongoing DNS hijacking and mitigation advice', NCSC-UK, 12-07-2019, https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice, consulted on 17-01-2020; 'Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyber attacks – sources', Reuters, 27-01-2020, https://www.reuters.com/article/us-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyber attacks-sources-idUSKBN1ZQ10X, consulted on 29-01-2020; 'DNS Infrastructure Hijacking Campaign', US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign, consulted on 17-01-2020; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html, consulted on 17-01-2020.

43 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen; 'DNS Attacks Grow More Frequent and Costly', Infosecurity Magazine, 18-06-2019, https://www.infosecurity-magazine.com/news/dns-attacks-grow-more-frequent; 'Worst DNS attacks and how to mitigate them', Network World, 18-07-2019, https://www.networkworld.com/article/3409719/worst-dns-attacks-and-how-to-mitigate-them.html; 'Ongoing DNS hijacking and mitigation advice', NCSC-UK, 12-07-2019, https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice; 'DNS Infrastructure Hijacking Campaign', US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html. All sources consulted on 17-01-2020.

44 For the last of these: 'X-Force Threat Intelligence Index 2020', IBM, February 2020.

45 'Results of online expert consultation for CSAN 2020', TNO, 15-01-2020; 'Phishing verschuift naar SMS en WhatsApp', Dutch Payments Association, 26-11-2019, https://www.betaalvereniging.nl/actueel/nieuws/phishing-sms-whatsapp; '1.105.987 euro schade door Smishing al dit jaar!', Cybercrime Info, 06-10-2019, https://www.cybercrimeinfo.nl/cybercrime/smishing/360597_1-105-987-euro-schade-door-smishing-al-dit-jaar.

46 AIVD 2019 Annual Report, April 2020.

47 2019 Annual Report, Dutch Police, 13-1-2020.

48 'Veel Nederlandse servers misbruikt voor botnetspam', Computable, 11-02-2020, https://www.computable.nl/artikel/nieuws/security/6877213/250449/nederland-in-top-drie-van-botnetspam.html, consulted on 13-02-2020.

49 '2019 DDoS Report', Dutch National Internet Providers Management Organization, draft version, 17-3-2020.

50 'Results of online expert consultation for CSAN 2020', TNO, 15-01-2020.

51 '2019 Report on Cybersecurity Risks', Netherlands Bureau for Economic Policy Analysis, October 2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

52 'Results of online expert consultation for CSAN 2020', TNO, 15-01-2020; AIVD 2019 Annual Report, April 2020; MIVD 2018 Public Annual report, April 2019.

53 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers', Vice, 25-03-2019, https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers, consulted on 17-01-2020.

54 'Avast deploys hardened self-defense and wider intelligence industry collaboration', Avast, 21-10-2019 https://blog.avast.com/ccleaner-fights-off-cyberespionage-attempt-abiss, consulted on 03-01-2020.

55 'ASUS releases fix for Live Update tool abused in ShadowHammer attack', ZDNet, 26-03-2019, https://www.zdnet.com/article/asus-releases-fix-for-live-update-tool-abused-in-shadowhammer-attack, consulted on 03-01-2020; 'Some ASUS Updates Drop Backdoors on PCs in 'Operation ShadowHammer', *Threatpost*, 25-03-2019, https://threatpost.com/asus-pc-backdoors-shadowhammer/143129, consulted on 20-02-2020;
'BIS spolupracovala se společností Avast na odvrácení útoku na její produkty', Czech Security Information Service (BIS), 21-10-2019, https://www.bis.cz/aktuality/bis-spolupracovala-se-spolecnosti-avast-na-odvraceni-utoku-na-jeji-produkty-6acda7bf.html, consulted on 03-01-2020.

56 'Avast deploys hardened self-defense and wider intelligence industry collaboration', Avast, 21-10-2019 https://blog.avast.com/ccleaner-fights-off-cyberespionage-attempt-abiss, consulted on 17-01-2020.

57 AIVD 2019 Annual Report, April 2020.

58 'Cybersecurity in Operational Technology: 7 Insights You Need to Know', Ponemon Institute, March 2019, https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report, consulted on 16-03 2020.

59 'FBI and Federal Partners Brief Pipeline Industry Leaders on National Security Threats to Energy Infrastructure', FBI, 07-11-2019, https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/fbi-and-federal-partners-brief-pipeline-industry-leaders-on-national-security-threats-to-energy-infrastructure, consulted on 22-01-2020; 'India confirms cyber attack on nuclear power plant', *Financial Times*, 31-10-2019, https://www.ft.com/content/e43a5084-fbbb-11e9-a354-36acbbb0d9b6, consulted on 22-01-2020; 'Drilling Deep: A Look at Cyber attacks on the Oil and Gas Industry', Trend Micro, 12-12-2019, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/drilling-deep-a-look-at-cyber attacks-on-the-oil-and-gas-industry, consulted on 22-01-2020. 'Global Oil and Gas Cyber Threat Perspective', Dragos, August 2019, https://dragos.com/wp-content/uploads/Dragos-Oil-and-Gas-Threat-Perspective-2019.pdf, consulted on 22-01-2020.

60 '2019 Year in review: The ICS landscape and threat activity groups', Dragos, 2020.

61 'New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East', Security Intelligence, 04-12-2019, https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east, consulted on 13-02-2020; 'A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems', *Wired*, 20-11-2019, https://www.wired.com/story/iran-apt33-industrial-control-systems, consulted on 13-02-2020.
62 'More than a Dozen Obfuscated APT33 Botnets Used for Extreme Narrow Targeting', TrendMicro, 12-12-2019, https://blog.trendmicro.com/trendlabs-security-intelligence/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting, consulted on 13-02-2020.
63 AIVD 2019 Annual Report, April 2020.
64 AIVD 2019 Annual Report, April 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID', MIVD 2019 Public Annual Report, April 2020; 'The Netherlands and China: a new balance', Ministry of Foreign Affairs, May 2019, https://www.rijksoverheid.nl/documenten/rapporten/2019/05/15/nederland-china-een-nieuwe-balans; Speech by the AIVD's Director-General Dick Schoof at the Dutch Transformation Forum on economic security, AIVD, 21-11-2019, https://www.aivd.nl/documenten/toespraken/2019/11/20/speech-dick-schoof-op-dutch-transformation-forum-over-economische-veiligheid, consulted on 15-2-2020.
65 'Iraanse overheidshackers vallen Nederlandse onderwijsinstellingen aan', NOS, 14-2-2020, https://nos.nl/artikel/2322945-iraanse-overheidshackers-vallen-nederlandse-onderwijsinstellingen-aan.html.
66 Feedback from an external partner. Permission was obtained to include it in this report.
67 'FINTEAM: Trojanized TeamViewer Against Government Targets', Check Point Research, 22-04-2019, https://research.checkpoint.com/2019/finteam-trojanized-teamviewer-against-government-targets/, consulted on 17-01-2020.
68 AIVD 2019 Annual Report, April 2020.
69 2019 Annual Report, Dutch Police, 13-01-2020.
70 Feedback from Prof. Herbert Bos, Computer Systems Section of the VU University Amsterdam.
71 'Fortinet SSL VPN vulnerability from May 2019 being exploited in wild', Kevin Beaumont, 22-08-2019 https://twitter.com/GossiTheDog/status/1164536461665996800, consulted on 06-01-2020; 'Pulse Secure SSL VPN vulnerability being exploited in wild', Kevin Beaumont, 22-08-2019, https://twitter.com/GossiTheDog/status/1164553625881972739, consulted on 06-01-2020.
72 'Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open', *De Volkskrant*, 28-9-2019, https://www.volkskrant.nl/nieuws-achtergrond/intern-netwerk-honderden-bedrijven-en-ministerie-lag-maandenlang-wagenwijd-open~b9c96034.
73 'Bedrijven en overheid maandenlang kwetsbaar door groot beveiligingslek', NOS, 28-09-2019, https://nos.nl/artikel/2303667-bedrijven-en-overheid-maandenlang-kwetsbaar-door-groot-beveiligingslek.html, consulted on 03-01-2020; 'Opnieuw groot risico door beveiligingslek bij thuiswerksysteem', NOS, 29-09-2019, https://nos.nl/artikel/2303866-opnieuw-groot-risico-door-beveiligingslek-bij-thuiswerksysteem.html, consulted on 03-01-2020.
74 'Mitigation Steps for CVE-2019-19781', Citrix, 17-12-2019, https://support.citrix.com/article/CTX267679, consulted on 22-01-2020.
75 'Exclusief: Interview Citrix CISO, Fermín Serna, waar ging het mis?', *Techzine*, 23-01-2020, https://www.techzine.nl/blogs/security/436866/exclusief-interview-citrix-ciso-fermin-serna-waar-ging-het-mis.
76 'Kwetsbaarheid gevonden in Citrix ADC, Citrix Gateway en Citrix SD-WAN WANOP', National Cyber Security Centre, 24-12-2019, https://www.ncsc.nl/actueel/advisory?id=NCSC%2D2019%2D0979.
77 'Aanvallers zoeken actief naar kwetsbare Citrix-servers', Security.nl, 09-01-2020, https://www.security.nl/posting/638551/Aanvallers+zoeken+actief+naar+kwetsbare+Citrix-servers, consulted on 22-01-2020.
78 'Honderden Nederlandse Citrix-servers kwetsbaar voor aanvallen', Security.nl, 13-01-2020, https://www.security.nl/posting/639015/Honderden+Nederlandse+Citrix-servers+kwetsbaar+voor+aanvallen, consulted on 22-01-2020.
79 Government response to questions from MP Van den Berg about the news report 'Leeuwarden hospital suspends all data traffic after cyber attack', House of Representatives, 10-02-2020, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020D05339&did=2020D05339.
80 'College Beoordeling Geneesmiddelen slachtoffer Citrix-aanval', Security.nl, 10-02-2020, https://www.security.nl/posting/643318/College+Beoordeling+Geneesmiddelen+slachtoffer+Citrix-aanval.
81 'Citrix releases final fixes for CVE-2019-19781', Citrix, 24-02-2020, https://www.citrix.com/blogs/2020/01/24/citrix-releases-final-fixes-for-cve-2019-19781/, consulted on 27-01-2020.
82 'Citrix: we volgden na lek standaardprocedure, gebeurt duizenden keren per jaar', NOS, 18-1-2020, https://nos.nl/nieuwsuur/artikel/2319236-citrix-we-volgden-na-lek-standaardprocedure-gebeurt-duizenden-keren-per-jaar.html.
83 'Results of online expert consultation for CSAN 2020', TNO, 15-01-2020.

84 'Voorbereiden op digitale ontwrichting', WRR, 2019, p. 11, https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf, consulted on 13-02-2020.

85 'NSA waarschuwt voor beveiligingsrisico's clouddiensten', Security.nl, 28-01-2020, https://www.security.nl/posting/641329/NSA+waarschuwt+voor+beveiligingsrisico%27s+clouddiensten.

86 'De storing bij KPN liet zien waarom de waarschuwing van de NCTV niet voorbarig is', *Volkskrant*, 24-06-2019, https://www.volkskrant.nl/nieuws-achtergrond/de-storing-bij-kpn-liet-zien-waarom-de-waarschuwing-van-de-nctv-niet-voorbarig-is~bb9e2e41; 'Onderzoek naar storing 112', Radiocommunications Agency, 26-06-2019, https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112; 'KPN: softwarefout was oorzaak van storing 112, drie backups lieten het afweten', *Volkskrant*, 25-06-2019, https://www.volkskrant.nl/nieuws-achtergrond/kpn-softwarefout-was-oorzaak-van-storing-112-drie-backups-lieten-het-afweten~b73d62b4 ; 'Had de storing van 112 voorkomen kunnen worden?', *Volkskrant*, 28-06-2019, https://www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093; 'Ook dode in Den Haag tijdens 112-storing', RTL Nieuws, 03-07-2019, https://www.rtlnieuws.nl/nieuws/nederland/artikel/4767526/dode-den-haag-112-storing.

87 'Politie oefende niet voor 'zwaarste scenario' noodnummerstoring', *Volkskrant*, 04-07-2019.

88 Letter to parliament on the national outage at KPN, Ministry of Justice and Security, 25-06-2019, https://www.tweedekamer.nl/downloads/document?id=cc85aa5e-1e2b-4f4c-82b3-b9b20e215e9c&title=Brief%20van%20KPN%20inzake%20landelijke%20storing%20.pdf.

89 'Grote Google-storing trof Gmail, YouTube en diensten van derden', Tweakers.net, 03-06-2019, https://tweakers.net/nieuws/153510/grote-google-storing-trof-gmail-youtube-en-diensten-van-derden.html; 'Als het internet een hartaanval krijgt', *nrc.next*, 13-7-2019, https://www.nrc.nl/nieuws/2019/07/12/als-het-internet-een-hartaanval-krijgt-a3966947; 'BGP Route Leak Causes Cloudflare and Amazon AWS Problems', Bleeping Computer, 24-06-2019, https://www.bleepingcomputer.com/news/technology/bgp-route-leak-causes-cloudflare-and-amazon-aws-problems; 'Major websites and services across the internet went down Tuesday because of a hosting-platform outage', *Business Insider Nederland*, 02-07-2019, https://www.businessinsider.nl/cloudflare-outage-causes-major-websites-across-internet-to-go-down-2019-7?international=true&r=US; 'Amazon AWS Outage Shows Data in the Cloud is Not Always Safe', Bleeping Computer, 05-09-2019, https://www.bleepingcomputer.com/news/technology/amazon-aws-outage-shows-data-in-the-cloud-is-not-always-safe; 'AWS-diensten acht uur lang slecht bereikbaar door DDoS-aanval AG Connect', AG Connect, 24-10-2019, https://www.agconnect.nl/artikel/aws-diensten-acht-uur-lang-slecht-bereikbaar-door-ddos-aanval.

90 'Grote storing in vast telefoonnetwerk Tele2', AG Connect, 12-05-2019, https://www.agconnect.nl/artikel/grote-storing-vast-telefoonnetwerk-tele2; 'Storing bij Tele2 door kabelbreuk treft overheidsinstanties - update 3', Tweakers.net, 25-11-2019, https://tweakers.net/nieuws/160342/storing-bij-tele2-door-kabelbreuk-treft-overheidsinstanties.html; 'Deskundige na ICT-storing bij Amphia: ziekenhuizen steeds kwetsbaarder', *BN DeStem*, 12-10-2019, https://www.bndestem.nl/breda/deskundige-na-ict-storing-bij-amphia-ziekenhuizen-steeds-kwetsbaarder~a8f9429c; 'Grote storing bij Gelre ziekenhuizen, operaties afgezegd', 02-09-2019, https://www.omroepgelderland.nl/nieuws/2423232/Grote-computerstoring-bij-Gelre-ziekenhuizen-opgelost; 'Netwerkstoring verholpen', Tergooi.nl, 15-08-2019, https://www.tergooi.nl/netwerkstoring-storing-verholpen; 'Storing aan computers in Meander verholpen, AD, 02-04-2019, https://www.ad.nl/amersfoort/storing-aan-computers-in-meander-verholpen~a1b4ba75; 'Pinprobleem Albert Heijn veroorzaakt door storing firewall', AD, 11-06-2019, https://www.ad.nl/tech/pinprobleem-albert-heijn-veroorzaakt-door-storing-firewall~af755fa9; 'Zwitsers bedrijf routeerde KPN- en ander Europees verkeer via China Telecom', Tweakers.net, 07-06-2019, https://tweakers.net/nieuws/153726/zwitsers-bedrijf-routeerde-kpn-en-ander-europees-verkeer-via-china-telecom.html.

91 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Dutch Safety Board, 13-02-2020, pp. 57-63, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.

92 See 'The Year in Review'.

93 'Duizenden bedrijven met Citrix-systemen nog steeds kwetsbaar', Security.nl, 07-02-2020, https://www.security.nl/posting/642973/Duizenden+bedrijven+met+Citrix-systemen+nog+steeds+kwetsbaar.

94 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Dutch Safety Board, 13-02-2020, p. 64, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.

95 'AIVD-baas Dick Schoof: spanning tussen privacy en mogelijkheden inlichtingendienst', WNL Op Zondag, 16-02-2020, https://wnl.tv/2020/02/16/aivd-baas-dick-schoof-spanning-tussen-privacy-en-mogelijkheden-inlichtingendienst. Schoof's segment can be heard between around minute 40 and minute 48.

96 'Agentschap Telecom: digitale veiligheid IoT-apparaten niet op orde', Security.nl, 25-09-2019, https://www.security.nl/posting/625469/Agentschap+Telecom%3A+digitale+veiligheid+IoT-apparaten+niet+op+orde.

97 'Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde', Netherlands Court of Audit, 15-05-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.

98 'Results of online expert consultation for CSAN 2020'.
99 'Results of online expert consultation for CSAN 2020'.
100 'Voorbereiden op digitale ontwrichting', WRR, 2019, pp. 9-14, 11 https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf.
101 2019 Annual Report, Dutch Police, 13-01-2020.
102 'Twee verdachten aangehouden in onderzoek naar gestolen wachtwoorden', Dutch Police, 17-01-2020, https://www.politie.nl/nieuws/2020/januari/17/02-twee-verdachten-aangehouden-in-cybercrimeonderzoek-naar-gestolen-wachtwoorden.html, consulted on 29-1-2020.
103 2019 Annual Report, Dutch Police, 13-01-2020.
104 'Minister JenV wijst vier computercrisisteams aan', 27-01-2020, NCSC, https://www.ncsc.nl/actueel/nieuws/2020/januari/27/aanwijzing-certs.
105 'Convenant Nationaal Response Netwerk ondertekend', NCSC, 07-02-2020, https://www.ncsc.nl/actueel/nieuws/2020/februari/7/nrn.
106 'Cybersecurity is a matter for the top brass', Arno Visser, *CSR Magazine*, Cybersecurity Council, 10-2019, p. 24.
107 Letter to parliamentary on cybersecurity in education, Ministry of Education, Culture and Science, 14-02-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.
108 'VS en VK willen niet dat Facebook end-to-end-encryptie uitrolt', Security.nl, 04-10-2019, https://www.security.nl/posting/626523/VS+en+VK+willen+niet+dat+Facebook+end-to-end-encryptie+uitrolt; for the letter itself: https://www.justice.gov/opa/press-release/file/1207081/download.
109 'Voorbereiden op digitale ontwrichting', WRR, 2019, p. 11, 48 https://www.wrr.nl/binaries/wrr/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting/R101-Voorbereiden-op-digitale-ontwrichting.pdf.
110 'Het Citrix-beveiligingslek: de laatste stand van zaken', Security.nl, 19-1-2020 (last updated 23-01-2020), https://www.security.nl/posting/639997/Het+Citrix-beveiligingslek%3A+de+laatste+stand+van+zaken, consulted on 27-01-2020; 'Positive Technologies: Citrix vulnerability allows criminals to hack networks of 80,000 companies', Positive Technologies, 23-12-2019, https://www.ptsecurity.com/ww-en/about/news/citrix-vulnerability-allows-criminals-to-hack-networks-of-80000-companies.
111 'The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture', Recorded Future, 10-06-2019, https://www.recordedfuture.com/huawei-technology-risks. See also 'Huawei security threat derives from its sheer scale, says analysis; Cybersecurity report warns Chinese tech firm's breadth exposes customers to risk', *The Guardian*, 10-06-2019.
112 'Horizonscan Nationale Veiligheid 2019' (Horizon Scan of National Security 2019), National Network of Safety and Security Analysts, 10-2019.
113 'Results of online expert consultation for CSAN 2020'.
114 'Europa sluit Huawei niet uit – nog niet', *nrc.next*, 04-12-2019; 'Wees niet passief, doe als de Chinezen', *NRC Handelsblad*, 30-09-2019.
115 'Cyber Security Assessment Netherlands 2019', NCTV, 12-06-2019.
116 *The Inevitable: Understanding the 12 Technological Forces That Shape Our Future*, Kevin Kelly (2016).
117 '2019 National Security Horizon Scan', National Network of Safety and Security Analysts, 10-2019.
118 'Vulnerabilities in IoT Devices Have Doubled Since 2013', 17-09-2019, https://www.infosecurity-magazine.com/news/vulnerabilities-in-iot-devices, consulted on 06-04-2020.
119 '2019 National Security Horizon Scan', National Network of Safety and Security Analysts, October 2019.
120 '2019 National Security Horizon Scan', National Network of Safety and Security Analysts, October 2019.
121 '2019 National Security Horizon Scan', National Network of Safety and Security Analysts, October 2019.
122 'How Today's Geopolitics Are Creating an Uncertain Future for Global Tech', Entrepreneur Europe, 16-10 2019, https://www.entrepreneur.com/article/340714, consulted on 06-04-2020.
123 'Russia "successfully tests" its unplugged internet', BBC, 24-12 2019, https://www.bbc.com/news/technology-50902496 consulted on 03-04-2020; 'China moves to ban foreign software and hardware from state offices', TechCrunch, Devin Coldewey, 09-12-2019, https://techcrunch.com/2019/12/09/china-moves-to-ban-foreign-software-and-hardware-from-state-offices, consulted on 03-04-2020.
124 '2019 National Security Horizon Scan', National Network of Safety and Security Analysts, October 2019.
125 AIVD 2018 Annual Report, April 2019, pp. 9-10; MIVD 2018 Public Annual Report, April 2019, p. 17.
126 MIVD 2018 Public Annual Report, April 2019, p. 16.

127 'Former Facebook security chief: hack and leak campaigns are the new normal', Federal Computer Week, 11-06-2019 https://fcw.com/articles/2019/06/11/stamos-campaign-hacks-new-normal.aspx, consulted on 16-03-2020.
128 For general information about the threat posed by cybercriminals see e.g. '2020 Global Threat Report', Crowdstrike, 2020 and M-trends 2020, FireEye Mandiant, 2020.
129 2019 Annual Report, Dutch Police, 13-01-2020.
130 'Internet Organised Crime Threat Assessment' (IOCTA) 2019, Europol, 09-10-2019, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019; 'Targeted Ransomware: Proliferating Menace Threatens Organizations', Symantec, 18-07-2019, https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat.
131 Review.
132 Ransomware Against the Machine: 'How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT', FireEye blog, 24-02 2020, consulted on 05-03-2020.
133 'U.S. government concludes cyber attack caused Ukraine power outage', Reuters, 26-02-2016, https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K consulted on 19-03-2020; 'How an Entire Nation Became Russia's Test Lab for Cyberwar', *Wired*, 20-06-2017, https://www.wired.com/story/russian-hackers-attack-ukraine, consulted on 19-03-2020; 'Cyber attack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks', Jackson School of International Studies (JSIS), 11-10-2017, https://jsis.washington.edu/news/cyber attack-critical-infrastructure-russia-ukrainian-power-grid-attacks consulted on 19-03-2020.
134 https://nos.nl/artikel/2330187-waarom-worden-door-heel-nederland-zendmasten-in-brand-gestoken.html.
135 AIVD 2018 Annual Report, April 2019; MIVD 2018 Public Annual Report, April 2019.
136 'Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs', Volexity, 02-09-2019, https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/, consulted on 12-03-2020; 'Missing Link', The Citizen Lab, 24-09-2019, https://citizenlab.ca/2019/09/poison-carp-tibetan-groups-targeted-with-1-click-mobile-exploits/, consulted on 12-03-2020.
137 'Voorbereiden op digitale ontwrichting', Scientific Council for Government Policy, report no. 101, September 2019, pp. 45-46 https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.
138 'Onderzoek naar storing 112', Radiocommunications Agency, 26-06-2019, https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112; 'Had de storing van 112 voorkomen kunnen worden?', Volkskrant, 28-06-2019, https://www.volkskrant.nl/nieuws-achtergrond/had-de-storing-van-112-voorkomen-kunnen-worden~b235b093; 'Ook dode in Den Haag tijdens 112-storing', RTL Nieuws, 03-07-2019, https://www.rtlnieuws.nl/nieuws/nederland/artikel/4767526/dode-den-haag-112-storing.
139 'VPN warning: REvil ransomware targets unpatched Pulse Secure VPN servers', ZDNet, 06-01-2020, https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers, consulted on 17-02-2020; 'Continued Exploitation of Pulse Secure VPN Vulnerability', US-CERT, 10-01-2020, https://www.us-cert.gov/ncas/alerts/aa20-010a, consulted on 17-02-2020.
140 CSAN 2019.
141 'What are Data Manipulation Attacks, and How to Mitigate Against Them', Threatpost, 06-02-2019, https://threatpost.com/what-is-a-data-manipulation-attack-and-how-to-mitigate-against-them/141563, consulted on 16-03-2020.
142 'Aanvallers wijzigen wereldwijd dns-instellingen domeinen', Security.nl, 11-01-2019, https://www.security.nl/posting/593796/Aanvallers+wijzigen+wereldwijd+dns-instellingen+domeinen; 'DNS Infrastructure Hijacking Campaign', US-CERT, 10-01-2019, https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign; 'Global DNS Hijacking Campaign: DNS Record Manipulation at Scale', FireEye, 10-01-2019, https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html. All sources consulted on 03-03-2020.
143 'Systemic cyber risk. February 2020', European System Risk Board, 19-02-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'ESRB publishes report on systemic cyber attacks', ESRB, 19-02-2020, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, consulted on 25-02-2020.
144 See 'The Year in Review'.
145 Chapter 2 'The Year in Review' and chapter 5 'Interests'.
146 AIVD 2019 Annual Report, April 2020; 'VOORUITZIEND VERMOGEN VOOR VREDE & VEILIGHEID, De Militaire Inlichtingen- en Veiligheidsdienst Beschermt wat ons dierbaar is.' MIVD 2019 public annual report, April 2020.
146 AIVD 2019 Annual Report, April 2020.
148 Moore, T., 'The economics of cybersecurity: Principles and policy options' in International Journal of Critical Infrastructure Protection (Volume 3), 2010, pp. 103-117.

149 'Measures to protect telecom networks and 5G' [Parliamentary Paper], Ministry of Justice and Security, 01-07-2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/07/01/kamerbrief-maatregelen-bescherming-telecomnetwerken-en-5g/Maatregelen+bescherming+telecomnetwerken+en+5G.pdf; 'Response to article "Nederland kiest harde lijn tegen Huawei in 5Gnetwerk"' [Parliamentary Paper], Ministry of Economic Affairs, 03-02-2020, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2020/02/03/kamerbrief-met-reactie-op-bericht-nederland-kiest-harde-lijn-tegen-huawei-in-5g-netwerk/kamerbrief-over-reactie-op-bericht-nederland-kiest-harde-lijn-tegen-huawei-in-5g-netwerk.pdf.

150 'Universiteit Maastricht werd besmet via phishingmail en verouderde software', Security.nl, 05-02-2020, https://www.security.nl/posting/642452/Universiteit+Maastricht+werd+besmet+via+phishingmail+en+verouderde+software.

151 Feedback from an external party on a draft version of this document.

152 'Losgeld betalen aan cybercriminelen? Experts weten: soms is er amper keus', AD, 04-01-2020, https://www.ad.nl/tech/losgeld-betalen-aan-cybercriminelen-experts-weten-soms-is-er-amper-keus~a8451ffb; 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld', NOS, 02-01-2020, https://nos.nl/artikel/2317078-universiteit-maastricht-betaalde-ransomware-aanvallers-losgeld.html; 'Universiteitsblad: Universiteit Maastricht betaalde tonnen losgeld aan hackers', *Volkskrant*, 02-01-2020, https://www.volkskrant.nl/nieuws-achtergrond/universiteitsblad-universiteit-maastricht-betaalde-tonnen-losgeld-aan-hackers~b70d0f6b, 'Verzekeraars moeten stoppen met losgeld bij digitale afpersing', *Het Financieele Dagblad*, 27-12-2019; 'Microsoft: betalen van ransomware vaak enige optie voor bedrijven', Security.nl, 17-12-2019, https://www.security.nl/posting/635699/Microsoft%3A+betalen+van+ransomware+vaak+enige+optie+voor+bedrijven; 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27-08-2019, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

153 'Cyberverzekeringen: goed voor erbij of noodzakelijk?', BNR Digitaal podcast, Herbert Blankesteijn & Wesley Schouwenaars, 08-01-2020, https://www.bnr.nl/podcast/digitaal/10399508/cyberverzekeringen-goed-voor-erbij-of-noodzakelijk.

154 'Ransomware is nu een businessmodel van criminelen', NOS, 06-02-2020, https://nos.nl/op3/artikel/2321876-ransomware-is-nu-een-businessmodel-van-criminelen.html.

155 'Losgeld betalen aan cybercriminelen? Experts weten: soms is er amper keus', AD, 04-01-2020, https://www.ad.nl/tech/losgeld-betalen-aan-cybercriminelen-experts-weten-soms-is-er-amper-keus~a8451ffb; 'Universiteit Maastricht betaalde ransomware-aanvallers losgeld' NOS, 02-01-2020, https://nos.nl/artikel/2317078-universiteit-maastricht-betaalde-ransomware-aanvallers-losgeld.html; 'Universiteitsblad: Universiteit Maastricht betaalde tonnen losgeld aan hackers', Volkskrant, 02-01-2020, https://www.volkskrant.nl/nieuws-achtergrond/universiteitsblad-universiteit-maastricht-betaalde-tonnen-losgeld-aan-hackers~b70d0f6b, 'Verzekeraars moeten stoppen met losgeld bij digitale afpersing', Het Financiële Dagblad, 27-12-2019; 'Microsoft: betalen van ransomware vaak enige optie voor bedrijven', Security.nl, 17-12-2019, https://www.security.nl/posting/635699/Microsoft%3A+betalen+van+ransomware+vaak+enige+optie+voor+bedrijven; 'The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks', ProPublica, 27-08-2019, https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

156 'Ransomware is nu een businessmodel van criminelen', NOS, 06-02-2020, https://nos.nl/op3/artikel/2321876-ransomware-is-nu-een-businessmodel-van-criminelen.html.

157 'Systemic cyber risk February 2020', European System Risk Board, 19-02-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'Understanding Systemic Cyber Risk', World Economic Forum, 21-10-2016, https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk; Lincoln Kaffenberger and Emanuel Kopp, 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment', Carnegie Endowment For International Peace, September 2019; Jonathan William Welburn and Aaron Strong, 'Systemic Cyber Risk and Aggregate Impacts', RAND Institute for Civil Justice, September 2019; 'Quantifying Systemic Cyber Risk. Report on the "Connectedness in Cyber Risk" Workshop', Global CRQ Network, 2018; 'ADDRESSING SYSTEMIC CYBERSECURITY RISK. APPLIED RESEARCH PROGRAM', The Henry M. Jackson School of International Studies, 22-05-2018, https://jsis.washington.edu/wordpress/wp-content/uploads/2019/02/JSIS_ARP_Report_1_Risk_2018_FINAL.pdf.

158 'Systemic cyber risk. February 2020', European System Risk Board, 19-02-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf .

159 'Systemic cyber risk. February 2020', European System Risk Board, 19-02-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; Lincoln Kaffenberger and Emanuel Kopp, 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment', Carnegie Endowment For International Peace, September 2019; Jonathan William Welburn and Aaron Strong, 'Systemic Cyber Risk and Aggregate Impacts', RAND Institute for Civil Justice, September 2019; 'Quantifying Systemic Cyber Risk. Report on the "Connectedness in Cyber Risk" Workshop', Global CRQ Network, 2018; 'Understanding Systemic Cyber Risk', World Economic Forum, 21-10-2016, https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk.

160 'Seven hackers have now made a million dollars each from bug bounties, says HackerOne', ZDNet, 25-02-2020, https://www.zdnet.com/article/seven-hackers-have-now-made-a-million-dollars-each-from-bug-bounties-says-hackerone.
161 'Systemic cyber risk. February 2020', European System Risk Board, 19-02-2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf; 'ESRB publishes report on systemic cyber attacks', ESRB, 19-02-2020, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, consulted on 25-02-2020.
162 'AIVD-baas Dick Schoof: spanning tussen privacy en mogelijkheden inlichtingendienst', WNL Op Zondag, 16-02-2020, https://wnl.tv/2020/02/16/aivd-baas-dick-schoof-spanning-tussen-privacy-en-mogelijkheden-inlichtingendienst. The interview with the head of the AIVD Dick Schoof taken place between minutes 40.00 and 48.00.
163 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen', Dutch Safety Board, 13-02-2020, pp. 57-63, https://www.onderzoeksraad.nl/nl/media/attachment/2020/2/13/patientveiligheid_bij_ict_uitval_in_ziekenhuizen.pdf.
164 'Cyber security in education' [letter to parliament], Ministry of Education, Culture and Science, 14-02-2020, https://www.tweedekamer.nl/downloads/document?id=4186214c-16fe-4891-842d-571b86e41a19&title=Reactie%20op%20het%20verzoek%20van%20het%20lid%20Wiersma%2C%20gedaan%20tijdens%20de%20Regeling%20van%20Werkzaamheden%20van%2014%20januari%202020%2C%20over%20een%20cyberaanval%20bij%20de%20Universiteit%20Maastricht.docx.
165 'Results of online expert consultation for CSAN 2020'.
166 'Risicorapportage cyberveiligheid economie 2019', Netherlands Bureau for Economic Policy Analysis, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.
167 'Risicorapportage cyberveiligheid economie 2019', Netherlands Bureau for Economic Policy Analysis, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.
168 Moore, T., 'Economics of Cybersecurity Market failures', 21-01-2015, https://delftxdownloads.tudelft.nl/EconSec101x-EconomicsCybersecurity/Week%204/EconSec101x-4a-slides.pdf; Pasquinucci, A., 'Economics of ICT security', in Computer Fraud & Security, 2008, pp. 4-6; Moore, T., 'The economics of cybersecurity: Principles and policy options' in International Journal of Critical Infrastructure Protection (Volume 3), 2010, p.103-117; Jalali, M. S., Siegel, M. and Madnick, S., 'Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment' in The Journal of Strategic Information Systems, 28(1), 2019, pp. 66-82.
169 Regarding methods of attack, see: 'X-Force Threat Intelligence Index 2020', IBM, February 2020.
170 '2019 Data Breach Investigations Report', Verizon, 08-05-2019.
171 'Google: Security Keys Neutralized Employee Phishing', Brian Krebs, 23-07-2018, https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing, consulted on 12-03-2020.
172 '2020 Cyber Security Report', Check Point, 18-01-2020.
173 '2019 Data Breach Investigations Report', Verizon, 08-05-2019.
174 'X-Force Threat Intelligence Index 2020', IBM, February 2020.
175 'X-Force Threat Intelligence Index 2020', IBM, February 2020.
176 'M-trends 2020', FireEye, 20-02-2020.
177 '2020 Global Threat Report', Crowdstrike, 04-03-2020.
178 Review.
179 'Response by the Maastricht University FOX-IT report', Maastricht University, 05-02-2020; 'UM Cyber Attack Symposium – Lessons learnt', Maastricht University, 05-02-2020, https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt, consulted on 11-03-2020; 'Servers Universiteit Maastricht misten belangrijke update uit 2017', Security.nl, 06-02-2020, https://www.security.nl/posting/642659/Servers+Universiteit+Maastricht+misten+belangrijke+update+uit+2017, consulted on op 11-03-2020.
180 'Results of online expert consultation for CSAN 2020'.
181 'Results of online expert consultation for CSAN 2020'.
182 Review.
183 'X-Force Threat Intelligence Index 2020', IBM, February 2020; 'M-trends 2020', FireEye, 20-02-2020.
184 'Policy response to CSAN 2019 and the NCSA progress report' [letter to parliament], Ministry of Justice and Security, 12-06-2019, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/06/12/tk-beleidsreactie-CSAN2019-en-voortgangsrapportage-ncsa/tk-beleidsreactie-CSAN2019-en-voortgangsrapportage-ncsa.pdf.
185 'Digitale dijkverzwaring: cybersecurity en vitale waterwerken', Court of Audit, 28-03-2019.
186 'Digitalisering aan de grens: Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol', Court of Audit, 20-04-2020.

187 'Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde', Court of Audit, 15-05-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.
188 'Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde', Court of Audit, 15-05-2019, https://www.rekenkamer.nl/actueel/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde.
189 'Staat van de rijksverantwoording 2019. Breekt nood wet?', Court of Audit, 20-05-2020, https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019/SRV-wr.pdf.
190 'Staat van de rijksverantwoording 2019. Breekt nood wet?', Court of Audit, 20-05-2020, https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2020/05/20/staat-van-de-rijksverantwoording-2019/SRV-wr.pdf.
191 'National Crisis Plan for Digital Incidents', National Coordinator for Security and Counterterrorism (NCTV), 21-02-2020.
192 'Initial Access', MITRE ATT&CK, 17-10-2018 (updated 19-07-2019), https://attack.mitre.org/tactics/TA0001, consulted on 12-03-2020.
193 'Factsheet Indicators of Compromise', NCSC, 08-12-2016, https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-indicators-of-compromise.
194 'Factsheets informatiedeling binnen de keten', Digital Trust Center, https://www.digitaltrustcenter.nl/factsheets-informatiedeling-binnen-de-keten, consulted on 12-03-2020.
195 See 'The Year in Review'.
196 'Double Dragon APT41, a dual espionage and cyber crime operation', FireEye, 04-09-2019, https://content.fireeye.com/apt-41/rpt-apt41.
197 'Critical infrastructure and critical processes', NCTV, https://english.nctv.nl/topics/critical-infrastructure-protection.

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 2020