National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

Cyber Security Assessment Netherlands

CSAN 2022

Cyber Security Assessment Netherlands 2022

Publication details

The Cyber Security Assessment Netherlands 2022 (CSAN 2022) offers insight into the digital threat, the interests that may be affected by it, resilience and, finally, the risks. The focus is on national security. CSAN 2022 also aims to provide insight into the strategic themes relevant to the digital security of the Netherlands now and in the next four to six years. The CSAN is published annually by the National Coordinator for Security and Counterterrorism (NCTV).

Together with its partners in the security domain, the NCTV contributes to a safe and stable Netherlands by identifying threats, boosting resilience and protecting national security interests. The purpose is to prevent and minimise social disruption. Since the establishment of the National Coordinator for Security and Counterterrorism, a single government organisation has been responsible for counterterrorism, cybersecurity, national security and crisis management.

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

Table of contents

Resilience can erect a dam against the threat

Imbalance between threat and resilience increases risk of disruption

In order to function without disruption, it is crucial that society can withstand digital threats. The security of digital processes is essential in our strongly digitized society. Digital security therefore is inextricably interlinked with national security. The question 'How digitally safe is the Netherlands?' is impossible to answer. Moreover, 100 percent security does not exist. Digital processes can always fail due to technical or human errors. Cyberspace is also the preferred playing field of a growing number of states, and cyber attacks are the new normal. Moreover, attacks by cybercriminals have now reached an industrial scale. The digital threat is therefore permanent and is increasing rather than decreasing, with all the associated consequences.

In spite of the efforts to improve resilience, there is an imbalance between the increased threat and the development of resilience. That imbalance increases the risk of disruption. A question that is relevant but difficult to answer is: 'When is the Netherlands sufficiently resilient?' Resilience can help to create a barrier against the threat. That calls for a conscious assessment of the balance between the dependence on digital processes and the importance attached to this, the threat against this and also the required level of resilience. Although they are different in nature, a comparison can be made with the COVID-19 pandemic and the war in Ukraine. They have confronted us with the existence of dependencies, vulnerabilities and unforeseen consequences of far-reaching events. The question of when the Netherlands is sufficiently resilient is not only a matter for technical experts. It is mainly a matter of governance and/or risk management for politicians, governments and administrators at national, sectoral and organisational level as well as between those three levels.

Complications of risk management present a threat to society

The NCTV, in cooperation with partners, has identified strategic themes that are relevant to the digital security of the Netherlands now and in the years ahead. Although they are different in nature, each of them in isolation and in combination with each other forms complications for strategic risk management. The themes are briefly introduced below; a detailed explanation will be given in Chapter 3.

Risks form the downside of a digitized society

Dutch society is highly digitized, and the COVID-19 pandemic has accelerated the further digitisation of processes. This has a downside: our dependence on digital processes has also made us vulnerable to outages and the activities of those with malicious intent. There are four risks to national security, which also apply directly or indirectly to specific sectors and organisations and individual citizens: 1) unauthorised access to information (and possibly its publication), in particular through espionage; 2)

inaccessibility of processes, due to sabotage and/or the use of ransomware or preparations for this; 3) breaches of (the security of) cyberspace, such as through the exploitation of global IT supply chains; 4) large-scale outages of digital processes. The high level of digitisation of our society and the dependence on digital processes are a fact. Getting vulnerabilities under control and keeping them under control is part of risk management.

Cyberspace is a playing field for regional and global dominance

A growing number of states are using cyberspace structurally and intensively to promote their geopolitical interests. Cyber attacks, for example to gather political and economic information, are an important instrument in that respect: they are relatively cheap and scalable, and they have a significant, often long-term result. Attribution is a difficult issue. Furthermore, geopolitical fencing is taking place about the building blocks of cyberspace and high technologies. Individual citizens, organisations, sectors and countries have little influence on that geopolitical competition, while it does contribute to the risks.

Cybercrime is scalable, while resilience – for now – is not

Serious, organised cybercrime has become very scalable and has therefore taken on industrial proportions in recent years in terms of victims, damage and criminal proceeds. The term scalability refers to the ability to adjust (upscale) a system or process in order to meet a higher demand. Serious cybercriminals and their service providers are primarily financially motivated and aim for maximum yields, while gratefully exploiting the options offered by the digital domain. Considering the nature and growing extent of the threat of cybercrime, making and keeping the resilience chain scalable will be a fundamental challenge in the coming years.

Market dynamics complicate controlling digital risks

Supply and demand for digital services, hardware and hardware components, software and networks meet on digital markets. These markets have several unique characteristics, such as the monopoly or semi-monopoly status of certain suppliers, the high level of interconnectedness and the focus on gathering as much data as possible. Moreover, incentives for digital security are not or not always decisive in these markets. Those characteristics complicate risk control for individual citizens, organisations, sectors and countries.

Coordinated and integrated risk management is still in its infancy

Coordinated and integrated risk management within and between the different levels of organisations, sectors and the national level is still in its infancy. Resilience in the Netherlands has not yet reached the required level. Digital risks do not yet form a structural part of broader risk management, and a coordinated approach is necessary.

Restrictions in digital autonomy also restrict digital resilience

Restrictions in digital autonomy apply for European countries and the Netherlands (hereafter: the Netherlands and Europe). That autonomy includes the ability and resources the Netherlands has to make independent decisions about further digitisisation and the required level of digital resilience. Restrictions in digital autonomy also involve restrictions for resilience. The fact that the autonomy is under pressure is due to various causes, which are related to the strategic themes mentioned above. Those causes reduce the options to influence and make choices in terms of the digital resilience of the Netherlands and how to control this resilience.

Insight in strategic themes relevant to the digital security of the Netherlands

1 Introduction

CSAN 2022 provides insight into the digital threat, the interests that may be affected by this, resilience and, finally, the risks. The focus is on national security. CSAN 2022 also aims to provide insight into the strategic themes relevant to the digital security of the Netherlands now and in the next four to six years. That insight provides the basis for the new cybersecurity strategy.

Purpose and scope

The Cyber Security Assessment Netherlands (CSAN) provides insight into the digital threat, the interests that may be affected by this and the resilience against this. On the basis thereof, risks have been formulated. The emphasis is on national security. Digitisation offers many opportunities, but it also lends itself to all kinds of exploitation, and outages may occur. The CSAN does not focus on the opportunities offered by digitisation. It does, however, focus on disruptions of critical and other processes with a digital component.

The CSAN is intended primarily for strategic planning and policy-making at national level (governance). It aims to provide the Cabinet, members of the Upper and Lower Houses of Parliament, civil servants, policy-makers, other public administrators and leaders of organisations with an insight into the risks for the Netherlands. Cybersecurity companies and professionals use the CSAN as a reference framework for their own management or customers. The CSAN is also intended as a tool for risk management, aimed specifically at the identification and analysis of risks, which is one of the steps in a risk management process. Finally, the CSAN can also be accessed by the general public.

Toelichting sleutelbegrippen

Due to the interconnectedness of the physical space and cyberspace and to improve readability, the terms 'cyber' and 'digital' have only been used occasionally.

Sleutelbegrippen

In the CSAN, the most important concepts have been defined as follows [1]:

Interest: values, achievements, tangible and intangible things that can be damaged when a cyber incident occurs and the weight that society or a party attaches to defending them. In the CSAN, the focus is on national security interests.

Attack: intentional activity by an actor aimed at disrupting one or more digital processes using digital resources.

Cyber incident: (coherent set of) events or activities that lead to disruption of one or more digital processes. Collective term for cyber attack and system failure.

Cybersecurity: the set of measures to reduce (relevant) risks to an acceptable level. The measures may be aimed at preventing cyber incidents and, once they have occurred, detecting them, limiting damage and making recovery easier. What is an acceptable level, is the outcome of a risk assessment.

Digital process (hereafter: process): a process carried out in whole or in part through the complex and interrelated interaction of people and many components of hardware, software and/or networks. Fully automated processes, such as process control systems, are also included.

Risk: the probability that a threat will lead to a cyber incident and the impact of the cyber incident on the interests, both in relation to the current level of digital resilience.

Cyberspace: the complex environment that is the result of interrelated digital processes, supported by globally distributed physical information and communication technology (ICT) devices and connected networks. Cyberspace is approached from three different angles or levels: 1) digital processes implemented (or initiated) by people; 2) the technology level (of IT and OT) enabling the digital processes; 3) the risk management and/or governance level managing the two other levels.
Threat: an intentional or unintentional danger that may lead to a cyber incident or a combination of simultaneous or consecutive cyber incidents.
System failure: a situation where one or more digital processes are disrupted due to natural or technical causes or as a consequence of human error.
Disruption: an undermining of the availability, integrity or confidentiality of information or the processing of information, i.e. a disruption at the technical level of cyberspace.
Resilience: the capacity to reduce relevant risks to an acceptable level by means of a series of measures to prevent cyber incidents and, when cyber incidents have occurred, to detect them, limit the damage and facilitate recovery. What constitutes an acceptable level of resilience depends on the outcome of a risk assessment. This may help to choose the right technical, procedural or organisational measures.

Structure

Chapter 2 looks at the current situation in terms of interest, threat and resilience. Chapter 3 specifies and describes the strategic themes relevant to the digital security of the Netherlands now and in the next four to six years. Chapter 4 looks back on the most important incidents of the past year. Annex 1 describes the process of creating the CSAN. Annex 2 contains the source references.

Cyber attacks by state actors are no longer rare, they are actually the new normal

2. Digital risks remain high

The basis for the analysis in the Cyber Security Assessment Netherlands is formed by interest, digital threat and resilience. These three together determine the digital risks. There are four risks for national security (see the box below). These risks also relate to sectors, organisations and individuals. This chapter will briefly look at the current situation of national security interests, the threat against them and our digital resilience. This situation has not changed fundamentally in comparison with last year. The threats, however, have evolved. Ransomware groups, for example, are aiming for optimum, scalable chains of attack. Attackers are also increasingly focusing on exploiting the cloud. Finally, cyber attacks on supply chains and the exploiting of zero-day vulnerabilities are also a growing problem.

Four national security risks

1. **Unauthorised access to information** (and possibly its publication), in particular through espionage. Examples include espionage targeting communications within the central government or the development of innovative technologies.
2. **Inaccessibility of processes**, due to sabotage and/or the use of ransomware or preparations for this. Examples include cyber infiltration in processes that ensure the distribution of electricity.
3. **Breaches of (the security of) cyberspace**, such as through the misuse of global IT supply chains.
4. **Large-scale outages**: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action.

Digital processes: the central nervous system of society

Digital processes are the 'central nervous system' of society and the economy, as they are indispensable to their uninterrupted functioning.[2] Digital security therefore forms an integral part of national security. When vital processes such as the electricity or drinking-water supply, the handling of shipping traffic or payment transactions are hit, society can be brought to a standstill for a brief or sustained period. Cyber incidents can therefore affect more and other interests than the functioning of technology alone. Each of the six national security interests described in the National Security Strategy[3] can be hit via cyberspace. Digital security has not been explicitly named as a national security interest, but it acts as a common thread for the six interests mentioned. They are discussed in brief below.

Territorial security is the unimpeded functioning of the Netherlands and its EU and NATO allies as independent states in a broad sense, or territorial security in a narrow sense. This not only concerns the integrity of our national territory and that of our allies, but also the integrity of the digital domain: the availability, confidentiality and integrity of essential information services and vital infrastructure and processes that depend on this.

Physical security is the ability of people to go about their lives in an unimpeded manner within the Netherlands and their surrounding area. Physical security in a narrow sense concerns the safety of life and limb of Dutch residents. In a broad sense, this concerns providing for the primary necessities of life, such as food, energy, drinking water and adequate housing.

Economic security is the unimpeded functioning of the Dutch economy in an effective and efficient manner. The three essential conditions for this are the continuity of vital processes, the integrity and exclusivity of information and knowledge and the prevention of undesirable strategic dependencies.

Ecological security is the unimpeded continued existence of the natural living environment in and around the Netherlands. When

ecological security is hit, this is evident from a long-term deterioration of the environment and nature.

Social and political stability is the continued and unimpeded existence of a social climate in which individuals are free to go about their lives and groups are able to coexist within and in accordance with the democratic and lawful state of the Netherlands and its shared values.

Finally, the **international rule of law** is the functioning of the international system of rules, standards and agreements established for the purposes of international peace and security. Our national security depends on the functioning of the international system of rules, standards and agreements, partly because of the international position of the Netherlands and the presence of physical and digital hubs in global networks and infrastructure.

Threat posed mainly by state actors, cybercriminals and outages

The threat against the national security interests may result from cyber attacks or outages of digital processes. An outage may be the consequence of natural or technical causes or human errors. State actors and cybercriminals form the greatest threat in terms of intentional action. It is not always easy to distinguish between them due to their interrelationships. The threat posed by hacktivists is relatively small, but may affect Dutch interests indirectly.

Cyber attacks by state actors are the new normal

The digital threat posed by state actors to Dutch society is diverse in nature. Cyber attacks by state actors can no longer be considered rare; instead, they are the new normal. Cyberspace is used by states for their geopolitical advantage. This may concern a financial-economic advantage, promoting domestic political and security interests or influencing foreign relationships.[4] The digital methods state actors can use for this purpose include:

1. influencing and interference (including the spread of disinformation);
2. espionage, including economic or political espionage;
3. preparatory action for disruption and actual disruption and sabotage.

The Netherlands is the target of offensive cyber programmes of countries such as Russia and China. They can use the digital methods mentioned against a broad range of possible targets, from local associations to international security organisations and from one individual to diaspora communities. According to the General Intelligence and Security Service, the threat of offensive cyber programmes against the Netherlands and Dutch interests continues to be high and will only increase in the future.[5]

Russian state actors have successfully carried out digital attacks on EU Member States on several occasions. This incident illustrates the current threat picture of Russian state actors and the continuous threat (including threat of espionage) this involves. These actors carry out multiple digital attacks on EU and NATO Member States, among others.

The Chinese digital espionage actor APT31 has carried out large-scale, sustained attacks on political targets in Europe and North America.[6] In the Netherlands, this actor also selected targets for attacks and reconnaissance activities. The interest shown by state actors for such targets illustrates the importance of solid security measures and network detection options for Dutch government networks in order to detect and withstand attacks and facilitate further investigation.

According to leaked documents, an Iranian cyber organisation investigated hacking industrial control systems in 2020. The Iranian investigators write that they do not yet have sufficient insight into the systems to enable physical sabotage. The documents show that the cyber actors were specifically looking for building control systems, also in the Netherlands. This fits in the puicture of the increasing emphasis on cyber sabotage in Iran.

Cybercriminals can impair national security

Cybercriminals continue to be able to inflict extensive damage to digital processes. Their actions are based on financial motives, and they do not intend to disrupt society. However, the impact of their attacks can be such that they affect national security interests. The capacity of a number of cybercrime groups is of an equally high level as that of some state actors. State actors can hire cybercriminals, give them permission to act or put them under pressure to carry out cyber attacks on specific targets.[7] The relationships between states and cybercriminals may lead to cybercriminals taking sides in geopolitical conflicts. This has been illustrated recently by the war in Ukraine, when cybercrime groups affiliated with Russia warned opponents of Russia that they would be digitally attacked.[8]

Cyber attacks on supply chains by criminals are a growing problem.[9] Cyber incidents not only have an impact on direct victims, but also on chains of suppliers, customers and citizens using the services provided by the affected organisations. More and more often, cybercriminals compromise their final targets via suppliers and business partners.[10] When processes are disrupted, chain effects may have an impact on entire sectors or even society as a whole.[11] Moreover, ransomware attacks are used increasingly often with double or even triple extortion.[12] In the case of double extortion, hackers can threaten to publish data if victims fail to pay after their files have been encrypted. When triple extortion takes place, hackers are also able to issue a ransom demand based on stolen data to customers, partners and suppliers of the affected organisation, in the hope that they will also pay, out of fear that their data will be published. [13]

Organisations subjected to a digital attack are often the victim of ransomware. The use of ransomware poses a risk to national security in terms of the continuity of vital processes, the leaking and/or publication of confidential or sensitive information and the deterioration of the integrity of cyberspace.[14] Vital processes can be hit by ransomware directly, with all the associated consequences, or via supply chains, especially now that those attacks involve double or even triple extortion.

Attackers focus on zero-days and the cloud

The exploitation of zero-day vulnerabilities is still a matter of concern.[I] The National Cyber Security Centre is seeing an increase in the number of zero-day vulnerabilities. The exploitation of zero-days can have a large-scale impact if the vulnerability is located in frequently used software or hardware. As soon as a zero-day has been publicised, it is called a one-day or n-day vulnerability. This also poses a risk because, while a patch may be available, the user may not yet have implemented this. For example, critical systems and applications for vital and other processes cannot always be taken offline immediately in order to install a patch, leaving them vulnerable to exploitation.

The Military Intelligence and Security Service and the General Intelligence and Security Service have evidence that state actors are exploiting an unknown vulnerability (zero-day) in PulseConnect SecureVPN software, namely CVE-2021-22893. The services advise national users to put into place security measures for this zero-day as soon as possible. The National Cyber Security Centre has published advice on its website, based partly on information from the General Intelligence and Security Service and the Military Intelligence and Security Service, to help organisations to mitigate this vulnerability.

The use of zero-day exploits by state actors against Dutch targets illustrates the structural and advanced state digital threat against Dutch economic and political security interests.

Attackers are also increasingly focusing on exploiting the cloud.[15] Cloud services have become crucial elements of many business processes over the past few years.[16] Malicious actors see this dependence as a new opportunity to disrupt digital processes.[17] More use of the cloud also means more potential victims. Outages or disruption of cloud services may have large-scale consequences for Dutch organisations and sectors.

Polarisation and international conflicts: a breeding ground for hacktivists

The direct threat to the Netherlands posed by hackers' collectives, such as hacktivists[II], is small. However, these groups do pose an indirect threat. In various countries, hacktivists are present who can have an impact through, for example, hack-and-leak operations or the systematic digital intimidation of individuals and organisations. Hackers' collectives can also play a part in hybrid warfare, as they are doing in the war in Ukraine in 2022. The danger is that the activities of hacktivists may be wrongly interpreted by countries that are the victim of their attacks, which may lead to counter-reactions. In addition, state actors may operate under the flag of hacktivists. Due to the increased activity of hackers' groups, there is a chance that the Netherlands will suffer direct or indirect damage from digital attacks. If hackers carry out cyber attacks on foreign targets from or via the Netherlands, the Netherlands could also be hit by a counter-reaction. Dutch residents may also participate in actions by hacktivists and as a result become involved in conflicts. Involvement in a conflict elsewhere by carrying out digital attacks may have unforeseen consequences and is also a punishable offence.[18]

Resilience not yet sufficient

It was concluded in CSAN 2021 that the level of resilience in the Netherlands is not yet sufficient.[19] This remains unchanged, as is evident from different reports published over the past year. According to the Dutch Safety Board, the gap between the extent of the threat and digital dependence as compared to the resilience of society against this is growing.[20] Reports from the Cyber Security Council and the Dutch Safety Board also indicate fragmented incident response, insufficient supervision and inadequate sharing of information.[21] In May 2022, the Netherlands Court of Audit stated that information security at the government level is improving step by step. However, inadequacies are still found, and

I A zero-day vulnerability is a vulnerability for which no patch is available yet, but which has been discovered by hackers and can be exploited.

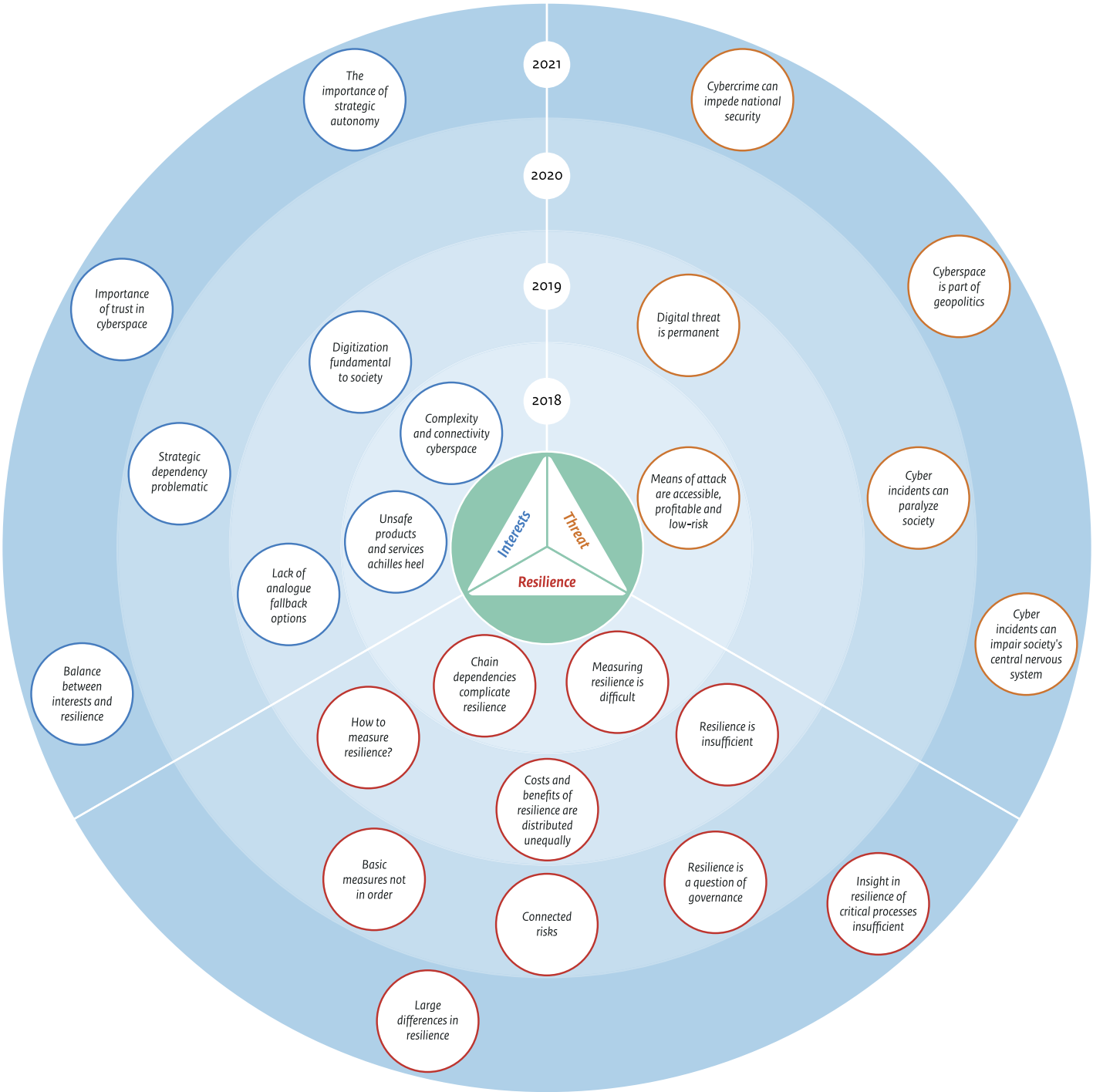
II 'Hacktivist' is a contraction of the words hacker and activist: an actor who launches digital attacks of an activist nature, motivated by a certain ideology.

their solution requires a determined and structured approach.[22] Full resilience against digital threats is impossible, but increasing the resilience against outages and exploitation is the most important instrument in controlling digital risks.

Digital resilience is not yet as it should be everywhere, because basic measures are insufficiently implemented. This concerns, for example, the use of multi-factor authentication and creating tests and backups.[23] There are large differences in resilience between and within sectors and supply chains. The Inspectorate of Justice and Security states that a lot of work still needs to be done to increase the resilience of organisations providing critical services, while also noting that the awareness of the importance of this has increased.[24] Organisations that are sufficiently resilient have not only taken basic measures but have also focused on a risk-based method of working.[25]

CSAN in retrospect

The image below shows the themes that have been included in the CSAN over the past four years in terms of interests, threat and resilience. CSAN 2022 builds on these findings by providing insight into the strategic themes relevant to the digital security of the Netherlands now and in the next four to six years.



Cyberspace is borderless, giving cybercriminals unprecedented opportunities to attack targets around the globe

3 Complications of risk management pose a threat to society

The NCTV, in cooperation with partners, has identified strategic themes that are relevant to the digital security of the Netherlands now and in the years ahead[26]:

- Risks form the downside of a digitized society.

- Cyberspace is a playing field for regional and global dominance.

- Cybercrime is scalable, while resilience – for now – is not.

- Market dynamics complicate controlling digital risks.

- Coordinated and integrated risk management is still in its infancy.

In addition, an overarching theme has been identified that affects all the other themes: restrictions in digital autonomy also restrict digital resilience. Although they are different in nature, each of the themes in isolation and in combination with each other illustrates complications for strategic risk management. The themes are discussed in more detail below. The strategic and policy-based handling of these themes will be addressed in the Netherlands Cyber Security Strategy.

Risks form the downside of a digitized society

Dutch society is highly digitised.[27] There are hardly any processes left without a digital component.[28] Education, the care sector, the corporate sector, the government and citizens all use digital processes for many purposes and cannot do without them. Moreover, certain developments in society, such as the energy transition, encourage further digitisation.[29]

Digitisation has made a positive contribution to society and the economy, but it also has a downside: the occurrence of risks. Dependence on digital processes, products, services and networks (hereafter: digital processes) makes us vulnerable. That dependence offers many opportunities for malicious individuals.

Targeted attacks on processes are commonplace. Vulnerabilities (for example, in software) are often actively exploited when attacks are launched. States carry out digital attacks to be able to spy on or (at a later stage) sabotage their opponents. There are countries that are attempting on a structural basis to gain access to the critical infrastructure of our allies to make preparations for digital disruption or even sabotage. In the past, the Netherlands has also been the target of such preparatory activities for sabotage.[30] Cybercriminals take advantage of the dependence on digitisation by means of ransomware attacks, gaining large sums of money. They also use data stolen via hacks for this purpose.

When digital processes do not work properly, this affects the functioning of organisations. Chain reactions can affect sectors or even society as a whole. The disruption of digital processes can also have physical consequences. For example, a power cut may occur, education may come to a standstill or patient care in a hospital may be compromised.[31] Critical processes also have a digital component and are therefore vulnerable. In the worst case, processes that are not functioning properly may lead to social disruption, putting national security at risk.

The high level of digitisation of our society and the dependence on digital processes are a fact. Getting vulnerabilities under control and keeping them under control is part of risk management, but this is not easy. When this is not done sufficiently successfully, the stability of society may be put at risk and social disruption may occur.

Cyberspace is a playing field for regional and global dominance

A growing number of states are using cyberspace structurally and intensively to promote their geopolitical interests. Conversely, cyberspace issues are increasingly of geopolitical interest.[32] Geopolitics is a broad concept, but it is always based on actively wanting to improve one's own relative starting position in a political, economic, military or cultural sense, both regionally and globally. Technology (in particular upcoming technologies such as 5G, AI and quantum technology) is the playing field, the resource as well as the stake of the game. Within cyberspace as it is now, attacks take place with the aim to gather information and data, disrupt operational processes and, for example, influence the sentiment of neighbouring countries. The ultimate geopolitical conflict, war, also involves cyber attacks. This is visible, for example, in Ukraine, where Russian state actors carried out digital attacks before and during the invasion, aimed at the disruption of communication and logistics. Finally, states promote their interests by making strategic use of the building blocks of cyberspace. This concerns resources, standards and building blocks such as hard and software components. Because of the importance of cyberspace for the economy and society, an increasing number of countries are acknowledging that digital security forms part of national security.[33]

Cyber attacks as a tool for promoting geopolitical interests

Cyberspace, by its nature, crosses national borders and covers land, sea, air and space. Gathering political and economic information, collecting and checking data and disrupting operational processes takes place without putting one foot across the border. Cyber attacks are relatively cheap, scalable, difficult to attribute and produce a significant, often long-term result. A successful hack can sometimes yield information invisibly, secretly and unpunished for many years.[34] Malicious state actors frequently manage to gain access to the information management of government organisations, NGOs and businesses.[35] Countries with an offensive cyber programme are increasing their lead. Smaller countries with above-average cyber capacities are also coming to the fore. Regional players such as Iran and North Korea are global players in terms of cyberspace.

The use of cyberspace by state actors seems to be increasing rather than decreasing.[36] An obvious explanation for this is that cyberspace is still increasing in extent and significance, which means the opportunities for exploitation are also increasing. This is evident from, for example, the continuous growth of the Internet of Things (IoT), where consumer items like lights and cars all become 'smart' and are linked to the internet, with vulnerability as the downside. This growth is visible in the development of data use and data applications.[37] As a consequence, the potential gain from cyber attacks increases.

A second explanation for the increasing use of cyberspace by state actors can be found in the developments in geopolitics itself. For many years, the global balance of power has been shifting due to the emergence of the BRICS[III] countries. This leads to more interventions, challenges and the pushing of boundaries. Both developments are autonomous, but they strengthen each other. A concrete effect of this is that states increasingly promote their interests by means of cyber operations[38], for example for political, economic and military espionage. China is unparalleled in terms of the scale on which and the range within which information is gathered. The intensity with which states use cyberspace means that digital systems, such as communication links, encryption mechanisms, but also the computers of individuals, are in the frontline, because they are constantly being tested or compromised.

Finally, cybercrime activities also have geopolitical significance because of the vague boundaries between state and criminal actors. Cybercrime groups are increasingly used by state actors for activities of national interest.[39] Such use is again influenced by current geopolitical developments. It is expected, for example, that Russia will continue to develop as a safe haven for cybercriminals as a consequence of the deteriorated relationship between the West and Russia because of the war in Ukraine. Due to the

III The acronym BRICS stands for: Brazil, Russia, India, China and South Africa.

economic sanctions, Russia will not be inclined to stand in the way of cybercriminals who attack western interests.

A cyber conflict between other countries could unintentionally lead to disruption or outages in the Netherlands. Dutch infrastructure could be exploited[40], or it could be affected by possible counter-actions, such as the disconnection of digital infrastructure by countries hit by a digital attack.

It may be the case that, in the midst of the current Ukraine crisis, phishing emails will be sent from compromised or spoofed email accounts belonging to the Ukraine government. Users are therefore advised to be alert for emails sent from Ukrainian government domains, even if they have been sent by what seem to be trustworthy senders.

During a global cyber campaign targeting security investigators, a hacked Dutch server was used. The attack campaign was specifically aimed against security investigators and very likely originated from a state actor.

A Russian state actor is hacking routers of random home users and SMEs all over the world, including a small number in the Netherlands. In doing so, the actor has formed a botnet that may be used for further cyber operations by the actor.

Geopolitical fencing about high technology and cyberspace

Cyberspace consists of all kinds of digital processes and is kept in the air by an intricate physical network of systems, data centres, hubs, cables and devices of end users.[41] Many layers of software are active on this hardware, which ultimately create cyberspace. All parts of cyberspace can be used for geopolitical control or exploitation. This can be done with hardware, with software and also with standards. Important geopolitical fencing is taking place concerning the so-called high technologies: technologies that are essential for knowledge development and innovations in a certain field, which are therefore of interest for strategic autonomy and earning capacity.

China is very keen to further develop its own semiconductor industry and to reduce its large dependence on foreign semiconductor technology for the production of high-quality chips. The ambition to become a leader in this technology has been embedded in several policy plans. To achieve the required knowledge level, China is investing large amounts in the development of the chip industry. The trade war with the US, export restrictions, a technology backlog and a lack of qualified staff are important obstacles for China to achieving their ambitions. China uses both legitimate and illegitimate resources to conquer these setbacks. The instruments at China's disposal include foreign investments, attracting highly qualified western staff, the use of digital and other espionage and importing western technology. These wide-ranging Chinese resources are used both individually and comprehensively. The combined use of these instruments increases the chance of successfully reproducing a product or technology and fits in within the overall Chinese approach of using different parties and collection methods to obtain foreign technology. The Chinese activities together form an extensive, diverse and persistent threat to the Dutch economic security interests. For the Netherlands, the Chinese efforts to obtain semiconductor technology result in risks of technology theft and undesirable end use. There is a high risk that Dutch semiconductor technology will also be used for the development of Chinese military technology. It is very likely that the current Chinese dependence on western – including Dutch – semiconductor technology will lead, for the time being, to an increase in the Chinese attempts to obtain such technology either legally or illegally.

States can do geopolitics in cyberspace in a number of different ways. When states can manage and control resources such as individual hardware components and software applications that are used for, for example, 5G communication technology, this will have an impact. That impact will be greater when states or partnerships of states are able to dominate building blocks, standards or design principles of cyberspace. This is visible, for example, in the development of cloud technology. Cloud technology involves a number of specific security issues but also has a strong geopolitical component, because the largest providers (Amazon, Microsoft and Google) are from the United States. Of course, the issues concerning big tech and those concerning specific countries will differ, but what matters here is the dependence on technology.

Dependence as such is not necessarily problematic. Moreover, countries and groups of countries will have fundamentally different views on the underlying principles of the internet. For a long time, the internet was the technology of 'tech optimism': a technology that could make information freely available to everyone and would therefore contribute to freedom, autonomy and democracy, at both country and individual level. However, the democratic or autocratic values of a system affect how the building blocks of the architecture are arranged. In autocratic countries, there has been much emphasis on limiting the freedom of information and expression, and the same technology can also be used here for monitoring, controlling and screening individuals. The ideas of authoritarian regimes about integrity and the confidentiality of data also differ from those of democratic societies. This has a fundamental impact on digital security. Digital security is not neutral. Unilateral dependence on building blocks of cyberspace stimulates the need for strategic autonomy. This need has both advantageous and disadvantageous consequences for digital security. For example, there is an area of tension between digital security and interoperability; individually developed

IV There are, of course, also positive examples, such as the standardisation of TLS 1.3 and the standardisation of cryptographic algorithms, etc.; the EU is making an important contribution to this.

building blocks must fit into the larger structure. Economies of scale, impact on the global market and worldwide standardisation are also less easy to achieve.[IV] Strategic autonomy comes at a price, but so does a lack thereof. That is why, at European level, investments are made in alternatives to existing building blocks, such as the data infrastructure program Gaia-X.[42] The challenge lies in looking for the right balance.

Cybercrime is scalable, while resilience – for now – is not

Serious, organised cybercrime has become very scalable and has therefore taken on industrial proportions in recent years in terms of victims, damage and criminal proceeds. Ransomware has proved to be a gamechanger. The term scalability is a core concept in ICT. It refers to the ability to adjust (upscale) a system or process in order to meet a higher demand. Serious cybercriminals and their service providers are primarily financially motivated and aim for maximum yields, while gratefully exploiting the options offered by the digital domain. For an important part, they upscale their processes and systems through effective cooperation and constant innovation in terms of automation. This working method forms an essential part of their revenue model and criminal market operation.

Considering the nature and growing extent of the threat of cybercrime, making and keeping the resilience chain scalable will be a fundamental challenge in the coming years. In terms of cybersecurity and combating cybercrime, achieving scalability in a technical sense is not the problem. Where possible, this is already happening. It is mainly the organisational aspects (cooperation) and the legal aspects (information exchange) that experience the most important issues and growing pains.

Maximum yields and minimum risks for attackers

Cybercrime is a form of crime that is perfect for upscaling. The digital domain is borderless by definition, which offers criminals endless opportunities to attack targets all over the world. This borderless aspect also limits the risks for cybercriminals, as it hampers investigation and persecution, which is more location dependent. Cybercriminals often know how to flawlessly exploit differences in jurisdiction by country. Moreover, some cybercrime groups operate from safe havens: countries where they are left alone by or even collaborate with the government.[43] Finally, the digital domain offers cybercriminals – as well as cybercrime providers – the opportunity to constantly optimise their processes and revenue models. Cooperation, specialisation and automation are central concepts in this respect and are closely intertwined.

Optimum attacks through cooperation and automation

Cooperation in the sense of outsourcing complex parts of the attack chain to specialist providers and the continuous automation of systems enable cybercriminals to optimise the attack chain in both quantitative and qualitative terms.[44] Criminal investigations show that cybercrime groups in the serious, organised crime segment have become professional partnerships with leaders who mainly require strong organisational skills.[45] It is no longer an exception that they have business operations that are similar to those of a legitimate SME in the high-tech sector.[46] They make pragmatic choices in terms of what they develop under their own management, which parts of the attack chain are outsourced to partners and which services are bought from specialist cybercrime providers.[47] All that matters is a maximum financial yield and minimum operational risks. Obtaining access to victim networks is often outsourced to parties specialised in this field.[48] Sophisticated resources to make maximum use of these networks are in turn bought from other criminal providers.[49]

The cybercrime ecosystem is characterised by innovation. Automation is a means to achieve a high level of efficiency in this respect. Cybercrime providers frequently use automation to provide an efficient service to as many customers as possible.[50] Suppliers of ransomware-as-a-service offer their customers control panels in which all aspects of the attack have been integrated.[51] Attackers convert the supply chain of their victims into automated attack vectors. For example, ransomware attackers managed to exploit a vulnerability of the servers of software supplier Kaseya and installed ransomware on the networks of more than 1,500 customers within a few hours.[52]

The industrial scale of cybercrime

The coronavirus crisis has accelerated the digital connectivity of society.[53] As a consequence, the opportunities for attack for cybercriminals have increased significantly.[54] This, in combination with the possibility to constantly optimise and therefore upscale the attack chain, has meant that cybercrime has taken on an industrial scale over the past few years in terms of victims, damage and criminal proceeds. For example, for several years, the group behind the Emotet botnet dominated the market of obtaining and selling on access to victim networks to ransomware groups. During an international criminal investigation in 2020-2021 aimed at taking this botnet off the air, the police acknowledged that, globally, there were 1.75 million infected IP addresses, 36 million stolen login details and more than four million compromised business and other email accounts.[55] Such large numbers of victims are no longer an exception.

Ransomware has thus developed into a cybercrime goldmine. This has increased the threat of cybercrime considerably. It was concluded in CSAN 2021 that ransomware has become a national security risk. The often insufficient level of digital resilience of victims is flawlessly being exploited, as is the opportunity to fully disrupt their – often essential – business continuity and publicise diverted sensitive information. The potential damage of such

attacks is huge, as a result of which victims are often willing to pay. This then leads to a high revenue for the cybercriminals involved. The antivirus company Emsisoft estimates that, in 2020, at least 18 billion US dollars were paid in ransoms for ransomware attacks in 10 investigated western countries. The total damage caused by these attacks is thought to amount to at least 80 billion dollars.[56]

Ransomware can therefore be rightfully called a gamechanger for the cybercrime ecosystem. It has led to cybercrime groups that have become incredibly wealthy. After the TrickBot botnet had been largely taken down at the end of 2020, the group – according to leaked internal communications – allegedly invested 20 million US dollars in recovering and improving the attack infrastructure and business operation in the following year.[58] It is thought that the Conti ransomware group recently had more than 2 billion dollars in virtual currencies.[V, 58] This means these groups are able to invest even more in effective and efficient attack processes. But the ability to survive, for example, disruption campaigns by investigative services also increases as a result of this. Both the TrickBot botnet and the Emotet botnet were back on the air less than a year after their respective takedowns.[59]

Is Dutch resilience sufficiently scalable?

Considering the nature and extent of the threat of cybercrime, making and keeping the resilience chain efficient and effective – i.e. scalable – will be a fundamental challenge in the coming years. This applies to cybersecurity and combating cybercrime by the police and the Public Prosecution Service as an integral part of resilience.

The economic rationality behind cybercrime is an important motive for the scalability of this type of crime. Cybercriminals try to generate maximum yields as effectively as possible, making use of the opportunities offered by the digital domain. Previously, it was in particular the financial sector that was attacked by, for example, banking malware, but the revenue model of ransomware is universal to such an extent that the cybercrime threat has become more sector independent.[60] In terms of resilience, this means that the potential area of attack that needs to be defended has grown.

In spite of the above conclusions, the required growth – and scalability – of Dutch resilience appears to be lagging behind. It is not only the CSAN that has been warning about this for several years. The Cyber Security Council concluded in an advisory report in 2021 that much has been invested in cybersecurity by the government, the corporate sector and science in recent years, but that there is not yet sufficient resilience everywhere in the Netherlands to withstand the increasing threats. The ability to cooperate effectively, outsource complex tasks and constantly innovate automation are important conditions for the perpetrators and service providers of cybercrime to achieve scalability. From the point of view of Dutch resilience, the report of the Cyber Security Council lists such conditions (especially in terms of effective cooperation and the exchange of information required for that purpose) as issues.[61]

Cybersecurity: cost item or investment?

From the point of view of the criminals, scalability forms an integral part of the revenue model and the criminal market forces amongst themselves. On the part of the defending side, investment in cooperation and the innovation of information security is essential in order to achieve scalable cybersecurity. However, the willingness to do so often depends more on goodwill than on economic motives.

Investments in cybersecurity are seen as a cost item and are often applied reactively, because they follow on from incidents and are not proactive investments that anticipate new threats.[62] The threat of ransomware could gradually change this, considering the increasing financial damage caused by such attacks. Scalable cybersecurity also requires innovation strength. In a preventive sense, for example, for the development and application of secure open standards and the broad availability of safe – open-source – solutions for fundamental building blocks of cyberspace.[63] Or to be able to mitigate the growing number of detected vulnerabilities effectively and efficiently.[VI] The Dutch Safety Board stated in a report in 2021 that rectifying (patching) them on this scale is no longer manageable for all organisations. The need for this is not always clear either.[64]

An increased cybercrime threat that has become less sector specific goes hand-in-hand with a growing need for cooperation and exchange of information of threats and vulnerabilities in terms of cybersecurity, both between the government and the private sector and between different sectors and between both critical and non-critical parties. With regard to these critical points, the advisory report of the Cyber Security Council identifies organisational and legal issues and growing pains. Finally, in its report from 2021, the Dutch Safety Board identified great differences in the resilience of organisations when it comes to prevention and preparation for incidents. Each organisation bears its own responsibility for this, but not every organisation has the sense of urgency, the expertise or the capacity to implement such measures adequately. According to the Dutch Safety Board, there is no collective base for increasing resilience.[65]

The challenges of combating scalable cybercrime

Because of the scale of cybercrime and the potentially large number of criminal cases, tough choices in investigation priorities must constantly be made. As a consequence of this, the police and the Public Prosecution Service mainly focus on combating the central cybercrime service providers and groups posing the greatest threat in the case of serious organised cybercrime. The increased resilience of cybercrime groups and the strongly transnational nature of cybercrime – including operating from safe havens – pose challenges for investigation and prosecution. Combating

V These amounts have not been verified. However, the police believe it is highly likely that groups like TrickBot and Conti have such budgets.

VI About 25,000 so-called security advisories are published for this purpose each year.

cybercrime therefore requires achieving scalability in the intervention method. This expresses itself in the need to be able to act on the basis of a proactive and targeted approach and to cooperate intensively with public and private partners in the Netherlands and abroad. The exchange of information is crucial for that purpose. It is questionable whether the current resources of the police and the Public Prosecution Service are still adequate to do so as effectively and efficiently as possible, which is also confirmed by recent research by the Research and Documentation Centre.[66]

The police and the Public Prosecution Service are investing in broad, data-driven control methods to counter cybercrime. These are characterised by the use of the full range of prevention, disruption, investigation and criminal prosecution.[67] Almost all investigations are based on cooperation: with national and international investigative services, public partners and the corporate sector in the Netherlands and abroad. Data-driven control means that tactical, digital and data-scientific methods and techniques are integrated into the investigations.[68] This requires the necessary adjustments throughout the criminal-law chain.[69] On the other hand, this will have the great advantage of being able to identify and develop the most effective and efficient scalable interventions in a proactive and targeted manner.

However, upscaling these interventions is currently often still difficult in practice, considering the many challenges involved. Achieving a coherent, joint international approach to a threat such as ransomware is still complex to organise because the investigative services usually focus on national interests and jurisdictions. Access to electronic evidence abroad is often hampered by slow international legal assistance. Sharing information with partners outside the EU can be hampered by the absence of the necessary agreements (adequacy decisions) between the EU and third countries. Moreover, exchanging information about threats with both public and private partners in the Netherlands and abroad is legally complex when it concerns data that is marked as personally identifiable, such as IP addresses. Bulletproof hosters offer cybercriminals secure data storage, out of the reach of investigation, so to speak, and are therefore among the most central cybercrime service providers. Relatively speaking, they use – or abuse – Dutch digital infrastructure a lot. Tackling this is difficult because of the – as yet – limited options under criminal law and a lack of clarity about the question as to who exactly is responsible for what, when it comes to hosting data. The latter is evident from the extremely complicated international constructions of so-called resellers who resell hosting packages with data that cybercriminals like to use.

Finally, identifying and informing the large numbers of victims brought to light by cybercrime investigations is still an extensive and complex task. This applies to both the police and the National Cyber Security Centre, with which the police cooperates in such cases. The process of notifying the many victims in the Emotet case confirms this, but this is also an example of how cooperation and the sharing of information between cybersecurity and partners in combating cybercrime can contribute to increased resilience.[70]

An asymmetrical situation

Cybercriminals have a number of tactical advantages in comparison with cybersecurity and combating cybercrime. A large area of attack offers attackers a broad choice, while defenders have to make a significantly greater effort to acknowledge, prevent, divert and mitigate all the attack options. As cybercriminals operate, by definition, outside the law, they will not adhere to legislation. Technical innovation and cooperation are integral parts of their joint revenue model. This collective basis has led to an optimum attack chain and a huge level of cybercrime. Achieving scalability in operations is essential for cybersecurity and combating cybercrime, but this is more difficult to accomplish. There are many options in technical terms, and these are already being explored. It is mainly the organisational aspects (cooperation) and the legal aspects (including information exchange) that pose the greatest challenges.

Market dynamics complicate controlling digital risks

Digital markets are markets where supply and demand for digital services, hardware and hardware components, software and networks come together. These markets have several unique characteristics, such as the monopoly or semi-monopoly status of certain suppliers, the high level of interconnectedness and the focus on gathering as much data as possible. Moreover, incentives for digital security are not or not always decisive in these markets. Those characteristics complicate risk control for individual citizens, organisations, sectors and countries. This creates a paradox. On the one hand, individual choices of citizens, organisations, sectors and countries can increase or reduce the risks for others. On the other, the scope for making autonomous choices for risk control is actually limited because of the lack of realistic or secure (or more secure) alternatives.

Characteristics of digital markets influence digital security

One of the characteristics of digital markets is that they are often of a monopolistic or semi-monopolistic nature. A few parties, mainly operating globally, have the largest segment of the market. This applies, for example, to suppliers of office applications or operating systems.[71] One reason for this is that the company that enters the market first and acquires many customers will have major advantages in comparison with competing companies. For customers, choosing a market leader has many advantages. It

simplifies data exchange with other organisations, staff may already be used to working with the market leader's product, etc.[72] Furthermore, the access thresholds for new companies for making similar products are high, barriers make it hard to switch (the lock-in effect) and market leaders tend to have enough money to buy up promising startups. This means that, effectively, there is a limited number of suppliers for specific services and products.

The second characteristic of digital markets is that digital services, hardware, software and networks use many other components and are therefore strongly interconnected. Different digital service providers may use the same development and monitoring tools, and hardware contains a number of components made by other suppliers. As a consequence, suppliers and customers become part of many different supply chains. Vulnerabilities in services and products of others, or their outage and exploitation, may potentially affect organisations all over the world. That interconnectedness leads to complexity, and connectivity and makes it very difficult to have an overview of all the components that are being used. That creates vulnerabilities, as became clear recently when it was announced that the Apache Log4-j software building block had a vulnerability. This building block in turn was used for many other kinds of digital processes, which were therefore also at risk.[73]

The strong focus on gathering as much data as possible is the third characteristic of digital markets. Data are not only crucial as a 'production factor' for services but also have an independent value. Because of this, providers are keen to gather data. Many services are offered to consumers free of charge, but often the providers earn money from the gathered data.[74] Even if consumers buy devices or software, it is not always transparent which data are recorded or erased, as is the case with cars or TVs. It is certainly not always clear either which data are provided for which purposes or are sold on, and to whom they are sold on.[75] Moreover, after a cyber attack, those data may become public knowledge or may be sold by criminals. There is a difference between the considerations as an individual or as a society. For an individual, it might not be a problem when personal data, for example about health, are shared in an app, but this may pose a risk to Dutch security if thousands or even millions of Dutch people do so. Organisations and state actors can make use of those data, for example, to further develop artificial intelligence or to draw up profiles of population groups.

The fourth characteristic is that incentives for digital security are not or not always decisive, while security risks may occur elsewhere. All kinds of interests are at stake in the production, supply and purchase of digital processes, hardware and software. In digital markets, it is not a foregone conclusion that parties will bear in mind the importance of digital security for themselves, others or society when weighing up the interests. The relevant parties will make decisions on the basis of costs, ease of use or the network effects.[76] In many markets, product recalls apply when the security of a product is at issue, but this is not standard practice in digital markets.[77] This means that insecure or possibly insecure digital products can circulate and be used longer than in other economic markets. Furthermore, 'security by design' is not yet the standard for providers, and introducing a new product on the market quickly may be deemed to be more important than optimising security. Also, purchasing and tendering procedures still put little emphasis on digital security, and the price, for example, can be decisive. Over the past few years, governments have been intervening in some markets to increase digital security, or they have considered doing so. In comparison with other markets, intervention in digital markets is still in its infancy.[78] While, for example, requirements are imposed on financial service providers to prevent abuse of the services, similar requirements are not common practice for hosting and access providers. Financial service providers are required by law to report unusual financial transactions. There are no requirements for reporting 'unusual digital transactions' for hosting and access providers. However, government intervention can also have unintended effects and, for example, complicate the market position of smaller parties.[79] Moreover, digital markets tend to be of a global nature, which limits options for intervention by an individual country.

Market dynamics lead to paradox: freedom of choice but also restrictions

On the one hand, market parties can make choices on the basis of their own considerations and interests, and they have a certain degree of autonomy in that respect. Those individual choices can, however, increase the risks for others and lead to collective risks, including a strong dependence on specific companies. An organisation may choose, for example, the cheapest variant of cloud services without setting any requirements for security and therefore choose the market leader. As a consequence, not only the organisation itself but also the customers of that organisation will run a higher risk of a cyber incident, without being aware of this. The data of the customers may become public knowledge as a result. When many organisations within a sector or within the Netherlands choose the market leader, this can lead to a high degree of dependence on that market leader. The opposite can also happen, if the organisation decides to opt for security or consciously decides not to use the market leader. All customers then benefit from those security measures, and the same may apply to the sector on the whole.[VII] On the other hand, the actual freedom of choice for market operators is sometimes limited by a lack of realistic or secure (or more secure) alternatives. It is usually not possible to buy a product or service and then decide not to become part of the supply chain.

VII Economists call these the negative or positive external effects. An example of negative external effects are the consequences of polluting factories for the environment, while consumers do not pay for those polluting effects when they buy the product. An example of positive external effects is a situation where a company sponsors a local association.

Coordinated and integrated risk management is still in its infancy

Coordinated and integrated risk management within and between the different levels of organisations, sectors and the national level is still in its infancy.[80] It was said above that the level of resilience in the Netherlands is not yet sufficient. It was also said that making and keeping the resilience chain scalable will be a fundamental challenge in the years to come. Digital risks do not yet have a structural place in broader risk management within and between the three levels mentioned above. Risk management is not yet a matter of course, even though a risk-based working method is instrumental for determining resilience and bringing it to the required level.[81] This requires a coordinated approach within and between the three levels. Embedding in the primary process is important at the organisational level. Where risk management already has many complications within organisations and within and between sectors, this certainly also applies at the national level.

Coordinated approach necessary to increase resilience

Without a coordinated approach – in which different approaches are compared with each other – there is a chance that unnecessary risks are taken.[82] In the development towards a mature approach of risk management at organisational, sectoral and national level, the key points to consider are that the parties involved should discuss the relevant scenarios with each other[83], that risk analyses should have a more central place in business operations[84] and that organisations should be encouraged to address risks affecting others.[85]

The fact that there are a number of different risk analysis methods hampers internal and cross-organisational discussions about risk mitigation and acceptance.[86] A shared metaphor and shared views on concepts such as 'area of attack' and 'attack routes' can be helpful in this respect.[87] However, it is likely that different dialects and paradigms will continue to exist[88] and that the conceptualisation of both risk analysis and the use of attack routes will not be comprehensive.[89] Nevertheless, the Dutch Agency Board advocates that organisations should render account for how they control digital risks unambiguously.[90]

Embedding in the primary process is important

Of course, there are many organisations that have adequately set up their risk management. Nevertheless, organisations have often not yet embedded risk analysis in their primary process or have not addressed specific aspects.[91] Without clear goals, limits, prioritisation, team composition, etc., a risk analysis is likely to become 'wobbly'.[92] The responsibility for an efficient and effective risk analysis lies with the instructing party: usually the process and risk owner.[93] However, risk analysis teams should also be acutely aware of the parameters described above and the creation of clear expectations. They also play a part in the follow-up of risk management recommendations, including a critical review of the effectiveness of measures taken.[94]

To change this, information and risk ownership as well as risk management can be integrated into the primary process as preconditions. This is done under the supervision of internal and external control bodies that not only have a traditional focus on financial risks but can also provide insight into broader digital risks, including digital risks for national security.[95] According to the Cyber Security Council and the Dutch Safety Board, this requires resources and additional legal frameworks.[96]

Mature supervision of resilience of critical processes not yet fully managed

The document *'Samenhangend inspectiebeeld cybersecurity vitale processen'* (Coordinated inspection framework of cybersecurity of critical processes) shows that much still needs to be done.[97] It shows that three out of six supervisory bodies in total have organised their supervision of cybersecurity on a solid basis. Other supervisory bodies are still working on this. That is why the cyber assessment cannot yet be used to express opinions about all critical processes. Cybersecurity not only requires the attention of organisations and supervisory bodies, but also that of the ministries. The assessment shows that the necessary steps have now been taken in terms of digitally resilient – and therefore secure – critical processes and providers in a number of areas. At the same time, much work still needs to be done in general terms, and this will never be fully completed. The supervisory bodies have the ambition to further develop the supervision of this collectively. No supervisory bodies have as yet been appointed for critical processes such as the chemical sector and digital government processes.

Risk management at national level is difficult

Risk management at national level is not yet taking place structurally and is still in its infancy. Where risk management already presents many complications within organisations and within and between sectors, this certainly also applies at national level. It is difficult for organisations, for example, to get a full breakdown of and insight into used components of hardware, software and networks. For sectors and at national level, it is often problematic to get a proper breakdown of vulnerabilities and insight into resilience. The data of a large number of citizens and organisations are now in the cloud of a very small number of parties. That leads to so-called lock-in effects and monopolisation, which involves all kinds of issues. The security of those parties tends to be much better organised than is the case elsewhere, but if it goes wrong, it will go very wrong. It is difficult to decide what that means for resilience on balance.

Reference has already been made to the underlying problem that parties – both providers and customers – make choices autonomously, without having to experience themselves their impact on others. The problem is that security is often not included in the price paid by organisations and individuals.[98] 'Polluters' do not pay for the 'pollution' that is caused.[99] Of course, this is a complex issue, as it is difficult to measure security. But as is shown by product recalls and liability claims, there are certainly steps that can be taken to pass on the costs of security

problems to those who are in the best position to do something about them.

Another reason why risk management at national level is still in its infancy is that concepts, methods and techniques are primarily tailored to the level of individual organisations. As far as is known, they do not exist for risk management at national level. Questions such as 'How digitally secure is the Netherlands?' are asked regularly, but it is virtually impossible to answer them. A new vulnerability may be discovered in an hour's time for something that is secure now. Moreover, a level of 100% security is not realistic. A better question would be, 'How resilient is the Netherlands?' Nevertheless, defining a desirable level of resilience is far from easy and is not easy to measure. A detailed conceptual framework for this does not exist. That resilience should certainly not be limited to preventing cyber incidents but should also focus on their discovery, limiting their damage and making it easier to recover from such incidents.

Articles have recently been published in scientific literature about considering the risks in different ways, for example by looking at complex adaptive systems. Many parties play a part when it comes to the resilience of cyberspace on the whole. Clearly, the possibilities open to the Dutch government to increase the resilience of cyberspace are limited. It is also difficult to comprehend the risks for cyberspace on the whole and the impact of this on society. This makes it difficult to assess the risks and decide whether or not any measures should be taken to control those risks. It is also not immediately clear which parties have the incentives, possibilities and willingness to limit the risks.[100]

Restrictions in digital autonomy also restrict digital resilience

Restrictions in digital autonomy apply for European countries and the Netherlands (hereafter: the Netherlands). These also entail restrictions for digital resilience. The fact that this resilience is under pressure is due to various causes, which are related to the strategic themes described above. Those causes reduce the options to influence and make choices in terms of the digital resilience of the Netherlands and how to control this resilience.

Digital autonomy is a complex, wide-ranging concept that affects the broader national interest in terms of the economy, society and democracy.[VIII] It includes the ability and resources the Netherlands has to make decisions independently about further digitisation and the required level of digital resilience. This concerns, for example, the degree of control of the use and architecture of critical digital systems and the dependence of the Dutch government on two global companies to make available government apps. This also concerns the influence the Netherlands can have on developments that affect security and the possibilities to choose from safe or safer alternatives.

Digital autonomy is under pressure

The Cyber Security Council states that the ability of the Netherlands to make decisions autonomously is under pressure from three directions:

1. Cyber threats will continue to increase.
2. The geopolitical tensions between the US and China are continuing to increase.
3. Society is becoming more and more dependent on the digital infrastructure controlled by a small number of dominant foreign market operators.[101]

Underlying causes and vulnerabilities in our digitized society can only be influenced to a limited extent by the Netherlands or by Europe. Attackers can operate from different countries, use the infrastructure of different countries, create victims in many countries and do not comply with legislation and regulations. This not only makes it more complicated for individual citizens, organisations and countries to increase their resilience against this, but also, as said above, makes it more difficult for intelligence and investigative services to combat this.

The geopolitical context also limits digital autonomy, and the Netherlands alone can do little to change this. As is the case in other countries, the Netherlands is facing the consequences of the structural and intensive use of cyberspace by states and the geopolitical fencing about high technology and the underlying standards of these technologies.

The unique characteristics of digital markets are also putting the digital autonomy under pressure. A consequence of this is, for example, that many digital processes largely depend on the services, infrastructure and ecosystem of a limited number of dominant foreign market operators. According to the Cyber Security Council, data of virtually all European companies and citizens are now in the cloud of American tech companies in particular.[102] This therefore also involves control by other countries, which apply different rules about privacy and the issue of data. The Cyber Security Council even uses the term 'tech colonialism'.[103] Realistic or safe (or safer) alternatives to digital services, hardware, software and networks are sometimes barely available. Moreover, the negotiating position with large global companies is limited.[104] The Dutch influence on all this is limited, but it does form a risk component.

In addition to the abovementioned causes that are putting the digital autonomy under pressure, the Netherlands alone has little influence and does not have any alternatives to cyberspace.

VIII The Cyber Security Council defines digital autonomy as 'strategic autonomy in the digital domain'. It describes strategic autonomy as 'a means to acquire and maintain sovereignty; it consists of the ability and resources to make and implement decisions about essential aspect of the long-term future of the economy, society and democracy.'

Violation of cyberspace is a risk. Digital processes can have many ramifications to other countries with very different legal regimes, standards and values. This lack of transparency is due to the basic design of the internet: data are led automatically via the shortest route, with as few intervening networks as possible. That route can be adjusted automatically when, for instance, there is a fault somewhere. This feature improves efficiency, but it also means that the routing and used networks are unknown. This causes a so-called 'black box' with a lack of information.[105] While some countries aim for so-called interoperability and free internet traffic, there are also a number of countries that wish to regulate incoming and outgoing internet traffic. Such regulation also affects foreign organisations that operate in or with these countries and therefore may impact on Dutch organisations. These Dutch organisations cannot influence this process, and there is frequently a lack of transparency.

Limitations in autonomy affect resilience

The combination of the causes and consequences mentioned above limit the extent to which the Netherlands can influence certain developments, as well as the options for realistic or safe (or safer) alternatives. All this limits the capacity and resources to reduce relevant risks to an acceptable level, to prevent cyber incidents and to detect cyber incidents when they have occurred, in order to limit the damage and facilitate recovery.

Every system using Log4j was vulnerable: a malicious actor could remotely execute random code

4 Annual review

Review of the most important cyber incidents

On the basis of its operational and coordinating task, the National Cyber Security Centre (NCSC) has produced a review of the most important cyber incidents that occurred in the period from April 2021 to March 2022. It used the information from previously published NCSC products for this purpose, such as the Monthly Monitor, as well as open sources. The focus is on incidents that have affected the Netherlands or that could affect the Netherlands. They illustrate the importance of the strategic themes identified in the previous chapter, which are relevant to digital security in the Netherlands.

2021

April 2021

Backdoor found in software development tool Codecov: users of the software development tool Codecov may have been the victim of a supply chain attack.[106] On 31 January 2021, an attacker managed to adapt the 'Bash Uploader' script, on the basis of a leaked key for a Google Cloud Storage account of Codecov. The 'Bash Uploader' script is normally only used to upload test results from the software developer's system to the Codecov servers. The backdoor meant that, in addition, login data were diverted to the attacker. The backdoor was detected by Codecov on 1 April 2021, when a user reported that the script version supplied via Codecov's web server did not correspond to information from the documentation. Investigators estimate that the attackers may have hit hundreds of Codecov's customers.[107]

Active exploitation of VPN vulnerabilities by actors: on 20 April 2021, PulseSecure stated in a blog post that vulnerabilities in the Pulse Connect Secure Appliance were being actively exploited.[108] The American Cybersecurity and Infrastructure Security Agency (CISA) announced that these vulnerabilities were actively being exploited.[109] Four vulnerabilities were concerned, including three older ones, for which security updates were published in 2019 and 2020. The fourth vulnerability, identified as CVE-2021-22893, concerned a zero-day vulnerability, for which there was no solution in the first instance. A security update was published for this vulnerability in early May 2021.[110]

Police remove Emotet malware from one million infected PCs: during the international police operation 'LadyBird', led by Europol, the police succeeded in taking over the Emotet botnet in January 2021. Partly because of the hacking authority of the police, the Emotet network could be further analysed and deactivated. In April 2021, a software update for all infected systems was put onto the Dutch servers.[111] This update was uploaded automatically by the infected systems, after which the Emotet infection was put into quarantine. The NCSC, in cooperation with the police and the Public Prosecution Service, informed Dutch victims whose accounts had been infected.

May 2021

American Colonial Pipeline hacked: on 7 May 2021, the oil pipeline company Colonial Pipeline became the victim of a ransomware attack.[112] Colonial Pipeline decided to shut down its operations to prevent the possible further spread of the ransomware. This had major consequences for fuel supplies on the east coast of the United States. Indirect consequences for society included the unrest that followed and people panic buying fuel. Operations were restarted after six days.[113] The FBI confirmed in a press release that the ransomware group Darkside was involved.[114]

Ransomware attack on Irish health service: on 14 May 2021, the Irish Health Service Executive (HSE) was hit by a ransomware attack. It was decided to take the IT systems offline to prevent any further spread.[115] This had consequences for the care provided to patients in a number of hospitals and institutions. It was reported on Twitter that there were either delays or appointment cancellations. The ransomware concerned was Conti ransomware. The malware entered the system via a phishing email.[116] The US Department of Health reported that 80% of the IT environment had been encrypted: 2,800 servers and 3,500 work stations.[117] In the same month, the Irish Department of Health was also attacked twice, after which it also temporarily had to close its services.[118]

Two-year targeted cyber attack on Belgian Ministry for Home Affairs: the Belgian Federal Public Service (Ministry) for Home Affairs has been the victim of a digital attack.[119] In March 2021, Microsoft reported that the actor HAFNIUM was exploiting vulnerabilities in Microsoft Exchange.[120] Following this news, the Centre for Cyber Security Belgium decided to start an investigation. This investigation concluded that backdoors had been installed in the Ministry's network. Further monitoring by the Centre brought to light that suspect activities had been taking place on the Ministry's network since April 2019. After this discovery, the vulnerability in the network was rectified, important sensitive information was secured and the systems were cleaned up. The Centre for Cyber Security Belgium has indicated that this concerns a very complex and sophisticated attack, probably carried out for espionage purposes.[121]

June 2021

Nobelium spear-phishing campaign (APT29) identified in the Netherlands: a spear-phishing campaign attributed by Microsoft to Nobelium (APT29) was also identified in the Netherlands.[122] The campaign was identified at a number of target group organisations of the NCSC via the National Detection Network. The threat mainly targets government organisations and NGOs, and specifically divisions involved in international cooperation and diplomatic relations, such as embassies.[123] The emails from this campaign are of a high quality and address current affairs. A recurring feature of this campaign is systems being infected with Cobalt Strike.

Ransomware attack, municipality of Liège: on 21 June 2021, the Belgian city of Liège became the victim of a targeted attack with ransomware.[124] As a consequence, municipality systems became partly inaccessibly, and the services provided to citizens were severely disrupted. The population records and associated services (births, funerals and marriages), for example, were not available. The Wallonian radio and television broadcasting service RTBF and RTC Tele Liège claimed that the criminals were demanding a ransom and speculated that Ryuk ransomware was involved.[125]

Hacking attempt on 'Testing for Access': on Friday 25 June 2021, a hacking attempt took place on the Testing for Access system.[126] The attempt led to technical problems. Emails with test results arrived later: too late for many people to attend the reopening of nightclubs that evening. The organisation Testing for Access organised COVID-19 access tests at locations throughout the Netherlands on behalf of the government.

July 2021

Kaseya supply-chain attack causes ransomware victims all over the world: on 2 July 2021, a global ransomware attack took place, affecting Managed Service Providers (MSPs) and their customers.[127] Some people in the Netherlands were also affected.[128] The criminals behind REvil ransomware were exploiting two vulnerabilities in Kaseya VSA. Kaseya was already aware of one of these vulnerabilities thanks to the Dutch Institute for Vulnerability Disclosure (DIVD), which informed Kaseya of this and five other vulnerabilities via a coordinated vulnerability disclosure process.[129] The other exploited vulnerability concerned an as yet unknown zero-day vulnerability. The NCSC issued advice on how to detect the vulnerabilities in systems and how to rectify them.[130] The CSIRT for Digital Service Providers (CSIRT-DSP) actively informed users of Kaseya software in its target group about this. On 13 July, REvil disappeared from several fora, and the website REvil used to communicate with victims also disappeared. By then, Kaseya had a decrypter, which it made available to affected organisations. The attackers demanded 70 million dollars, but Kaseya claims not to have paid for a universal decrypter.[131]

Pegasus spyware once again demonstrates the vulnerability of mobile devices to the general public: a consortium of 17 news organisations published a study in July, claiming that dissidents, human rights lawyers, activists, journalists and politicians all over the world were the target of espionage activities by means of Pegasus software.[132] It was said that the software, developed by the Israeli NSO Group, provided the attacker with access to the content of iPhones and Android smartphones, without any interaction with the victim. This therefore concerns a so-called zero-click attack. Following these revelations, Israel set up a task force to investigate whether any policy changes are required in terms of the export of such software.[133] The NSO Group claims that it only sells the software to states for the purpose of combating crime and terrorism.

DDoS attacks on DigiD supplier disrupt Municipal Health Service websites: on 21 July, the websites of the Municipal Health Service could not be accessed. This was due to the fact that the supplier of DigiD experienced three DDoS attacks within 24 hours.[134] It was impossible to log in with DigiD on several of the Service's websites. It was impossible to arrange an appointment for a test or vaccination. It was also impossible to view test results. A number of branches of the Service had to revert to call centres to notify people of their test results and book test appointments. The DDoS attacks were ultimately warded off by the National Internet Providers Management Organisation.

August 2021

PKIoverheid stops issuing publicly trusted web server (SSL/TLS) certificates: the State Secretary for the Interior and Kingdom Relations has decided not to launch a new publicly trusted root, following the expiry of the publicly trusted Domain Server CA2020.[135] According to an evaluation, the Dutch government was the only EU country that issued publicly trusted (SSL/TLS) certificates in 2021. In other countries, this is done by private companies. It is as least as easy for market operators – and cheaper – to issue the certificates as it is for the government. The issue of publicly trusted (SSL/TLS) certificates by PKIoverheid is therefore no longer necessary. Organisations that were using such certificates had to look for an alternative.[136] The NCSC has issued several publications with recommendations about this subject.[137]

Attack of several weeks on two Dutch hospitals: the hospitals in Zutphen and Apeldoorn of Gelre Ziekenhuizen were attacked by cybercriminals over a period of three weeks.[138] The attacks were identified at an early stage. Malicious individuals managed to gain access to one mailbox of an employee in a medically supportive role. For safety reasons, it was not explained how the criminals had gained access to this mailbox. It is unknown who was behind the attacks, but apparently it originated from different countries.

Province of Gelderland hacked: around 18 August 2021, the staff files of 1,400 employees of the province of Gelderland were stolen during a cyber attack. The attack was aimed at an ICT supplier of the province. Gelderland did not appear to be the main target, as the cybercriminals responsible did not contact the province. All the employees affected were given the opportunity to get a new passport at the province's expense.[140]

Regional Training Centre Mondriaan hacked: on 21 August 2021, Regional Training Centre Mondriaan discovered that it had been hacked.[141] According to an investigation, the attackers gained access on 10 August by means of brute-force and other attacks. Business information, general personal data and sensitive personal data were stolen.[142] In the night of 21 August, all systems of the 27 schools were found to have been encrypted. The educational institution decided to make all its systems inaccessible and to build up its entire ICT landscape from scratch. Russian cybercriminals subsequently demanded a ransom of four million euros.[143] Following consultation with the Ministry of Education, Culture and Science and other parties, Regional Training Centre Mondriaan decided not to pay this ransom.[144] The stolen data were published on the dark web one week later.

September 2021

DDOS attacks on CoronaCheck app: on Friday 25 September 2021, the COVID-19 passport was introduced.[145] In the evening, the app crashed, partly because of the large volume of traffic and partly because of several DDoS attacks on the underlying servers. The app requires an internet connection to retrieve the code. The connection with the crashed servers was either not established at all or very slowly.

October 2021

Ransomware attack at VDL: the industry group VDL Group was hit by a digital attack in the night of 6 October 2021.[146] VDL Group consists of 105 companies in the Netherlands, Belgium and other countries. One of the consequences of the attack was that part of production at car manufacturer Nedcar in Born came to a standstill. Companies that depend on VDL Group as a supplier, such as Philips and ASML, were also affected.[147] A month after the attack, VDL had fully recovered from the cyber attack. Thanks to backups, the company was able to recover the production environment from safe environments.[148]

Google warns 14,000 users against hacking attempts by Russian government: at the beginning of October, Google warned 14,000 users that they were the target of a focused Russian phishing campaign. According to Google, this involved APT 28, also known by the name Fancy Bear. According to a spokesperson, as much as 86% of Google's alerts in September concerned phishing campaigns by this hacker group. The company ensured users that the campaigns had been blocked: the sent emails were automatically marked as spam. Google encourages the warned users to take extra security measures.[149]

November 2021

Ransomware attack at retail business MediaMarkt: on 9 November 2021, MediaMarkt became the victim of a Hive ransomware attack.[150] As a result, it was only possible to buy products physically in branches anywhere in Europe. Collection of orders, exchanges and returns were no longer possible. The criminals behind the attack demanded a ransom of 240 million dollar.[151] MediaMarkt did not pay the ransom in the end and was able to recover backups.[152]

Cyber attack on Heijmans: on Sunday 14 November 2021, hackers attempted to gain access to the internal systems of the construction firm Heijmans by means of a major attack. The attack lasted 24 hours, during which the attackers tried to break into about 1,300 accounts.[153] As the accounts were blocked after three attempts, they could no longer be accessed by either hackers or staff. Because of this security measure, Heijmans did not suffer any harmful consequences.

Digital attack on large Danish wind turbine producer: Vestas, a Danish company and one of the largest producers of wind turbines, was hit by a ransomware attack on 19 November.[154] Following this, the company disabled several of its IT systems. According to Vestas, there are no indications that customers and partners have also been hit via the supply chain. At the end of November, the company indicated that nearly all the IT systems were available and active again.[155] The wind turbines had apparently not been affected by the attack either.

December 2021

Pegasus spyware found on iPhones of US diplomats: at the beginning of December 2021, espionage software was found on the iPhones of at least nine employees of the US Department of State.[156] The officials concerned were working in Uganda or were working on files related to this country. The espionage software was detected after Apple had informed all affected systems (and therefore users) of the FORCEDENTRY exploit in November.[157] Apple sued NSO group, the Israeli maker of Pegasus software, at the end of November. The legal documents confirmed that NSO Group had used FORCEDENTRY to put their Pegasus spyware on mobile phones.

Digital break-in at technology supplier of Ministry of Defence and the police: at the beginning of December 2021, a number of sensitive documents of the company Abiom were put online by the ransomware group Lockbit 2.0.[158] An article about this was published in Dutch newspaper De Volkskrant, which sparked concern about the sensitive information that was now public. Among the products supplied by Abiom are handheld transceivers for the C2000 network of the police.[159] It later turned out that the company had been the victim of a ransomware attack at the end of October.[160] The attack was spotted quickly: the potentially infected systems were isolated and the company was operational again after 48 hours on the basis of backups.[161] In consultation with the police, the company decided not to contact the ransomware group.[162]

Vulnerabilities in Apache Log4j: on 10 December 2021, the NCSC issued security advice on a vulnerability in Log for Java (Log4j), in which it warned about potential major damage and advised organisations to rectify the vulnerabilities as quickly as possible.[163] Log4j is a Java library (software program) for organising logging in Java applications. Every system using Log4j turned out to be vulnerable: a malicious actor could perform a random code remotely. An exploit code was published immediately, and there also turned out to be several vulnerabilities.[164] The first updates that had been issued by Apache turned out to be inadequate to mitigate 'new' vulnerabilities. As Log4j is used in a large number of systems all over the world, this vulnerability caused a great deal of concern. The Chamber of Commerce decided to take its systems offline as a precaution.[165] The NCSC published a list of vulnerable applications on GitHub and gave advice to organisations on how to reduce the risk of exploitation. The most up-to-date general perspective for action was published on the NCSC website.[166] Furthermore, a joint webinar was organised by the NCSC and the Digital Trust Centre, with the aim to provide general information to Dutch organisations. In the end, exploitation of this vulnerability by both state actors and cybercriminals was identified.[167] These attacks have occurred in the Netherlands as well as abroad.[168] The Belgian army, for example, was hit by a cyber attack via the Log4j vulnerability. This meant the army could not communicate with the outside world by email for more than a month: this lasted until 11 January. Several other servers were not back online until February.[169]

2022

January 2022

Digital attacks on Ukraine: The number of digital attacks on Ukraine increased in January 2022.[170] The NCSC published a timeline on its website of the different attacks that could be related to the war.[171] On 14 January, the Security Service of Ukraine (SSU) issued a statement about an attack on various government websites. Messages were put on the websites, in which it was stated in threatening language in Polish, Ukrainian and Russian that personal data of Ukrainian citizens had been stolen and that citizens should 'prepare for the worst'.[IX,172] There may have been a supply-chain attack on the supplier maintaining the websites.[173]

On 15 January, Microsoft published a blog about WhisperGate malware, also called WhisperKill. This malware was used against a number of government organisations and other organisations in Ukraine.[174] WhisperGate is a form of wiperware that masquerades as ransomware: the difference is that there is no way in which damaged systems or files can be recovered. What this amounts to is that files are deleted or the operating system is disabled.[175] WhisperGate malware cannot spread without human intervention.

On 26 January, CERT Ukraine (CERT-UA) published part of the investigation into both the defacements and the malware attack.[176] This investigation identified major similarities between WhisperGate malware and WhiteBlackCrypt ransomware. According to CERT-UA, this shows that it was the attacker's intention to make it seem as if Ukraine itself was behind these cyber attacks.[177] In addition to the timeline of the different attacks in relation to the war, the NCSC has published guidance and a perspective for action for organisations in the Netherlands.[178]

Digital attacks on terminal operators in Germany, the Netherlands and Belgium: since 29 January 2022, several digital attacks on storage and transshipment sites for oil and other products of the companies Oiltanking, SEA-Invest and Evos have been reported.[179] The attacks appeared to have been aimed at the companies' IT systems. This meant that logistic processes were disrupted or delayed.[180] In Germany, it was impossible to deliver supplies to more than 200 filling stations, and Shell had to divert to other terminals to guarantee stocks.[181] According to the German Federal Office for Information Security, the systems of Oiltanking had been compromised by BlackCat ransomware.[182] This is a sophisticated ransomware family that has been active since the end of 2021. BlackCat uses a ransomware-as-a-service model and seems to have created victims in different countries and sectors.[183] SEA-Invest (responsible for loading and unloading food products like fruit) in the port of Antwerp and the oil terminals of Evos in Terneuzen and Ghent experienced the consequences of a digital attack at the beginning of February.[184]

IX Such an attack, in which a website is defaced, is also called 'defacement'.

February 2022

Digital attacks on Ukraine: On 15 and 16 February 2022, a number of digital attacks took place on different targets in Ukraine.[185] These included DDoS attacks. The Ministry of Defence and two national banks in Ukraine were hit. According to the NCSC-UK, it is highly likely that the Russian military intelligence service was behind these attacks.[186] On 15 February, an SMS campaign also took place, distributing the message that ATMs had a technical fault.[187] Official channels in Ukraine have indicated that this was disinformation. According to them, there were no such faults.

Dutch digital infrastructure used for DDoS attacks on Ukrainian websites: According to investigators, Dutch digital infrastructure was used for DDoS attacks on various Ukrainian websites.[188] Attackers used Dutch servers to control the botnet that generated the DDoS attacks. It had already been concluded in CSAN2020 that it is attractive for attackers to exploit Dutch IT Infrastructure, as this is of a high quality and it is relatively simple to hire IT capacity.[189]

Logistics giant Expeditors brought to a standstill globally by cyber attack: The company Expeditors, which provides logistics and customs services for air and sea cargo all over the world, was hit by a targeted cyber attack in February. This affected business operations, and services could not be performed for several weeks.[190]

Russian secret service infected Dutch routers: on 23 February 2022, several authorities warned that 'small office and home office' routers of the brand Watchguard and other brands had been compromised.[191] These SOHO routers had been hacked by the actor APT Sandworm, which is affiliated to the Russian military intelligence service GRU. A week later, the Military Intelligence and Security Service revealed that it had investigated this actor. The investigation also revealed that a small number of routers in the Netherlands of random victims who do not seem to have any connection with the Ministry of Defence, the government or critical sectors had also been hacked.[192] The routers form part of a botnet, which can be used for different purposes, such as digital espionage, sabotage or manipulation. Following the GRU hack, the NCSC published a target group message with security advice on the NCSC website.[193]

Appendices

Annex 1

Rationale behind the creation of the CSAN

The Cyber Security Assessment Netherlands has been drawn up by the NCTV and the NCSC. It is defined annually by the NCTV. It gratefully makes use of the information, insights and expertise of government services, organisations in critical processes, science and other parties. Completing the CSAN consists of three stages:

1. Analysis

The NCTV collects and analyses relevant information about incidents, trends and shifts in terms of the three key aspects of interest, threat and resilience. For the purpose of CSAN 2022, it was explicitly checked whether the assessment set out in CSAN 2021 was still up to date. That is the reason why Chapter 2 has been included. CSAN 2022 contains the basis for the new cyber strategy of the Dutch government. To form that basis, the following questions were formulated:

1. What have been the fundamental factors that have influenced digital security in the Netherlands since the year 2000?
2. Which substantive theme will influence the digital security of individual companies and organisations in the Netherlands in the next four to six years?
3. Which substantive theme will influence the digital security of Dutch society in the next four to six years?

During the analytical stage, these questions were put to external partners. In November 2021, an expert consultation took place in writing, in which government departments, organisations involved in critical processes, science and other parties were requested to provide input. The three analytical questions were answered on the basis of all the gathered information. This led to the formulation of the five themes explained in Chapter 3.

2. Writing and peer review

Once the analytical phase was completed, the draft CSAN was written by authors within the NCTV (Essence, Chapter 2 and parts of Chapter 3), the NCSC (parts of Chapter 3 and the Annual Review) and the police (part of Chapter 3). The whole text was assessed by colleagues within the NCTV and the NCSC several times. The NCTV is responsible for the final editing of all the chapters.

3. Validation

The CSAN undergoes an extensive validation process, in which the draft text is presented to external partners for comments. These are the same partners who were asked to provide input during the analytical phase. After processing all the comments, the definitive text is prepared and adopted by the NCTV. Following the publication of the CSAN, an extensive internal and external evaluation takes place. The collected feedback is processed in the CSAN procedure of the following year.

Annex 2:

Sources and references

1 Since CSAN 2021, a revised conceptual framework has been used, in the creation of which the authors have made grateful use of the following document: J. van den Berg, 'A basic set of mental models for understanding and dealing with the cybersecurity challenges of today', Journal of Information Warfare 19:1 (2020). https://www.jinfowar.com/journal/volume-19-issue-1/basic-set-mental-models-understanding-dealing-cybersecurity-challenges-today

2 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

3 'Nationale Veiligheid Strategie 2019', NCTV, juni 2019; 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021. The National Security Strategy will be updated in the Nationwide Security Strategy in 2022. This CSAN is still based on the National Security Strategy from 2019.

4 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

5 AIVD, 'Tweede Kamer geïnformeerd over prioriteiten en accenten AIVD voor 2022', 17 december 2021. https://www.aivd.nl/actueel/nieuws/2021/12/17/tweede-kamer-geinformeerd-over-aivd-prioriteiten-en-accenten-voor-2022.

6 'China: Declaration by the High Representative on behalf of the European Union urging Chinese authorities to take action against malicious cyber activities undertaken from its territory' - Consilium (europa.eu).

7 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

8 https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

9 See, for example, M. Buningh, 'Als de keten zelf de zwakste schakel is: cybersecurity in de supply chain', TNO, december 2021.

10 N. van der Voort, 'Cyber-jaaroverzicht 2021 en een vooruitblik op 2022', Emerce Security, 31 december 2021, https://www.emerce.nl/achtergrond/cyberjaaroverzicht-2021-vooruitblik-2022; Mark Buningh, 'Als de keten zelf de zwakste schakel is: cybersecurity in de supply chain', TNO, december 2021.

11 On behalf of the National Cyber Security Centre, the Netherlands Organisation for Applied Scientific Research has carried out preliminary research into the risks and issues concerning ICT supply chains. This research shows that Dutch organisations have very different ideas about the risks and that their views about ICT supply chains do not coincide due to the high level of complexity of digital chains. https://www.ncsc.nl/onderzoek/onderzoeksresultaten/grote-verschillen-in-benadering-risico%E2%80%99s-ict-supply-chains-bij-nederlandse-organisaties.

12 https://www.ncsc.nl/onderwerpen/ransomware/wat-is-ransomware

13 Check Point, 'Cyber attack trends: mid year report 2021', 2021, p. 8-9. https://securitydelta.nl/media/com_hsd/report/443/document/cyber-attack-trends-report-mid-year-2021.pdf.

14 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

15 See, for example, CrowdStrike, '2021 Global Threat Report', 2022, p. 22-23; IBM, 'X-Force threat intelligence index 2022', 2022.

16 CSAN 2021 describes three scenarios involving the outage and exploitation of the cloud (Chapter 8). You can use them to check within your organisation whether events such as those described in the scenarios could occur in your organisation, which preparatory measures you have put into place and how you can improve your cloud strategy.

17 Research has shown that many organisations experience problems with detecting and combating security incidents in their cloud environment. https://www.ncsc.nl/onderzoek/onderzoeksresultaten/huidige-standaarden-op-het-gebied-van-cloud-incident-bestrijding

18 https://www.trouw.nl/binnenland/oekraine-vraagt-hackers-om-hulp-maar-is-digitaal-activisme-wel-zo-slim~bfed0e93/

19 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

20 Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', december 2021, p. 122.

21 Cyber Security Raad, 'Integrale aanpak cyberweerbaarheid', april 2021; Onderzoeksraad voor Veiligheid, 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix', december 2021, p. 121.

22 'Staat van de rijksverantwoording 2021. Goed beheer is het halve werk', Algemene Rekenkamer, mei 2022, p.31, 40.

23 'Handreiking Cybersecuritymaatregelen', NCSC, juni 2021.

24 Inspectie Justitie & Veiligheid, 'Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021', 2021.

https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021.

25 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.

26 Annex 1 (Explanation) describes the method followed to select the themes.

27 The Netherlands is fourth in de Digital Economy and Society Index of the most digitised EU countries, produced by the EU. The index considers 1) Connectivity, 2) Human Capital, 3) Use of Internet, 4) Integration of Digital Technology and 5) Digital Public Services. https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

28 An exception to this are some process support systems, where there are hesitations in terms of far-reaching digitisation from a security perspective.

29 This concerns the transition to a different energy supply system, in which fossil fuels have been largely replaced by sustainable energy sources such as solar and wind energy. See, for example, https://www.agentschaptelecom.nl/actueel/nieuws/2021/07/12/kwetsbare-digitale-infrastructuur-vormt-risico-voor-energietransitie

30 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021.

31 https://www.onderzoeksraad.nl/nl/page/4980/pati%C3%ABntveiligheid-bij-ict-uitval-in-ziekenhuizen

32 See also the analysis of the influence of geopolitics for threats and interests in CSAN 2021: 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021, hoofdstuk 6, p. 39-42.

33 D. Koh, 'The geopolticics of cybersecurity', The diplomat.com, 9 december 2020.

34 A well-known example is the successful supply chain hack in Solarwinds Orion, detected on 14 December 2020, which compromised in particular federal government organisations in the US (State Department, Homeland Security, National Nuclear Security Administration) for a considerable period of time.

35 'Dreigingsbeeld Statelijke Actoren', AIVD, MIVD en NCTV, februari 2021.

36 Clearly, geopolitics is not the only reason for the activities of state actors. Many attacks serve a domestic purpose, such as providing insight into the travel data of individuals who pose a risk to the domestic security of the relevant state.

37 Papieren acceptgiro verdwijnt na ruim veertig jaar op 1 juni 2023 (After 40 years, paper Acceptgiros are set to disappear on 1 June 2023) – Security.NL.

38 'AIVD jaarverslag 2020', 29-04-2021, p. 8-10.

39 See: 'The blurry boundaries between nation-state actors and…', Intel471.com.

40 See, for example, the news item in De Volkskrant of 3 March 2022, in which the Military Intelligence and Security Service declared it was carrying out disruptions on compromised Dutch private routers, which had been included in a botnet. 'MIVD verstoort Russische digitale aanval op routers van Nederlandse burgers' (Military Intelligence and Security Service disrupts digital attack on Dutch citizens' routers), De Volkskrant.

41 For a further description of the term cyberspace, see 'Cyber Security Assessment Nederland 2021', National Coordinator for Security and Counterterrorism, June 2021, Chapter 5.

42 See: 'Gaia-X: A Federated Secure Data Infrastructure'.

43 See also 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021, p. 9; Insikt Group: 'Dark Covenant: Connections Between the Russian State and Criminal Actors', 09-09-2021.

44 D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic', European Law Enforcement Research Bulletin, (SCE 5), 2022, 45-60. https://doi.org/https://doi.org/10.7725/eulerb.voiSCE%205.475

45 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html; https://www.politie.nl/nieuws/2021/oktober/29/11-ransomware-bende-opgerold-wegens-vernietigende-aanvallen-op-kritieke-infrastructuur.html; https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

46 https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

47 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019; https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve.

48 https://ke-la.com/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/

59 https://securelist.com/russian-speaking-cybercrime-evolution-2016-2021/104656/

50 E. van De Sandt, 'Deviant Security: The Technical Computer Security Practices of Cyber Criminals', 7 mei 2019;

51 https://therecord.media/an-alphv-blackcat-representative-discusses-the-groups-plans-for-a-ransomware-meta-universe/

52 https://www.ncsc.nl/actueel/nieuws/2021/07/03/schakel-kaseya-vsa-uit-mogelijke-ransomware-aanval-via-leverancier sketen-gaande; https://www.ncsc.nl/actueel/nieuws/2021/juli/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya; https://www.datacenterknowledge.com/security/kaseya-ransomware-attack-wakeup-call-msp-reliant-it-shops; https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware

53 'Cybersecuritybeeld Nederland 2021', NCTV, juni 2021.
54 'National Cyber Strategy 2022. Pioneering a cyber future with the whole of the UK', 2021; D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending', School of Law, 2021, University of Leeds.
55 https://www.politie.nl/nieuws/2021/januari/27/11-internationale-politieoperatie-ladybird-botnet-emotet-wereldwijd-ontmanteld.html;
https://www.security.nl/posting/689433/Emotet-checker+politie+bevat+inmiddels+4%2C2+miljoen+e-mailadressen
56 D. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending', 2021, School of Law, University of Leeds.
57 https://www.sentinelone.com/labs/anchor-project-the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/; https://www.wired.com/story/trickbot-malware-group-internal-messages/
58 https://www.cyberscoop.com/ransomware-gang-conti-bounced-back/
59 https://research.checkpoint.com/2021/when-old-friends-meet-again-why-emotet-chose-trickbot-for-rebirth/
60 Zie o.a.: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021. Incidentmeldingen en aangiften die de politie ontvangt bevestigen dit beeld.
61 CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid', 6 april 2021.
62 S. Zeijlemaker, 'Unravelling the dynamic complexity of cyber-security: Towards identifying core systemic structures driving cyber-security investment decision-making', maart 2021. Radboud University;
https://www.engineersonline.nl/nieuws/id35289-bedrijven-moeten-niet-meer-maar-slimmer-investeren-in-cybersecurity.html
63 https://csrc.nist.gov/publications/detail/white-paper/2018/09/07/economic-impacts-of-the-advanced-encryption-standard-1996-2017/final
64 Onderzoeksraad voor Veiligheid: 'Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix', 16-12-2021.
65 Onderzoeksraad voor Veiligheid: 'Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix', 16-12-2021.
66 WODC-rapport 'Opsporen, vervolgen en tegenhouden van cybercriminaliteit', 18-10-2021.
67 Politie jaarverantwoording over 2020.
68 Erik van de Sandt, Arthur van Bunningen, Jarmo van Lenthe en John Fokker: Towards Data Scientific Investigations: A Comprehensive Data Science Framework and Case Study for Investigating Organized Crime and Serving the Public Interest (White paper, March 2021
69 Position paper Dienst Landelijke Recherche: 'Het antwoord van de Dienst Landelijke Recherche op de georganiseerde criminaliteit', 12-10-2020.
70 Politie jaarverantwoording over 2021.
71 'Amazon, Microsoft lead 40% growth of IaaS public cloud services market in 2020: Gartner', ZDNet, 28-06-2021 https://www.zdnet.com/article/amazon-microsoft-lead-40-growth-of-iaas-public-cloud-services-market-in-2020-gartner/ .
72 'Five Reasons Why The Big Techs Dominate the Market', Medium, 20-06-2021. https://medium.com/cornertechandmarketing/five-reasons-faang-companies-are-dominant-in-their-respective-markets-90b0b4d8fa3d .
73 'Log4j', Nationaal Cyber Security Centrum (2021). https://www.ncsc.nl/onderwerpen/log4j
74 'We hebben een monster gecreëerd (en misschien is dat helemaal niet erg)', Financieel Dagblad, 06-08-2021; 'De toekomst van online platformen', Rathenau Instituut, 20-05-2021. https://www.rathenau.nl/nl/berichten-aan-het-parlement/de-toekomst-van-online-platformen
75 'Uitspraak privacywaakhond heeft grote gevolgen voor cookies', HCC, 03-02-2022. https://www.hcc.nl/kennis/5018-uitspraak-privacywaakhond-heeft-grote-gevolgen-voor-cookies ; '3 critical challenges for governing digitalization', World Economic Forum for the Global Technology Governance Summit, 06-04-2021. https://www.weforum.org/agenda/2021/04/3-critical-challenges-for-governing-digitalization-gtgs/ .
76 'Market Power Is Eating the Economy', Project Syndicate, 25-06-2021. https://www.project-syndicate.org/onpoint/high-stock-markets-reflect-market-power-no-competition-by-jan-eeckhout-2021-06?barrier=accesspaylog
77 Although product recalls are not standard practice in digital markets, the European Commission issued a product recall for GPS watches for children in 2019. Research revealed that, among other things, the GPS location could be detected and manipulated by malicious individuals and that the microphone of the watches could be switched on remotely. It was also unclear how personal data were sent and where they were sent. https://threatpost.com/eu-recalls-childrens-smartwatch-that-leaks-location-data/141511/ ; '3 critical challenges for governing digitalization', World Economic Forum for the Global Technology Governance Summit, 06-04-2021. https://www.weforum.org/agenda/2021/04/3-critical-challenges-for-governing-digitalization-gtgs/
78 'Corona versterkt nog eens de macht van techbedrijven', Financieel Dagblad, 01-08-2021.
79 Gal, M.S. en O. Aviv, 'The competitive effects of the GDPR', Journal of Competition Law & Economics, 04-03-2020.

80 An example of an organisation advocating cross-sector cooperation to increase resilience is Agentschap Telecom. See 'Veiligheid in tijden van verandering. Jaarbericht 2021', Agentschap Telecom, april 2022.
81 As indicated in CSAN 2021, risk management is instrumental for increasing resilience, but there are still many organisations that do not deal with risk management seriously, and there are major differences between and within sectors and chains in the application of this. Some sectors are more mature than others. For example, the IB-monitor 2021 of DNB (https://www.dnb.nl/media/ldwjtxlk/ib-monitor-2021.pdf) shows that, in the financial sector more than 50% meets maturity level 4 for the three control measures in the risk management cycle. There are also sectors that traditionally have a strong safety culture.
82 This is not about determining a specific risk level: that is a political decision.
83 Methodology for sectoral cybersecurity assessments. ENISA. 2021. https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.
84 Integrating cybersecurity and enterprise risk management. NIST. 2020. https://csrc.nist.gov/publications/detail/nistir/8286/final.
85 Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix. OVV. 2021. https://www.onderzoeksraad.nl/nl/page/17171.
86 Risk management can be carried out in different ways. ENISA's Compendium of Risk Management Frameworks describes different risk management methods (https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks). Two frequently applied standards are ISO 27005, with a focus on information, and the more general ISO 31000, with a focus on business operations. In both standards, risk analysis features as the driving force for a thorough approach.
ISO 27005: information security risk management. ISO. 2018. https://www.iso.org/obp/ui/#!iso:std:75281:en.
ISO 31000: risk management guidelines. ISO. 2018. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en.
87 Insight into data storage and data flows as well as insight into interconnectivity and dependencies between systems are very important for digital resilience, as are confidentiality, integrity and the availability of information. See also https://idsa.in/system/files/monograph/monograph60.pdf#page=61. The Attack Navigator van Probst et al. schetst deze metafoor in meer detail (https://pure.tudelft.nl/ws/portalfiles/portal/27938232/GramSec_ProbstWillemsonPieters.pdf).
88 Advisers, technicians, developers, analysts, etc. each have their own framework and risk management methods, with differing premises and assumptions and the blind spots associated with this. See also the focus of the ISO 27000 series on information versus the additional focus of cyber security on physical effects.
89 See, for example, the publications following the Court of Twente case, as well as the paper 'A new accident model for engineering safer systems' by Nancy Leveson (https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.1541&rep=rep1&type=pdf).
90 https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software---lessen-naar-aanleiding-van
91 Risk management often turns out to be organisationally complex. Sore points include analysing information flows, having a list of hardware and software, keeping abreast of developments and keeping risks consistently up to date.
92 These factors generally play a part in whether or not ICT projects are carried out successfully.
93 See also https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing en https://www.ncsc.nl/documenten/brochures/2021/november/9/risicobeheersing. Please note: in addition to ownership of information, ownership of processes is also concerned here.
94 The measurability of security is a challenge in this respect. Different sources of information and different points of view can help to get a better understanding of the effectiveness (see the role of triangulation). Empirical data from experiments and expert opinions from, for example, Delphi sessions can reinforce one another. (https://people.scs.carleton.ca/~paulv/papers/oakland2017science.pdf en https://www.cybersecuritycouncil.nl/documents/advisory-documents/2021/03/12/csr-recommendation-letter-concerning-focus-of-and-approach-to-the-evaluation-of-the-ncsa). Setting out assumptions explicitly and weighing up the uncertainties play an important part in this, but this remains complex (https://cormac.herley.org/docs/justifyingSecurityMeasures.pdf en https://people.inf.ethz.ch/basin/pubs/essos16.pdf).
95 The Dutch Safety Board calls on the government to make it compulsory for all organisations to render account unambiguously for how they control digital security risks.
96 The Cyber Security Council advocates strengthening the capacity and expertise of supervisory bodies (https://www.cybersecurityraad.nl/adviezen/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid). The Dutch Safety Board states, 'Create a legal basis for digital safety control by the government by analogy with the Government Accounts Act.' The Network and Information Systems Security Act currently already contains obligations for parties to control risks (the Act contains a duty of care for suppliers of essential services and digital service providers, including the relevant supervision).
97 'Samenhangend inspectie beeld cybersecurity vitale processen 2020 – 2021' (Coordinated inspection framework of cyber security of critical processes 2020 – 2021), Inspectorate of Justice and Security, June 2021.
98 Financial incentives are often the most important trigger for organisations to analyse their risks. Without these financial incentives, the organisations will not necessarily feel the urgency to do so. In some types of service provision, responsibility for security is better

organised than in others. Compare, for example, SaaS with the purchase of a stand-alone software package. See also the extra attention paid to wireless and other IoT devices in the Radio Equipment Directive.

99 See also the discussion about CO2, nitrogen, etc. for parallels.

100 'Cybersecuritybeeld Nederland CSBN2020', NCTV, 2020.

101 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.

102 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.

103 'CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?', Cyber Security Raad, mei 2021.

104 'Privacytoezichthouders onderzoeken gebruik clouddiensten door overheidsinstellingen', Autoriteit Persoonsgegevens, 15-02-2022. https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/privacytoezichthouders-onderzoeken-gebruik-clouddiensten-door-overheidsinstellingen

105 '50 jaar internet: tijd voor herziening', De Lichtkogel, 02-09-2021. https://delichtkogel.nl/nieuwe-editie/50-jaar-internet-tijd-herziening/

106 'US investigators probing breach at code testing company Codecov', Reuters, 16-04-2021, https://www.reuters.com/technology/us-investigators-probing-breach-san-francisco-code-testing-company-firm-2021-04-16/; 'Codecov hackers breached hundreds of restricted customer sites - sources', Reuters, 20-04-2021, https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/

107 'Codecov hackers breached hundreds of restricted customer sites', Reuters, 20-04-2021, https://www.reuters.com/technology/codecov-hackers-breached-hundreds-restricted-customer-sites-sources-2021-04-19/

108 'Pulse Connect Secure Security Update', Ivanti, 20-04-2021, https://www.ivanti.com/blog/pulse-connect-secure-security-update-1?psredirect

109 'Alert (AA21-110A) Exploitation of Pulse Connect Secure Vulnerabilities', CISA, 20-04-2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-110a

110 'Misbruik ernstige kwetsbaarheden Pulse Connect Secure appliance', NCSC, 20-04-2021, https://www.ncsc.nl/actueel/nieuws/2021/april/20/pulse-secure

111 'Politie verwijdert Emotet-malware van 1 miljoen besmette pc's wereldwijd', security.nl, 25-04-2021, https://www.security.nl/posting/700775/Politie+verwijdert+Emotet-malware+van+1+miljoen+besmette+pc%27s+wereldwijd

112 'Largest U.S. pipeline shuts down operations after ransomware attack', BLEEPINGCOMPUTER, 08-05-2021, https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

113 'Oliepijplijnbedrijf Colonial Pipeline weer opgestart na grote cyberaanval', nu.nl, 13-05-2021, https://www.nu.nl/tech/6133132/oliepijplijnbedrijf-colonial-pipeline-weer-opgestart-na-grote-cyberaanval.html

114 'FBI Statement on Network Disruption at Colonial Pipeline', Federal Bureau of Investigations (FBI), 09-05-2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline

115 'Irish health service shuts down IT systems after 'sophisticated' ransomware attack', CNBC, 14-05-2021, https://www.cnbc.com/2021/05/14/irish-health-service-hit-by-sophisticated-ransomware-attack.html

116 'Irish Health Service ransomware attack happened after one staffer opened malware-ridden email', The Register, 10-12-2021, https://www.theregister.com/2021/12/10/ireland_health_conti_ransomware_attack_report/

117 'Ransomware versleutelde 80 procent it-omgeving Ierse gezondheidszorg', Security.nl, 07-02-2022, https://www.security.nl/posting/741985/Ransomware+versleutelde+80+procent+it-omgeving+Ierse+gezondheidszorg

118 'Department of Health hit by cyberattack similar to that on HSE', THE IRISH TIMES, 16-05-2021, https://www.irishtimes.com/news/health/department-of-health-hit-by-cyberattack-similar-to-that-on-hse-1.4566541

119 'Binnenlandse Zaken al twee jaar gehackt', De Standaard, 25-05-2021, https://www.standaard.be/cnt/dmf20210525_96103510

120 'HAFNIUM targeting Exchange Servers with 0-day exploits', Microsoft Security, 02-03-3033, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

121 'De FOD Binnenlandse Zaken heeft het hoofd geboden aan een cyberaanval en moderniseert zijn informatica-infrastructuur', Federale Overheidsdienst Binnenlandse Zaken, 25-05-2021, https://www.ibz.be/nl/pers/de-fod-binnenlandse-zaken-heeft-het-hoofd-geboden-aan-een-cyberaanval-en-moderniseert-zijn

122 'New sophisticated email-based attack from NOBELIUM', Microsoft Security, 27-05-2021, https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/

123 'Alert (AA21-148A) Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs', Cybersecurity & Infrastructure Security Agency (CISA), 28-05-2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-148a

124 'Cyberaanval treft IT-systemen van stad Luik', tweakers, 22-06-2021, https://tweakers.net/nieuws/183436/cyberaanval-treft-it-systemen-van-stad-luik.html

125 'Ville de Liège : réseau informatique piraté et demande de rançon', RTC Tele Liège, 22-06-2021, https://www.rtc.be/article/info/divers/ville-de-liege-reseau-informatique-pirate-et-demande-de-rancon-_1509612_325.html?1244#

126 'IT-problemen Testen voor Toegang 'gevolg van hackpoging', RTL nieuws, 25-06-2021, https://www.rtlnieuws.nl/tech/artikel/5238395/wachttijden-bij-testen-voor-toegang-door-technische-problemen

127 'REvil ransomware attacks systems using Kaseya's remote IT management software', THE VERGE, 03-07-2021, https://www.theverge.com/2021/7/2/22561252/revil-ransomware-attacks-systems-using-kaseyas-remote-it-management-software

128 'How a Small Dutch IT Company Caught Up in the Kaseya Attack Stepped Up for Customers', THE WALL STREET JOURNAL, 14-07-2022, https://www.wsj.com/articles/how-a-small-dutch-it-company-caught-up-in-the-kaseya-attack-stepped-up-for-customers-11626255002

129 'KASEYA VSA LIMITED DISCLOSURE', Dutch Institute for Vulnerability Disclosure (DIVD), 07-07-2021, https://csirt.divd.nl/2021/07/07/Kaseya-Limited-Disclosure/

130 'Schakel Kaseya VSA uit: mogelijke ransomware aanval via leveranciersketen gaande,' NCSC, 03-07-2021, https://www.ncsc.nl/actueel/nieuws/2021/07/03/schakel-kaseya-vsa-uit-mogelijke-ransomware-aanval-via-leveranciersketen-gaande; 'Patch beschikbaar voor kwetsbaarheden VSA-software Kaseya', NCSC 12-07-2021, https://www.ncsc.nl/actueel/nieuws/2021/juli/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya/patch-beschikbaar-voor-kwetsbaarheden-vsa-software-kaseya

131 'Updates Regarding VSA Security Incident', Kaseya, NCSC 26-07-2021, https://www.kaseya.com/potential-attack-on-kaseya-vsa/

132 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', The Guardian, 18-07-2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

133 'Israeli authorities inspect NSO Group offices after Pegasus revelations', The Guardian, 29-07-2021, https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations

134 'GGD ging plat door aanvallen op DigiD-leverancier', Computable, 22-07-2021, https://www.computable.nl/artikel/nieuws/zorg/7219367/250449/ggd-ging-plat-door-aanvallen-op-digid-leverancier.html

135 'Nederlandse overheid stopt met uitgifte publiek vertrouwde TLS-certificaten', security.nl, 02-08-2021 https://www.security.nl/posting/714980/Nederlandse+overheid+stopt+met+uitgifte+publiek+vertrouwde+TLS-certificaten

136 'Factsheet PKIoverheid stopt met webcertificaten', Nationaal Cyber Security Centrum (NCSC), 30-09-2021, https://www.ncsc.nl/documenten/factsheets/2021/september/29/factsheet-pkioverheid-stopt-met-webcertificaten

137 'NCSC publiceert factsheet "PKIoverheid stopt met webcertificaten: Kies een andere leverancier"', NCSC, 30-09-2021, https://www.ncsc.nl/actueel/nieuws/2021/september/29/ncsc-publiceert-factsheet-pkioverheid-stopt-met-webcertificaten-kies-een-andere-leverancier

138 'Cybercriminelen proberen wekenlang in te breken in ziekenhuis', Omroep Gelderland, 17-08-2022, https://www.gld.nl/nieuws/7346816/cybercriminelen-proberen-wekenlang-in-te-breken-in-ziekenhuis

139 'Buitenlandse hackers plegen digitale 'megadiefstal': gegevens 1400 medewerkers provincie Gelderland gestolen', De Gelderlander, 30-08-2022, https://www.gelderlander.nl/home/buitenlandse-hackers-plegen-digitale-megadiefstal-gegevens-1400-medewerkers-provincie-gelderland-gestolen~aa88c78f/

140 'Slachtoffers hack bij provincie geadviseerd nieuw paspoort aan te vragen', De Gelderlander, 04-09-2021, https://www.gelderlander.nl/home/slachtoffers-hack-bij-provincie-geadviseerd-nieuw-paspoort-aan-te-vragen~af01960b/?referrer=https%3A%2F%2Fduckduckgo.com%2F

141 'Grote hack bij ROC Mondriaan: computers plat en bestanden ontoegankelijk', RTL nieuws, 23-08-2021, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5249593/roc-mondriaan-gehackt

142 'Vragen en antwoorden hack ROC Mondriaan', ROC Mondriaan, 16-12-2021, https://www.rocmondriaan.nl/vragen-en-antwoorden-hack-roc-mondriaan

143 'Hackers ROC Mondriaan eisen miljoenen euro's: 'Absurd veel geld'', Omroep West, 19-09-2021, https://www.omroepwest.nl/nieuws/4460774/hackers-roc-mondriaan-eisen-miljoenen-euros-absurd-veel-geld

144 'ROC Mondriaan weigert losgeld te betalen, hackers publiceren gevoelige gegevens', AD, 14-09-2021. https://www.ad.nl/den-haag/roc-mondriaan-weigert-losgeld-te-betalen-hackers-publiceren-gevoelige-gegevens~aad5747e/

145 'CoronaCheck-app soms onbereikbaar door DDos-aanvallen en grote drukte', NOS, 25-09-2021, https://nos.nl/artikel/2399240-coronacheck-app-soms-onbereikbaar-door-ddos-aanvallen-en-grote-drukte

146 'Industrieconcern VDL Groep getroffen door digitale aanval', NOS, 07-10-2021, https://nos.nl/artikel/2400694-industrieconcern-vdl-groep-getroffen-door-digitale-aanval

147 'Ook ASML en Philips worden geraakt door problemen bij VDL na cyberaanval', Omroep Brabant, 22-10-2021, https://www.omroepbrabant.nl/nieuws/3977729/ook-asml-en-philips-worden-geraakt-door-problemen-bij-vdl-na-cyberaanval

148 'VDL Groep maand na cyberaanval volledig hersteld dankzij back-ups', security.nl, 08-11-2021, https://www.security.nl/posting/729158/VDL+Groep+maand+na+cyberaanval+volledig+hersteld+dankzij+back-ups

149 'Google warns 14,000 Gmail users targeted by Russian hackers', Bleeping Computer, 07-10-2021, https://www.bleepingcomputer.com/news/security/google-warns-14-000-gmail-users-targeted-by-russian-hackers/
150 'Elektronicaketen MediaMarkt getroffen door aanval met Hive-ransomware', security.nl, 09-11-2021, https://www.security.nl/posting/729252/%22Elektronicaketen+MediaMarkt+getroffen+door+aanval+met+Hive-ransomware%22
151 'MediaMarkt hit by Hive ransomware, initial $240 million ransom', Bleeping Computer, 08-11-2021, https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/
152 'Gehackt en gegijzeld: hoe MediaMarkt onderhandelde met ransomwarecriminelen', RTL nieuws, 19-03-2022, https://www.rtlnieuws.nl/tech/artikel/5289859/mediamarkt-ransomware-hive-cybercriminelen-onderhandelingen-helpdesk
153 'Cyberaanval op Heijmans, hackers proberen 1300 accounts te kraken', Omroep Brabant, 17-11-2021, https://www.omroepbrabant.nl/nieuws/3991167/cyberaanval-op-heijmans-hackers-proberen-1300-accounts-te-kraken
154 'Wind Turbine Giant Vestas Confirms Ransomware Involved in Cyberattack', Security Week, 30-11-2021, https://www.securityweek.com/wind-turbine-giant-vestas-confirms-ransomware-involved-cyberattack
155 'Second update on cyber incident', Vestas, 29-11-2021, https://www.vestas.com/en/media/company-news/2021/second-update-on-cyber-incident-c3462120
156 'U.S. State Department phones hacked with Israeli company spyware - sources', Reuters, 04-12-2021, https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
157 'Apple sues NSO Group to curb the abuse of state-sponsored spyware', Apple, 23-11-2021, https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
158 'Technologieleverancier van Defensie en politie gehackt, losgeld geëist voor vertrouwelijke informatie', de Volkskrant, 06-12-2021, https://www.volkskrant.nl/nieuws-achtergrond/technologieleverancier-van-defensie-en-politie-gehackt-losgeld-geeist-voor-vertrouwelijke-informatie~bcc2f42b/
159 'Ransomwaregroep steelt data van leverancier Nederlandse politie en Defensie', security.nl, 06-12-2021, https://www.security.nl/posting/732892/Ransomwaregroep+steelt+data+van+leverancier+Nederlandse+politie+en+Defensie
160 'Statement Ransomware Aanval', Abiom, 06-12-2022, https://abiom.nl/statement-ransomware-aanval/
161 'Statement Ransomware Aanval', Abiom, 6-12-2021, https://abiom.nl/statement-ransomware-aanval/
162 'Antwoorden Kamervragen over het bericht over hacken technologieleverancier van Defensie en politie', Rijksoverheid.nl, 04-02-2022, https://www.rijksoverheid.nl/documenten/kamerstukken/2022/02/04/antwoorden-kamervragen-over-het-bericht-technologieleverancier-van-defensie-en-politie-gehackt
163 'Beveiligingsadvies Advisory Kwetsbaarheden verholpen in Apache Log4j', Nationaal Cyber Security Centrum, 10-12-2021, https://www.ncsc.nl/actueel/advisory?id=NCSC%2D2021%2D1052
164 'Weer 'ernstig' lek in serversoftware, daags na dichten vorig lek', RTL nieuws, 17-12-2021, https://www.rtlnieuws.nl/tech/artikel/5275131/apache-server-log4j-log4shell-lek-kwetsbaarheid-ddos
165 'Beveiligingslek dwingt KVK website en diensten offline te halen', RTL nieuws, 25-12-2021, https://www.rtlnieuws.nl/tech/artikel/5276898/internetbeveiliging-log4j-onlinedienst-software-kvk-koophandel-website
166 'Log4j', NCSC, https://www.ncsc.nl/onderwerpen/log4j
167 'Nation-state actors from China, Iran, North Korea, and Turkey join the Log4Shell exploitation party', cybernews, 15-12-2021, https://cybernews.com/news/nation-state-actors-from-china-iran-north-korea-and-turkey-join-the-log4shell-exploitation-party/ ; 'Conti ransomware uses Log4j bug to hack VMware vCenter servers', bleeping computer, 17-12-2021, https://www.bleepingcomputer.com/news/security/conti-ransomware-uses-log4j-bug-to-hack-vmware-vcenter-servers/
168 'Vragen en antwoorden Log4j-informatiesessie 15 december 2021', Digital Trust Center, 20-12-2021, https://www.digitaltrustcenter.nl/vragen-en-antwoorden-log4j-informatiesessie
169 'Belgische leger kon 4 weken niet e-mailen door cyberaanval', RTL nieuws, 13-01-2022, https://www.rtlnieuws.nl/tech/artikel/5280782/belgische-leger-cyberaanval-log4j-hack-server
170 'Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict', Reuters, 14-01-2022, https://www.reuters.com/technology/massive-cyberattack-hits-ukrainian-government-websites-amid-russia-tensions-2022-01-14/
171 'Digitale aanvallen Oekraïne: een tijdlijn,' NCSC, 10-03-2022, https://www.ncsc.nl/actueel/nieuws/2022/februari/10/digitale-aanvallen-oekraine-een-tijdlijn
172 'Cyber attacks on government websites', Security Service of Ukraine, 14-01-2022, https://ssu.gov.ua/en/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv
173 'SSU investigates Russian involvement in cyber attacks on Ukrainian government websites', Security Service of Ukraine, 14-01-2022, https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskykh-spetssluzhb-do-sohodnishnoi-kiberataky-na-orhany-derzhavnoi-vlady-ukrainy
174 'Destructive malware targeting Ukrainian organizations', Microsoft Security, 15-01-2022,

https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
175 'Analysis of Destructive Malware (WhisperGate) targeting Ukraine', S2W blog, 18-01-2022, https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3
176 'Comparative analysis of WhisperKill and WhiteBlackCrypt', CERT-UA, 26-01-2022, https://cert.gov.ua/article/18108
177 'Wiper in Ukraine Used Code Repurposed From WhiteBlackCrypt Ransomware', Kim Zetter, 26-01-2022, https://zetter.substack.com/p/wiper-in-ukraine-used-code-repurposed?s=r
178 'Digitale aanvallen Oorlog Oekraïne', NCSC, https://www.ncsc.nl/onderwerpen/oekraine
179 'Antwerps parket onderzoekt cyberaanval op havenbedrijven: tankopslag SEA-invest hersteld, andere activiteiten ondervinden nog hinder', Het Laatste Nieuws, 03-02-2022, https://www.hln.be/binnenland/antwerps-parket-onderzoekt-cyberaanval-op-havenbedrijven-tankopslag-sea-invest-hersteld-andere-activiteiten-ondervinden-nog-hinder~a0814f02/
180 'Hacker greifen Zulieferer von Tankstellen an', Wirtschafts Woche, 01-02-2022, https://www.wiwo.de/technologie/digitale-welt/oiltanking-hacker-greifen-zulieferer-von-tankstellen-an/28027806.html
181 'Shell re-routes oil supplies after cyberattack on German firm', Reuters, 01-02-2022, https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
182 'BlackCat ransomware implicated in attack on German oil companies', ZDNet, 02-02-2022, https://www.zdnet.com/article/blackcat-ransomware-implicated-in-attack-on-german-oil-companies/
183 'ALPHV BlackCat - This year's most sophisticated ransomware', Bleeping Computer, 09-12-2021, https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/
184 'Olieopslagplaatsen in Terneuzen en Gent hebben vertragingen na cyberaanval', Tweakers, 03-02-2022, https://tweakers.net/nieuws/192808/olieopslagplaatsen-in-terneuzen-en-gent-hebben-vertragingen-na-cyberaanval.html
185 'Cyberattacks knock out sites of Ukrainian army, major banks', ABC News, 15-02-2022, https://abcnews.go.com/Business/wireStory/cyberattack-hits-ukrainian-government-sites-major-banks-82906222
186 'UK government assess Russian involvement in DDoS attacks on Ukraine', NCSC-UK, 18-02-2022, https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine
187 'Ukrainian military agencies, state-owned banks hit by DDoS attacks', Bleeping Computer, 15-02-2022, https://www.bleepingcomputer.com/news/security/ukrainian-military-agencies-state-owned-banks-hit-by-ddos-attacks/
188 '360 Netlab' Twitter, 16-02-2022, https://twitter.com/360Netlab/status/1493797519725367302
189 'Cybersecuritybeeld Nederland 2020', Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), pag.18 https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020
190 'Expeditors Downtime notification', Expeditors website 06-03-2022, https://www.expeditors.com/022022-downtime-notification
191 'New Sandworm malware Cyclops Blink replaces VPNFilter', National Cyber Security Centre, 23-02-2022, https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter
192 'MIVD ontdekt Russische spionnen in Nederlandse routers', Ministerie van Defensie, 03-02-2022, https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/nieuws/2022/03/03/mivd-ontdekt-russische-spionnen-in-nederlandse-routers
193 'NCSC-UK, CISA, FBI en NSA waarschuwen voor compromittatie van SOHO-routers door APT Sandworm', NCSC 23-02-2022, https://www.ncsc.nl/actueel/nieuws/2022/februari/23/ncsc-uk-cisa-fbi-en-nsa-waarschuwen-voor-compromittatie-van-soho-routers-door-apt-sandworm

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

July 2022