



National Coordinator for Security and
Counterterrorism
Ministry of Justice and Security

Cyber Security Assessment Netherlands CSAN 2021



Cyber Security Assessment Netherlands

CSAN 2021

Publication details

The Cyber Security Assessment Netherlands 2021 (CSAN 2021) offers insight into the cyber threat, the interests that may be affected by it, resilience and, finally, the risks. The focus here is on national security. The CSAN was drawn up by the National Coordinator for Security and Counterterrorism (NCTV) and the National Cyber Security Centre (NCSC). It is defined annually by the 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 NCTV is the central government body responsible for counterterrorism, cybersecurity, national security, crisis management and state threats, with a solid accent on preventing and minimising social disruption.

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

Table of Contents

Core CSAN: Cyber Attacks Impair Society's Central Nervous System	7
1 Introduction	13
2 Retrospective	17
3 COVID-19: current events influence threat picture	23
4 Ransomware risk to national security	27
5 Violation of cyberspace poses a risk	33
6 Geopolitics influences threats and interests	39
7 Risk management instrumental in boosting resilience	43
8 Threat scenarios	49
Appendix: Creating the CSAN	55

.....
*Cybersecurity inextricably interlinked
with national security*



Core CSAN: Cyber Attacks Impair Society's Central Nervous System

Digital processes are the 'central nervous system' of society, as they are indispensable to its uninterrupted functioning. Cyber attacks impair this central nervous system and this can ultimately lead to paralysis, as also noted in the Cybersecurity Assessment Netherlands (CSAN) 2020. COVID-19 has accelerated the digitisation of processes, including in healthcare and education. The digital and the physical world are increasingly interlinked and it is becoming more and more difficult to distinguish between the two. There are hardly any processes left without a digital component.

As the digital and the physical world are so interlinked, a governance approach that addresses the importance of cybersecurity, the cyber threat and resilience solely from a technology-based perspective is too narrow. This is also, and perhaps above all, about how organisations and people use digitisation, and therefore about the functionality for society and the economy. A cyber incident affects digital processes and when these do not work properly, this affects the functioning of organisations. Chain reactions can affect entire sectors or even society as a whole. For example, a ransomware attack on a municipality, university, hospital or electricity distributor renders systems unusable: the technology no longer works. As a result, the municipality can no longer perform its duties properly, research and education come to a halt, patient care is impeded or there may be a power outage. This means that the cyber threat jeopardises not only the functioning of technology, but also a range of other interests. Therefore, resilience-enhancing measures not only contribute to the security of technology, but also help to protect our society and economy.

Cybersecurity remains inextricably interlinked with national security: cybersecurity breaches can lead to social disruption. The cyber threat keeps evolving as actors continue to develop and the geopolitical context keeps changing, and is also impacted by

current events such as COVID-19. Resilience also continues to evolve. Whether there is an adequate balance between the various interests, the cyber threat and resilience is a question that needs to be resolved through governance and/or risk management.

In this Cybersecurity Assessment Netherlands, the National Coordinator for Security and Counterterrorism identifies four risks to national security:

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 infiltration in processes that ensure the distribution of electricity.
3. Breaches of (the security of) cyberspace, such as through the abuse of global IT supply chains.
4. Large-scale outages: a situation where one or more processes are disrupted due to natural or technical causes or unintentional human action.

Espionage, sabotage and outages have already been extensively discussed in the CSAN 2020. The risks associated with this (risks 1, 2 and 4) are still relevant. Espionage and sabotage are also explained in detail in the publication ‘State Actors Threat Assessment’. This CSAN discusses risks 2 (specifically ransomware, chapter 4) and 3 (breaches of cyberspace, chapter 5) in detail.

Looking back: Netherlands hit by wide range of cyber incidents

In the period from March 2020 to March 2021, there were numerous cyber incidents in or relating to the Netherlands. Malicious parties especially exploited the current issue of COVID-19 to carry out attacks. Remote working services were also the target of attacks. In addition, processes with a digital component were made inaccessible and organisations in supply chains were attacked. There were many incidents where large amounts of vulnerable business and privacy-sensitive information were made public. Lastly, unintentional failures led to outages.

The various incidents are discussed in detail in chapter 2 ‘Retrospective’.

Threat continues to evolve

COVID-19 exploited to carry out attacks

While the COVID-19 pandemic also led to social disruption in the Netherlands, the digitisation of Dutch society enabled resilience and continuity. Society has become even more digitised as a result of the pandemic. Thanks to IT, commercial, educational and social activities that threatened to come to a halt could continue, at least in part. This places heavy demands on cyberspace, which has become even more important to the functioning of society.

The pandemic has also led to shifts in the threat assessment. Actors seize on current issues that dominate headlines worldwide to carry out digital attacks. This also holds true for COVID-19. For example, many phishing emails from cybercriminals and state actors last year exploited COVID-19. Current events have also given rise to an intelligence need among state actors. In relation to COVID-19, a need for knowledge about vaccines arose, which resulted in digital espionage and even the spreading of disinformation. Disinformation around current issues such as the pandemic can lead to polarisation because it fuels and magnifies differences of opinion. One example of this is whether or not people trust vaccines against COVID-19. It is conceivable that polarisation will also get a digital component. For example, opponents of the COVID-19 restrictions could express their dissatisfaction by disrupting digital processes, such as by launching DDoS attacks against public authorities or parties with different ideas. They might also try to hack into public authorities to get information that could put an authority in a bad light.

In the Netherlands, the pandemic has also led to increased attention to risks and the (accelerated) implementation of resilience-enhancing measures by companies and organisations, for example in education. To what extent the initiatives to increase resilience now and in the near future will be sufficient to curb the evolving threat is difficult to assess. However, at present it does not appear that the threat has been brought fully under control (see below under ‘Resilience’).

Chapter 2 ‘Retrospective’ describes a number of cyber incidents that occurred around COVID-19 in and in relation to the Netherlands. Chapter 3 explains how the pandemic, as the most important current issue, has affected the threat assessment.

Attacks can cause long-term damage to organisations and chains

The impact of digital attacks varies. Some, such as DDoS attacks, lead to short-term disruption of processes, paralysing websites for a few hours. Other types of attacks, such as ransomware attacks, have a long-term impact. Cybercriminals take time to infiltrate victims’ networks, to find out how they can achieve maximum disruption of processes and determine what would be an ‘appropriate’ (i.e. realistic) ransom amount. They often spend long periods unseen in a network. They further increase the impact of their attack by also rendering system backups unusable. In extreme cases, the damage to systems is so severe that repair is impossible. Then the only option left is to rebuild systems from scratch (which sometimes even requires regathering lost data). When various means of pressure are used, ransomware attacks can also have a long-term impact on processes. In addition to making processes inaccessible, the aim is to steal information, which the actor then makes public or threatens to make public. Attackers can go a step further by trying to extort their target’s customers. This can happen quickly, or only after some time, in which case victims of a ransomware attack may have to deal with the consequences of the original attack for a long time.

Attacks with a long-term impact on processes are not only launched by cybercriminals, but also by state actors. They use backdoors to gain access to networks, for example, and remain there unseen for a long time. Meanwhile, they explore the systems and create new access points. In the case of the SolarWinds campaign, for example, it was found that the Russian state actor behind the attack had been inside the system for over a year before being detected (see chapter 2 ‘Retrospective’). Furthermore, it has been established that state actors launch targeted attacks against cybersecurity companies and individual security researchers. This gives them insight into the working methods of these security companies and researchers and into any weaknesses in the security of their customers. Actors can then use this knowledge to launch new attacks.

In chapter 4, the cybercrime threat is further explained by the police. Here, the focus is on the use of ransomware as the final element of a comprehensive cybercrime process. The geopolitical motives behind the activities of state actors are further explained in chapter 6.

Cybercriminals can impair national security

Cybercriminals can cause extensive damage to digital processes through their attacks. A number of cybercrime groups now have capabilities on par with those of state actors. This implies that their attacks may have a similar impact as those of state actors. Although cybercriminals are mainly focused on making money and do not deliberately set out to disrupt society, their attacks can cause so much damage that national security interests are affected. This may be the case, for example, when they make critical processes inaccessible by means of ransomware.

Although targeted attacks on critical processes have not yet been observed in the Netherlands, they do occur abroad. The CSAN 2020 reported ransomware attacks on industrial control systems (ICS) that are part of the drinking water and energy supply infrastructure, for example. In the past year, critical processes in the electricity, water, oil & gas, chemical, food, transport and healthcare sectors worldwide were again targeted by criminal groups through cyber attacks. Various reports have found that the resilience in critical processes in the Netherlands is sometimes inadequate. The Cyber Security Council has concluded that even in organisations that are part of critical processes, basic ICT and security hygiene is frequently inadequate, as a result of which basic threats to their processes cannot be countered or detected. In addition, a report by the Human Environment and Transport Inspectorate shows that Waternet, which supplies drinking water to Amsterdam and the surrounding area, is insufficiently in control of its cybersecurity. As a result, there is an increased risk of a cyber incident with possible consequences for the quality and/or continuity of the drinking water supply. Lastly, research conducted following a hack at a water supply company in the United States shows that many ICSs in the Netherlands are easily accessible. Using relatively simple Google searches, the researchers found many systems that had no or hardly any cybersecurity.

In addition to the fact that cybercriminals (also) target critical processes, the relationships they maintain with state actors are a source of concern. For example, cybercrime groups are hired by the national government of the country in which they are based to carry out cyber attacks (hackers-for-hire). Or cybercrime groups are tolerated by the state and pressured to carry out attacks for hire. Sometimes this involves appealing to their 'patriotism'. Lastly, there are examples of criminal hackers who (also) work for government agencies that have a public task in fighting cybercrime.

Due to the possible impact on national security, this CSAN pays more attention to cybercriminals than in previous years. Today's cybercrime ecosystem is a mature system. It is a system where actors are supported by facilitators who offer technical, financial and legal services for cyber attacks. Professional and customer-friendly service providers also bring new actors onto the scene: criminals engaged in 'traditional' types of crime (such as drug dealers) branch out into cyber attacks, such as phishing. In the future, cyber attacks by criminals also engaging in all kinds of other crime may lead to the addition of a physical component to cybercrime, such as the threat or use of force after a phishing or ransomware attack, or physical consequences due to the inaccessibility of processes.

Chapter 4 explains the cybercrime threat in more detail, focusing on the use of ransomware.

Attacks breach security of cyberspace

All our digital processes are strongly interlinked with and dependent on the global cyberspace. Digital processes, such as those of providers of critical infrastructure, but also those of large and small organisations and citizens, use the services and products of globally operating companies. Examples include products enabling remote working, managing and sending emails and storing and processing information with a cloud provider. In addition, digital processes are interlinked with and dependent on the technical infrastructure of the internet, including undersea cables. This interwovenness has brought many benefits and continues to offer opportunities, but also poses a risk. What if, in today's tense geopolitical context, state actors were to tap undersea communications cables for intelligence gathering or manipulate internet protocols on a massive scale? What if – in times of conflict – state actors sabotaged those cables? What if malicious parties manipulated or sabotaged digital processes or products of global companies? What if the services of one of the three largest global cloud providers became unavailable for a short or long period due to a technical failure?

Such types of abuse or outages that breach (the security of) cyberspace have a major impact on the functioning of all digital processes. They make sensitive or vulnerable personal, economic or political information accessible to malicious parties. This could hurt the Dutch economy or put the Netherlands at a disadvantage in international negotiations. In such a scenario, critical tasks of organisations, such as distributing energy, carrying out financial transactions or providing education, can no longer be carried out. Besides this direct impact, breaches of cyberspace also have a wider impact. This includes, for example, the costs of investigating and repairing systems, the potential need to rebuild infrastructure and being forced to temporarily fall back on analogue alternatives. Breaches of cyberspace can also impair citizens' and organisations' confidence in processes. Furthermore, individual states and organisations often have only very limited capabilities to increase their resilience to outages and the abuse of cyberspace. For example, they often lack insight into the levels of resilience in

various parts of their ICT supply chains. This may generate additional risks that are not properly identified. For example, risks may arise due to the purchasing and public procurement of products and services from an ICT supplier that provides a product with a vulnerability or where a (temporary) staff member has access to digital processes containing sensitive information. Breaches of (the security of) cyberspace are not merely a theoretical possibility but are already taking place. Recently, additional sophisticated attacks in ICT supply chains with a global impact came to light and vulnerabilities in globally used products were exploited.

Chapter 5 discusses the risk of breaches of cyberspace in more detail.

Resilience not yet sufficient

The National Cyber Security Centre (NCSC) observes positive developments when it comes to increasing the resilience of the Netherlands: an increase in the use of multi-factor authentication, the phasing out of a number of unsafe technologies, an improvement in detection and response and, lastly, a wide range of concrete initiatives to improve the resilience of organisations. These positive developments notwithstanding, the cyber incidents that recently hit the Netherlands show that resilience is not yet sufficient (see chapter 2 'Retrospective'). In May 2021, the Netherlands Court of Audit stated that the level of information security throughout the central government had not changed in 2020. Virtually all organisations that lacked adequate information security in 2019 took action in 2020 to address this. However, this has not yet led to sufficient control of the risks, and consequently the deficiencies have not yet been resolved. The Cyber Security Council has concluded that additional efforts and investments will be required in the Netherlands in the coming years to strengthen resilience.

No or insufficient basic measures

One of the core messages in the CSANs in recent years has been that no or insufficient basic measures are applied to counter the digital threats, such as using strong passwords and prompt patching to fix vulnerabilities. The incidents discussed in chapter 2 'Retrospective' show that too often, it is still the case that no or insufficient basic measures are applied. Actors are quick to exploit serious vulnerabilities in hardware and software and they often continue to do so over long periods of time. They remain successful on an ongoing basis in exploiting publicly known vulnerabilities through cyber attacks on a global scale. The Dutch intelligence services (the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD)) have observed that state actors persist in exploiting publicly known vulnerabilities to carry out digital attacks. An example of this is the serious vulnerability in Citrix servers, which became known in December 2019 and was exploited by various parties, including

state actors. At the time, the NCSC concluded that many Dutch Citrix servers were also vulnerable to attacks. In June 2020, six months after the vulnerability was publicised, an investigation by Fox-IT showed there were still 39 compromised Citrix servers in the Netherlands. Some of these servers were not promptly patched by the relevant organisation, which means attackers could already have installed a backdoor and made digital processes inaccessible or gained unauthorised access to information. In the case of the vulnerabilities in Microsoft Exchange that were publicised in early March 2021, it was also found that organisations had not promptly patched vulnerable servers. The NCSC warned that the vulnerabilities would be exploited, resulting in data being stolen and criminals installing malware and backdoors and selling emails. This will enable them to carry out new attacks or to hit digital processes in the near future; for example, through identity fraud based on captured personal data.

Several incidents illustrate that there is a systemic time lag between the moment when critical vulnerabilities are publicised and the (subsequent) implementation of security updates. As a result, Dutch companies, organisations and ministries run an increased risk of digital espionage by state actors.

The NCSC product 'Guide to Cybersecurity Measures' lists the most important basic measures.

Considerable differences in the area of resilience

Cybersecurity experts observe considerable differences in levels of resilience in the Netherlands. Large companies can invest in knowledge and skills in the field of cybersecurity. Suppliers of essential services and digital service providers also have a statutory duty of care, laid down in the Network and Information Systems Security Act (*Wet beveiliging netwerk- en informatiesystemen*, Wbni). Small businesses, on the other hand, including small and medium-sized enterprises (SMEs), often lack the expertise and resources to take resilience to the next level. Yet SMEs can also be targeted by sophisticated actors. For example, the MIVD stated that in the Netherlands, the EXIM vulnerability which the US intelligence service NSA warned about had also been exploited by a state actor to compromise victims in the SME sector. Furthermore, vulnerable SMEs can be part of the supply chains of critical processes. SMEs are increasingly dependent on IT service providers, but they do not always have adequate basic security measures; for example, it is often unclear who is responsible for updates or back-ups. This makes digital processes vulnerable to all kinds of abuse. Experts fear that the differences in the level of resilience will further increase in the coming years. To reduce these differences, various initiatives have been launched to provide public and private parties with information and to work together to increase resilience. In this context, the NCSC serves as the national information exchange within the Nation-Wide System.

Risk management as an instrument in increasing resilience

Security experts, regulatory authorities and scientists emphasise the importance of risk management as an instrument to gain better insight into levels of resilience. By making a risk assessment, it can be determined which measures are required to adequately control risks. To make risks less abstract, they can be translated into scenarios. A risk-based approach helps to make choices about which digital processes, and consequently which systems, are important to an organisation and in which areas disruption is not acceptable. Risk management involves weighing up of interests, which implies that it should also be on the agenda of government bodies.


Chapter 7 further explains the importance of risk management as an instrument in increasing resilience. Chapter 8 outlines scenarios where processes that use cloud services are affected by outages or compromised.

Tension between security, freedom and economic growth increases

In a digitised society, security is not an end in itself. It is closely linked to values such as freedom and economic growth. In some respects, security is even a prerequisite for these other interests. Ideally, a certain balance is maintained between the different interests. This balance is under pressure, as the tension between the different interests is increasing. Today, cyberspace is the domain of (geo) politics. Digitisation plays an increasingly important role in relations between states. It is a domain in which states want to distinguish themselves from each other in order to improve their competitiveness. In addition, groups of states have different aims. Some states, for example, primarily seek to regulate the flow of information to and from their country, while others aim for openness and interoperability. These different perspectives have an impact on discussions about norms and values in cyberspace, but also on the formulation of (future) standards.

Along with many advantages, digitisation also has disadvantages. Digital processes can be sources or targets of espionage and sabotage, for example. As geopolitical and technological developments reinforce each other, governments need to take action to continue to safeguard national security and public interests. States and intergovernmental organisations such as the EU are uneasy about the influence of tech companies such as Google and Facebook and want to be less dependent on big players from a limited number of states. All of society relies on a digital infrastructure that is owned and access to which is controlled by only a handful of tech companies. Government, too, can be dependent on this digital infrastructure for the implementation of its policies. This creates a need for digital or strategic autonomy, which in the European context is also referred to as digital

sovereignty. In a situation where tension between different interests is growing and cyberspace is also a domain for espionage or actions against other states, trust in cyberspace is especially important.

 [Back to Table of Contents](#)

.....
*Insight into the cyber threat, the interests
that may be affected and resilience*



1 Introduction

The CSAN 2021 builds on the previous CSANs. The box at the end of this introduction summarises the key messages of 2020. In the 2021 edition, the focus is on interpreting the shifts in interests, threats and resilience.

Purpose and scope

The CSAN provides an insight into the cyber threat, the interests that may be affected, resilience and risks. The emphasis is on national security.¹ Digitisation offers opportunities, but it also lends itself to all kinds of misuse and is vulnerable to system failure. The CSAN does not focus on the opportunities of digitisation. It does focus on disruptions to processes with a digital component, including forms of cybercrime in which the process and/or the underlying ICT is the target. Other forms of misuse of processes, for example dissemination of propaganda, distribution of child pornography and all kinds of fraud, are outside the scope. This scope does not mean that other forms of misuse are not important. The in-depth chapters (new for 2021) may cover broader topics if they can have an impact on the cyber threat, interests and resilience.

The CSAN is primarily intended for strategy and policy-making on a 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.

¹ National security is jeopardised when one or more national security interests are threatened to such an extent that this results or could result in social disruption. The Netherlands distinguishes six national security interests: territorial security, physical security, economic security, ecological security, social and political stability, and finally, international legal order. All security interests can also be affected through cyberspace. Social disruption has a physical aspect (casualties, damage or failure of critical functions) and a socio-psychological aspect (such as disruption of daily life). Social disruption also looms when the continuity or availability of critical processes is affected. Together, these processes constitute the Netherlands' critical national infrastructure. The transport and distribution of electricity, access to the Internet and provision of drinking water are examples of critical processes. Source: 'National Security Strategy 2019', NCTV, June 2019.

Cybersecurity companies and professionals also use the CSAN as a frame of reference for their own directors or clients. The CSAN is also intended as a risk management tool, focusing specifically on the identification and assessment of risks, one of the steps in a risk management process. Finally, the CSAN is also accessible to the general public. The reporting period of this CSAN is March 2020 to March 2021. However, incidents from January/February 2020 and incidents between April 2021 and the publication date of this CSAN (June 2021) have been included if there was a relevant impact.

Key terms

In the CSAN, the most important terms are defined as follows:

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

Interests: 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. The CSAN focuses on national security interests.

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 (hereinafter: 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.

Cyberspace: the complex environment resulting from intertwined digital processes, supported by globally distributed physical information and communication technology (ICT) devices and

connected networks. Cyberspace is approached from three angles: 1) digital processes including human behaviour, 2) the technical layer, 3) risk management and/or governance.

Threat: a cyber incident that may occur or a combination of simultaneous or consecutive cyber incidents.

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

System failure: a situation where one or more processes are disrupted due to natural or technical causes or human error.

Disruption: an impairment of the availability, integrity or confidentiality of information (processing).

Resilience: the ability to reduce (relevant) risks to an acceptable level through a set of measures to prevent cyber incidents and, when they do occur, to detect them, limit their damage and facilitate recovery. What is an acceptable level of resilience, is the outcome of a risk assessment. This can be done with technical, procedural or organisational measures. Other ways are, for example, legislation, subsidies, training to educate users in safe behaviour, information and awareness campaigns, cooperation between parties and standardisation frameworks for digitisation of services and processes, and design of systems.

Key messages of CSAN 2020

The key messages of CSAN 2020 still apply. They are reiterated in the box below.

Cyber incidents can paralyse society

- Cybersecurity is a precondition for the functioning of society.
- The digital threat is permanent.
- Digital resilience is not yet in order everywhere because of the lack of basic measures.
- Boosting resilience is the most important tool for managing cyber risks.
- A complete and accurate picture of the resilience of critical processes is (still) missing.
- Cyber risks are as great as ever and cannot be separated from other risks.
- The Netherlands' dependence on countries with offensive cyber programmes is a risk-increasing factor.
- Risks to national security are: sabotage and espionage by states, system failure. In addition, cyber attacks by criminals are relevant.


Source: CSAN 2020, NCTV, June 2020.

Structure

This CSAN consists of a core and seven in-depth chapters. The chapter before this Introduction, the Core CSAN, contains the main messages. Some of them are further elaborated on in a chapter. The division into a core and several themes is intended to allow readers from different target groups to easily navigate the CSAN and focus on the topics that match their professional role or interest. The in-depth chapters have the following themes:

- Chapter 2, the Retrospective, provides an overview of relevant incidents in the Netherlands in the period March 2020 to March 2021. This chapter is factual.
- Chapter 3 explains how COVID-19 has affected the threat picture.
- Chapter 4 further examines ransomware as a risk to national security.
- Chapter 5 outlines how violations of cyberspace pose a risk.
- Chapter 6 describes the influence of geopolitics on interests and threats.
- Chapter 7 discusses risk management as a tool for boosting resilience.
- Chapter 8 outlines a threat scenario with an elaboration of various aspects of the large-scale increase in the use of cloud services and the risks that may accompany it. This chapter is more technical than the other thematic chapters and is mainly intended to help the reader anticipate possible incidents.

The Appendix describes the process of creating the CSAN.

 [Back to Table of Contents](#)

.....
*Numerous cyber incidents with intentional
and unintentional causes*



2 Retrospective

In the period from March 2020 to March 2021, numerous cyber incidents occurred in or in relation to the Netherlands, with both intentional and unintentional causes. None of these incidents led to social disruption. The impact of incidents varied widely, from a brief interruption of processes to the need to rebuild parts of the technical infrastructure. Cyber incidents not only have an impact on direct victims, but also on (chains of) suppliers, customers and members of the public who use the services of (public) organisations. In public organisations, there is no choice of service for members of the public, but rather a dependency relationship. In a number of incidents, the interests of individual and sometimes vulnerable members of the public have been affected, such as when personal data has been stolen. The following are recurring themes in an open source summary of incidents: COVID-19 as an opportunity for malicious actors; targeting facilities for remote working; deliberately denying access to processes; attacks on organisations in supply chains; data breaches, and finally, process outages. The Retrospective chapter is structured around these themes and provides concrete examples of incidents that have occurred.

2.1 COVID-19 an opportunity for malicious actors

The global COVID-19 pandemic strongly influences the Retrospective. The pandemic was and is being exploited by malicious actors. For example, state actors have used digital espionage activities in their search for information on medical knowledge and policy follow-up on COVID-19. These include research data on treatment, test results and vaccines, information on the estimated spread of infection and possible policy strategies. Criminals are exploiting the COVID-19 pandemic for attacks through phishing, ransomware and distribution of malicious apps. They are increasing the pressure to pay ransom by launching ransomware attacks on the processes of organisations that are crucial in the fight against COVID-19, including patient care facilities, medical suppliers and laboratories. For example, the Dutch healthcare sector was advised by Z-CERT^{II} in close cooperation with the NCSC following a ransomware attack on a medical supplier. The need in society for information and financial support under COVID-19 has been exploited frequently in phishing campaigns as a stepping stone for attacks. These were often pre-existing malware campaigns in which the theme of emails, malicious attachments and links were adapted to COVID-19. In the

Netherlands, for example, SMS phishing (smishing) has been observed, in which malicious parties pretend to be the National Institute for Public Health and the Environment (RIVM). According to Z-CERT, the effect of the phishing campaigns in the Dutch healthcare sector has been limited. Finally, the hacking of the European Medicines Agency (EMA) in December 2020 showed that both medical knowledge and information on policy monitoring had been misused in a disinformation campaign.

II Z-CERT has been designated as the computer emergency response team for the entire healthcare sector (Network and Information Systems Security Act) since January 2020.

EMA documents used for disinformation

In December 2020, the EMA became the target of a hack and leak attack. At that time, the agency was working on the approval of two COVID-19 vaccines. In late December 2020, parts of EMA documents appeared on web forums such as the Russian darknet forum Rutor. The leaked files had been partially altered and provided with commentary and context that is intended to make it appear as though fraudulent research is being conducted by the EMA. Email conversations had also been altered to give the impression that EU authorities wanted to put pressure on the EMA to accelerate the approval of vaccines. It therefore seems that obtaining intelligence was not the actor's sole intention, but that the aim was also to fuel a disinformation campaign targeting public confidence in vaccine developers and European institutions. According to open sources, the attack on the EMA was made possible by a lack of cyber hygiene, which allowed the two-factor authentication to be circumvented.

2.2 Targeting facilities for remote working

In March 2021, the Dutch government called on the working population to work from home whenever possible. Technical facilities to work remotely became necessary for continuity of business operations. In addition, the potential for exploiting vulnerabilities increased; for the attack surface had been greatly increased. Because of the many home-based workplaces, more vulnerable systems are connected to the Internet and digital processes take place at home. This has increased both the likelihood and the impact of a cyber incident with or through home working facilities.

Remote working facilities can be divided into three categories:

- Online meeting facilities such as Zoom, Teams, Jitsi, Google meet, and Webex.
- Facilities to remotely control the office environment or office applications such as Virtual Desktop Infrastructure (VDI), Remote Desktop Service (RDS) and TeamViewer.
- Systems to connect to the office at network level: VPN solutions.

Vulnerabilities and non-secure use were observed in all categories during the reporting period. For example, a journalist managed to gain access to a secret European defence meeting in November 2020. In June 2020, a vulnerability was found in TeamViewer with which malicious parties could gain increased rights and access to files on a system, allowing them to gain unauthorised access to information or make processes inaccessible. VPN and VPN-SSL solutions are constantly being scanned for vulnerabilities by malicious parties. The NCSC has regularly warned of increased scanning activity for VPN vulnerabilities in Pulse Connect Secure and Fortigate SSL, among others, by state actors. Foreign CERTs such as CISA have also regularly warned against this.

Not all incidents involving home working facilities have a similar impact. This depends on the type of misuse, the processes involved and the actor. Misuse of meeting facilities is usually carried out by cyber vandals. Misuse of underlying network solutions is not readily detected, is more likely to be persistent and forms a greater risk to processes. Exploitation of existing vulnerabilities has more impact due to the increased attack surface. The Citrix vulnerability that was extensively reported in CSAN 2020 has, a few months after the patch was released, still made new victims. New vulnerabilities in Citrix products were also revealed in June 2020, which were classified by the NCSC as high/high (high risk of exploitation and major damage).

Dutch organisations still infected six months after Citrix crisis

'De Volkskrant' reported on active exploitation of the Citrix vulnerabilities at Dutch companies, even after the leaks had been fixed. According to an analysis by Fox-IT, at least 25 Dutch companies have been infected via a leak in Citrix, including a pharmaceutical company and an organisation for the care of the disabled. It concerns a vulnerability in the Citrix NetScaler and ADC. Companies that had patched were also found to be infected. In some cases, it was not one criminal or group that had left a backdoor, but several. Fox-IT saw servers with as many as four or five backdoors. In June 2020, Fox-IT discovered that there were still 39 servers in the Netherlands that were infected. This does not mean that 39 companies are affected; some companies use multiple servers, for example.

State actors actively scanning for vulnerable VPN systems

State actors are actively seeking vulnerable VPN systems in networks of both (semi-) public and private parties. Vulnerable systems can also be used at a later time to launch a larger attack, on the entire chain for example. The NCSC received reports from various sectors about observed scanning activities and that some organisations were vulnerable, but that no exploitation had taken place. Foreign CERTs have also observed increased scanning activity for VPN vulnerabilities in the period March 2020 to March 2021. The following VPN vulnerabilities, among others, have been frequently exploited to gain access to a system: Pulse Connect Secure (CVE-2019-11510), Fortigate SSL (CVE-2018-13379, CVE-2018-13382 and CVE-2018-13383) and Citrix ADC (CVE-2019-19781). Meanwhile, patches exist for these VPN vulnerabilities and several warnings and control measures have been published. Nevertheless, there are still organisations in the Netherlands that use vulnerable VPN solutions. Organisations in the SME sector in particular have not yet resolved the vulnerabilities.

There is also a fourth (unofficial) category of remote working facilities: shadow ICT; solutions that are not part of the approved office applications, but which are used for work-related purposes. Examples are messaging apps, private email and private cloud applications. This category has also gained in importance because, as a result of COVID-19, there was a need for workarounds to quickly share information and documents. In November 2020, in a report on safe working from home, the Court of Audit pointed out the serious security risks that the use of shadow ICT can entail.

2.3 Deliberately denying access to processes

There are many ways to deliberately deny access to processes. The two most important are disruption with a DDoS attack and the use of ransomware.

DDoS: bigger, heavier and longer lasting attacks

In the reporting period, digital processes of Internet Service Providers (ISPs), the financial sector, education and public organisations were affected by DDoS attacks. Notable was the trend towards heavier and more complex attacks combining multiple attack vectors. Exceptionally heavy DDoS attacks were carried out in the month of August 2020 with peaks of up to 260 Gigabits per second. The attacks mainly targeted the shared infrastructure at ISPs. In a number of cases, not only customers experienced disruptions in their online services, but also the providers themselves. In its annual DDoS data report, the Dutch Internet

Providers Management Organisation states that DDoS attacks have become more powerful and complex in 2020, while the number and duration of DDoS attacks has also increased. Attackers are said to have above-average skills. They target the underlying infrastructure and the attackers often change misused protocols, which makes defending difficult. Despite this, the Anti-DDoS Coalition says that through cooperation, it has been able to limit the consequences of the DDoS attacks in the Netherlands.

DDoS has traditionally been the tool of cyber vandals or individuals who launch attacks out of frustration with the target organisation. There is also the phenomenon of RDDoS (Ransom Distributed Denial-of-Service): extortion using a DDoS attack as a means of applying pressure. Worldwide warnings were issued about DDoS extortion emails sent to financial institutions in various states, including the Netherlands.

Several providers suffered DDoS attacks; but no major disruptions

In August 2020, several Dutch providers experienced DDoS attacks. Several providers were temporarily taken down as a result. In the case of a provider from the province of Zeeland, the attack meant that internet, TV and telephony were unavailable in large parts of the province for some time. This also caused a regional PIN malfunction.

Ransomware leads to inaccessible processes and irreversible damage

During the reporting period, actors held key systems hostage with ransomware attacks. As a result, digital processes of public organisations, among others, (largely) came to a standstill and irreversible damage was caused to ICT systems. The method used to perpetrate ransomware attacks has changed significantly in recent years. There has been a move towards Big Game Hunting, compromising carefully selected organisations. These are usually wealthy organisations, responsible for continuity of processes or in possession of unique data. The pressure on the victim is greatly increased by the ransomware being deployed at the most strategic location in the network. In addition, the means of applying pressure has also changed. Where initially data or systems were encrypted, now data is also stolen and threatened to be made public. This is why data breaches are regularly seen as significant collateral damage in ransomware attacks. There are also examples of actors who accompany a ransomware attack with a threat of a DDoS attack as an additional means of applying pressure. According to the FBI, telephone threats with physical visits to the home are also occurring in ransomware attacks. The combination of these strategies poses an increased risk to organisations where many people depend on, where unique and high-quality knowledge is generated and where responsibility for processing

personal data on a large scale is borne. This explains the selection of targets such as knowledge institutions (universities and colleges), hospitals and pharmaceutical companies and public organisations such as municipalities.

In February 2021, several knowledge institutions in the Netherlands were attacked by criminal actors. Among others, the Netherlands Organisation for Scientific Research, the University of Amsterdam (UvA) and the Amsterdam University of Applied Sciences (AUAS) were hit by cyber attacks, with the attacks on the UvA and AUAS being successfully repelled.

Although various ransomware activities against public and private organisations within the healthcare sector have been observed worldwide, there are no concrete indications of state control. The Dutch security and intelligence services AIVD and MIVD consider that these sabotage activities have most likely been criminal in nature so far.

Hof van Twente municipality victim of ransomware attack

In December 2020, the municipality of Hof van Twente was hit by a ransomware attack. The attack meant that several service processes could not be carried out, and the municipality could not be contacted by e-mail. Data stored on servers was inaccessible, data in the cloud remained available. According to the municipality, hackers did not make any data public and no ransom was paid. However, the municipality will have to rebuild the ICT infrastructure, which is expected to take two years. In early March 2021, it emerged that part of the administration could be restored after all. It also turned out that the password used to secure the ICT environment consisted of the easy-to-crack 'welkom2020'.

2.4 Attacks on organisations in supply chains

An attack on supply chains does not target a specific organisation, but one (or several) weak spots in the chain. The actor can hit many organisations via that weak spot(s). Conversely, every organisation has to deal with supply chains and therefore with vulnerabilities to attacks via these chains. There is no such thing as a single supply chain attack; it is a collective term in which different types of chains can be distinguished. There are also attacks on suppliers of semi-finished products that disrupt deliveries in the chain.

The CSAN 2020 also addressed attacks on supply chains, which at the time were mainly seen as a stepping stone to (more) interesting targets. These attacks have increased in number, scale and complexity in recent months. Here, too, accelerated digitisation plays a role. For chains to function efficiently, it is necessary to

share more and more information with chain partners. This makes cyber risks also a risk of the chain, because malicious parties will deliberately seek the weakest link. Globally, the supply chain strategy has been used by various actors, including against companies involved in vaccine development or transport. The most prominent example of an attack on the ICT supply chain, however, was the vulnerability introduced into SolarWinds' Orion software.

SolarWinds: ICT supply chain attack with global impact

In December 2020, it was revealed that attackers had introduced a vulnerability into an update to SolarWinds' Orion software. This company makes software programs for government bodies and major companies to monitor and manage ICT environments. According to SolarWinds, the intentionally created vulnerability has the underlying purpose of compromising the systems of customers using the affected version of SolarWinds Orion. The vulnerability was actually exploited at several US government agencies. Several cybersecurity and tech companies with global customers, such as FireEye, Mimecast and Microsoft, have reported being compromised via the vulnerable version of Orion. Microsoft stated that the attackers' ultimate goal was probably to gain access to the cloud services of the targeted organisations. Experts assume the motive was espionage. The vulnerable version of SolarWinds has also been found in the Netherlands, including within the government and critical processes. The NCSC has not detected any exploitation as yet. In April 2021, the US attributed the SolarWinds campaign to the Russian intelligence service SVR (APT29). This attribution was supported by the EU and the Dutch government.

2.5 Large amounts of business- and privacy-sensitive information made public

Digital processes are partly concerned with collecting, selecting, processing and distributing information. Virtually any disruption of a digital process therefore results in data breaches. The most important distinction is between data breaches that occur deliberately (through the actions of a malicious actor) and unintentional data breaches, leaving behind a USB stick for example. In total, tens of thousands of data breaches (deliberate and unintentional) occur in the Netherlands every year. Last year, 23,976 data breaches were reported to the Dutch Data Protection Authority (DPA). These can be extensive: in March 2021, it emerged that private data of possibly millions of Dutch car owners had been stolen and were for sale on the Internet. This includes name and address details, e-mail addresses, vehicle registration numbers, telephone numbers and dates of birth. The data was stolen from RDC, an ICT service provider for car companies.

Public organisations are among the largest data processing entities and are therefore strongly represented in the Dutch Data Protection Authority's data breach summary. Unintentional data breaches often occur due to a lack of knowledge or awareness. It should be noted here that an increase in awareness can also lead to more reports, because data breaches will be recognised sooner as a result. Data breaches can lead to silent disruption, as data that has been stolen can come into the possession of malicious third parties and can be the basis for cyber attacks. The impact of a data breach is not always immediately clear. Sometimes it only becomes apparent in retrospect, when leaked data is misused for espionage purposes, for example. Data breaches can affect the organisation where the breach occurs, but often others, including customers or members of the public, are the victims of the misuse of the information that has been made public.

Data theft from the GGD's Corona system

The Municipal Health Service (GGD) processes hundreds of thousands of Coronavirus tests every week, storing personal data such as citizen service numbers, dates of birth and address details in various systems. In November 2020, it became known that GGD employees had accessed the files of (at least) two Dutch celebrities without authorisation. At the time, the GGD announced that anyone working with the database(s) must sign a confidentiality agreement to prevent misuse. In January 2021, it was revealed that for months there had been large-scale trade in the private data of members of the public from the GGD's Coronavirus systems. These systems had serious vulnerabilities, which had been known for some time. Employees had access to data they did not need, there was no structural monitoring of (mis)use of systems and data could be exported. In the end, it turned out that the data of 1,000 people had been accessed without authorisation, stolen and possibly sold, via screenshots from the CoronIT system. A total of seven suspects were arrested. This was an insider threat. Data breaches such as these can have an impact on the willingness of members of the public to be tested or vaccinated and thus on the reduction of COVID-19 infections.

Private organisations also process large amounts of data and there have been incidents of large-scale breaches in the past year. Hackers managed, for example, to gain access to a database of the Royal Dutch Cycling Union containing data of 90,000 people. Following unauthorized access to a Transavia mailbox, the data of tens of thousands of customers who travelled with the airline in January 2020 was leaked.


2.6 Non-functioning processes due to system failure

A cyber incident leads to disruption of one or more processes. This may be a deliberate disruption by a malicious actor. It may also include system failures due to natural or technical causes or due to unintentional human action. In terms of concrete impact, it makes little difference whether a process is unavailable due to disruption by a malicious actor or due to system failure.

The past year has seen regular process disruptions at Internet Service Providers, financial institutions, the telecom sector, hospitals and the public sector. At the GGD, system overloading disrupted its digital processes, but also limited national insight into the number of infections. This type of system failure has the immediate consequence that digital processes of critical providers that depend on these organisations also cease to function. Thus, system failures have a domino effect. The aforementioned accelerated digitisation means that analogue and physical fallback options are disappearing at an equal pace.

ICT malfunction at various hospitals due to problems with hosting provider

On 8 October 2020, ICTZ, an ICT service provider for Dutch hospitals, was hit by a malfunction. The immediate effect was the disruption of digital processes at several ICTZ clients. Patients could not log in digitally at the hospital and could not view their online records. General practitioners were also unable to log in at a number of hospitals due to the malfunction. ICTZ announced in a statement that the problem lay in the connectivity with the data centre where ICTZ itself was a customer. The hosting provider solved the malfunction by repairing the platform and replacing components in the data centre.

 [Back to Table of Contents](#)

.....
*The pandemic accelerated
process of digitisation*



3 COVID-19: current events influence threat picture

Current events, which receive a lot of attention worldwide, influence the threat picture. Since the beginning of 2020, COVID-19 has been one of the most important current events worldwide. The digitisation of society has accelerated as a result of COVID-19. This means that cyberspace will be used even more heavily than before the pandemic. Digital processes provide resilience and continuity during the pandemic, but cybercriminals and state actors are quick to exploit new vulnerabilities. Cybercriminals have been running phishing and malware campaigns with a COVID-19 theme. State actors have used the pandemic for espionage purposes. In the future, actors will continue to use global events to carry out attacks. This has once again demonstrated the permanent nature of the cyber threat. In the Netherlands, the pandemic has also led to increased attention to risks and the (accelerated) implementation of measures by companies and organisations.

Digital processes provide resilience and continuity

Society has been confronted with the consequences of COVID-19 over the past year. The deaths, the closure of schools, restaurants, cultural and sports venues, the temporary cessation of contact professions and working from home have major economic and social consequences. Processes with a digital component ensure resilience and continuity in today's pandemic. Thanks to the further digitisation of society, commercial, educational and social activities that would otherwise have come to a complete standstill as a result of the pandemic could still (partially) take place.

Digital infrastructure crucial during the pandemic

Today, even more than before the pandemic, the continuation of daily life depends on cyberspace. Major shifts and peaks in the demand for data and an increase in mobile phone traffic in the Netherlands show the crucial importance of the availability of the digital infrastructure. Disruption or system failure of cyberspace can lead to disruption of daily life or even to social disruption.

Heavy reliance on cyberspace

The digital society offers plenty of opportunities and solutions, especially during COVID-19, but the large-scale shift to 'living and working online' also makes us vulnerable. The rapid transition to mass working from home has led to an increase in the attack surface and the various ways in which an attacker can strike, increasing the likelihood of successful attacks. Secure equipment configured by the ICT department is not always used. More work is being done with home devices for which people themselves are responsible, including in the field of security. Working from home on a massive scale increases the chance that the sensitive or confidential data of organisations and companies will end up outside the usual secure network. The digital processes of organisations involved in combating the pandemic also pose a risk. In the past year, the GGD has had a number of incidents that have made the news (see the Retrospective). From the various incidents, the picture emerges that confidentiality and privacy were subordinate to getting the business process up and running. The great social importance of acting quickly during the pandemic, combined with a large amount of personal data on members of the public, made the potential for misuse of Coronavirus-related systems great.

Actors exploit current events

Actors are opportunistic and act quickly when it comes to exploiting new vulnerabilities in processes, technology and human behaviour. Parallel to the global spread of the COVID-19 virus, the assessment of the threat also changed. Since the beginning of the pandemic, several COVID-19 themed cyber attacks have been observed, using different *modi operandi*. Cyber attacks have been carried out on hospitals, research institutes and the World Health Organisation (WHO). Not only was the healthcare sector targeted, but governments and companies also had to deal with various attacks. The Police, the Public Prosecutor's Office and Europol warned of the various forms of misuse, ranging from cybercriminal attacks to distribution of disinformation.

COVID-19 lends itself to social engineering

Since the outbreak of COVID-19, actors have been exploiting people's need for information and their fear. The WHO warned about phishing campaigns with a COVID-19 theme. A phishing attack is aimed at stealing system login details or other sensitive information by persuading recipients of a phishing message to click on a malicious link. Cybercriminals use social engineering tactics to do so: they play on emotions such as fear, emphasise the urgency of their message or play on positive emotions, such as collegiality. Various ransomware variants were sent via phishing. Ransomware attacks can also take place by exploiting vulnerabilities in systems. Targeted ransomware attacks pose a serious threat to the healthcare sector. The healthcare sector can be a lucrative target for cybercriminals, as preventing disruption in this sector is of great social importance. Several European hospitals fell victim to ransomware attacks. In the past year, Dutch healthcare institutions also received large-scale malware via email that was configured to download ransomware. Despite the fact that they were targeted, no impactful ransomware attacks against Dutch healthcare institutions were observed in the reporting period.

The pandemic also created intelligence needs

On 11 March 2020, the WHO declared that the outbreak of COVID-19 had officially developed into a pandemic. Shortly afterwards, the British NCSC and US authorities warned of espionage campaigns by state actors. The AIVD found that there is an increased digital espionage threat worldwide towards the pharmaceutical and medical industries, and research centres developing medicines, antibodies or vaccines in relation to COVID-19. Dutch companies and research institutions involved in the prevention and combating of COVID-19 are likely targets of this digital espionage. There is also a possibility of Dutch government agencies that coordinate the prevention and combat of COVID-19 becoming victims of digital espionage. In addition, it is possible that cyber attacks will be carried out on (central) databases in which personal data of Dutch members of the public are stored within the framework of COVID-19.

A motive for espionage could be to promote the public health of one's own country. The motive may also be economic in nature. Stolen knowledge can benefit the domestic pharmaceutical industry or other research and development organisations. The impact of the current digital espionage threat will last longer than the pandemic. Both established and emerging state actors can use the stolen knowledge to gain an economic and strategic advantage even after the pandemic. It is likely that COVID-19-related cyber attacks will continue as long as the pandemic continues and vaccines and treatment methods are not yet available worldwide.

Increasing polarisation could acquire a digital component


Current issues, including the COVID-19 measures, demonstrate or give rise to polarisation in society. This polarisation can lead to extremist behaviour, but also to cyber incidents. While a large part of the population supports the COVID-19 measures, others fiercely oppose them. Ad hoc coalitions of opponents of various topics may arise around various themes. An (online) context has been created in which the threshold for resorting to extremist behaviour has been lowered. This context reinforces polarisation, and in some cases, leads to hardening, intimidation or (incitement to) violence. The curfew riots are an example of this. It is conceivable that polarisation will also have a digital component in the form of cyber attacks. For example, opponents of the COVID-19 restrictions could express their dissatisfaction by disrupting digital processes, such as by launching DDoS attacks against government bodies or parties with different ideas. They might also try to hack into public authorities to get information that could put an authority in a bad light. The hack and leak operation at the European Medicines Agency has shown that actors use stolen information in a manipulated form to spread disinformation (see the Retrospective). The Threat Assessment for State Actors explains how state actors use disinformation to influence, including in relation to the COVID-19 pandemic. It is extremely difficult for the general public to distinguish manipulated information from real information. Differences of opinion regarding the value of information can thus also contribute to processes of polarisation.

COVID-19 also leads to attention to cybersecurity

Public reports and an expert consultation show that the pandemic in the Netherlands has also led to increased attention to cybersecurity risks and the (accelerated) implementation of measures by companies and organisations, in education for example. For example, Z-CERT aims to make the healthcare sector more resilient to digital threats such as phishing and ransomware. The NCSC helps Z-CERT to provide the healthcare sector with the best possible knowledge and (threat) information. The NCSC has shared various (security) advice and threat analyses with its target

groups, with the aim of making them more resilient to COVID-19-related digital threats. Due to the increased threat to the healthcare sector, the NCSC's target group has been broadened by a temporary extension of the Network and Information Systems Security Act to include research centres, pharmaceutical companies and production companies that are conducting research into the development or have a role in the production of a vaccine against COVID-19. Therefore, the NCSC has also offered its services to this type of organisation.

The Dutch education sector has also invested more in cybersecurity in the past year. The ransomware incident at Maastricht University and the pandemic were important reasons for this. The Dutch public is also increasingly aware of risks and how to limit them. On 15 December 2020, EU Council Conclusions were adopted on strengthening the resilience of the EU and its Member States and combating hybrid threats, including disinformation, in the context of the COVID-19 pandemic. It is difficult to assess the extent to which these initiatives to increase resilience sufficiently counterbalance the further developed threat.

 [Back to
Table of Contents](#)

.....
*Financial gain main motivation
of cybercriminals*



4 Ransomware risk to national security

Ransomware - the criminal act of encrypting files and systems in order to demand a ransom for making them accessible again - has evolved in such a way that it poses a risk to the national security of the Netherlands.^{III} In previous editions of the CSAN, the NCTV and the NCSC had already identified ransomware as a phenomenon that can have a major impact on society. It also has a solid revenue model and is part of an extensive, mature, cybercriminal economy. Tracking down and prosecuting the perpetrators behind ransomware is therefore not enough: increasing resilience and disrupting the revenue model deserve just as much attention. In this chapter, the Police describe the phenomenon of ransomware at perpetrator level, based on observations made by investigators and supplemented by open sources. The result is a picture of the current nature and scale of ransomware, the cybercriminal ecosystem of which it is a part and the threat it poses.

The cybercriminal ecosystem

Your files have been encrypted! To decrypt the files, follow the following instructions... Behind this dreaded message is much more than the cybercriminal sending it. Often, the deployment of ransomware is the most visible (and painful) step in a much larger process in which many criminal actors and activities combine to form a complex whole.

A mature cybercriminal economy

The main motivation of cybercriminals is financial gain. This is underlined by the fact that this form of crime cannot be separated from a large underground service economy. Specialisation and diversification play an important role here: almost every step for both committing and protecting cybercrime is offered as a service. The cybercriminal ecosystem can therefore increasingly be characterised as a mature, global economic sector where supply and demand come together in cybercriminal forums, among others, and where rational economic trade-offs are made between investment, risk and return. This service makes cybercrime accessible to a wide range of perpetrators. ICT (and its outsourcing) has a significant amplifying effect here: with minimal effort and resources, a perpetrator can carry out a large number of criminal acts worldwide and thus achieve maximum effect. This form of scalability is what distinguishes cybercrime from other forms of crime.

Cybercrime is also highly transnational. Perpetrators, service providers, victims and used or misused infrastructures can be located all over the world, which poses challenges in terms of detection, prosecution and the fight against it. The Netherlands stands out as a country where an above-average amount of cybercriminal infrastructure is hosted. This is evident from numerous investigations and foreign requests for mutual legal assistance.

The extent to which and the way in which perpetrators make use of cybercrime services varies from one category of perpetrator to another. Three perpetrator categories can be distinguished: cybercriminal service providers, dependent perpetrators and autonomous groups. This rough classification does not alter the fact that these categories may overlap.

Cybercriminal service providers

These service providers offer Cybercrime-as-a-Service (CaaS). They offer their products and services primarily on underground, online platforms such as closed cybercriminal forums, but also on so-

.....
 III Ransomware can also be used by state actors with the aim of causing damage to and failure of processes (examples are WannaCry and NotPetya from 2017). This chapter focuses specifically on the use of ransomware by criminal actors and the risks it poses to national security.

called booter and stresser sites or Telegram channels. They are often able to optimise their business processes, automate them and make them very user-friendly, which contributes to the scalability of cybercrime. For example, Webstresser, a DDoS-as-a-Service provider taken down by the Police and the Public Prosecutor's Office, carried out around 4 million DDoS attacks with primarily criminal motives on over 150,000 users worldwide in the space of six months.

Dependent perpetrators

These are the main customers of cybercriminal services. This is a very diverse and large category of perpetrators that can operate both individually and in groups and commit various forms of cybercrime. These perpetrators do not have high technical skills to develop malware themselves, for example. To be able to commit cybercrime and protect themselves from detection by law enforcement agencies, they are therefore largely dependent on products and services from cybercriminal service providers.

Autonomous groups

This category of perpetrator is smaller in size, but responsible for often sophisticated attacks with a high degree of organisation and global impact. These are mostly loose, non-hierarchical partnerships that have been active for a long time and therefore have a lot of capital and expertise and are able to conduct long-term cybercriminal attack campaigns. Such campaigns require a long lead time, in the beginning characterised by a lot of investment and little return. If successful, however, the proceeds could run into millions of euros. These groups are autonomous because they develop and carry out their cybercriminal process mainly on their own. An exception is the purchase of very specific and specialised services, such as the laundering of large financial flows.

In recent years, there has been increasing cooperation between autonomous groups. This involves combining different specialities into combined attacks that, through their persistence, complexity and sophistication, approach the level of cyber attacks by state actors. However, autonomous groups differ from state actors as they act out of individual self-interest and not out of national (geopolitical) interests. In some cases, however, there is overlap or cooperation between these two actor groups. In addition to the transnational nature of cybercrime, this intertwining makes the investigation and prosecution of especially serious, organised cybercriminals even more complex.

Ransomware as a solid revenue model

Ransomware offers cybercriminals of all categories a solid and attractive revenue model. The first forms of ransomware were developed as early as the mid-1990s. For the first few years, this form of virus lay dormant, as it proved difficult to receive the ransom paid in a way that was safe for the criminal. The introduction of Bitcoin in 2009 changed this. Cryptocurrencies offer ransomware attackers the opportunity to have the victim transfer money in a fast, irreversible and relatively anonymous way. Moreover, there is no monitoring of transactions and payouts, which makes it extremely attractive for criminal use. Within five years, ransomware had developed into a lucrative revenue model, which was further strengthened by the emergence of the Ransomware-as-a-Service (RaaS) phenomenon.

Ransomware kill chain

A ransomware attack is not an isolated event, but is often part of a wider process in which several steps can be distinguished:

- It starts with obtaining access to a network, access that may later be re-sold.
- Then consolidation of the position within the network takes place, and additional malware is installed.
- After that, the choice can be made to siphon-off valuable, sensitive information. For example, to offer it for sale on the underground cybercriminal market, or as a means of extorting the victim through (the threat of) publication.
- The deployment of ransomware is often the part of the attack that has the greatest impact.
- The final step consists of any final financial settlement of the extortion: the negotiations between the perpetrator and the victim, the payment by the victim if necessary, the transfer of the ransom paid, and the laundering by the perpetrator.

Figure 1: The ransomware kill chain



Diversification and specialisation can also be seen here. Each step in this ransomware kill chain has specialists who either offer this as a service or cooperate with other specialists to carry out highly effective combined attacks.

Here, too, clear cost-benefit considerations apply. In a targeted attack, factors considered in determining a ransom demand include the effort required to penetrate and gain control of a network, the risks to the attacker of being discovered, the capital strength of the victim and the extent to which business continuity and/or sensitive data play an important role for the victim. Moreover, the higher the general willingness of victims to pay, the higher the demands will be. The Police also note that an appropriate portion of the ransom paid by victims is directly invested in new attack infrastructures, and thus in attacking new victims.

Ransomware-as-a-Service: a plague for SMEs

The majority of ransomware attacks are characterised as RaaS. Ransomware developers found this to be a way to spread their malware on a large scale without running any risks themselves. RaaS offers the customers of this product the opportunity to apply ransomware to networks or systems even without significant programming skills. These customers, also known as affiliates, fall into the dependent perpetrators category. For each successful ransomware attack, they pay the ransomware developer a fixed, agreed percentage of the ransom paid.

The victims of these mostly indiscriminate attacks are generally small to medium-sized enterprises and increasingly public institutions such as local authorities. These are victims with generally low to limited digital resilience, where relatively little time and effort needs to be invested by the attacker. In April 2020, Help Net Security estimated, following a survey of more than 500 executives within international SMEs, that 46% of SMEs had, at some time, been victims of ransomware.

Big Game Hunting: customisation for maximum yield

These are targeted attacks on large organisations, whereby customised attacks are carried out in order to achieve maximum financial gain. It is mainly autonomous groups - often Eastern European - that (are able to) carry out such attacks. Ransomware is often 'just' a part of a process with several combined attack techniques.

In this process, different groups, each with their own specialisation, often work together, which significantly increases the threat. The Emotet botnet, for example, which was taken down by the Police and the Public Prosecution Service in 2021, infected more than a million systems worldwide with attack methods that were not very sophisticated. In many cases, computers were infected with spam without being targeted. This was possible because the investigation revealed that victims' often low level of digital resilience could be exploited to the full. A striking example: finding two-factor authentication on a system was already a reason not to continue the attack. The next steps in the attack process were often targeted and advanced. The group behind Emotet manifested itself as a service provider by reselling access to networks within a select customer base. Somewhere in this process, a form of triage also took place, whereby the wealthiest networks were ranked higher. The customers, in the sense of other autonomous groups, could then install their additional malware or have it installed. For example TrickBot, which was used to consolidate the position and steal information. Ultimately, using Ryuk ransomware, actors were able to target ransomware on these networks at strategic locations, where they were able to make a realistic assessment of what the maximum ransom demand could be. The publication or threat of publishing the previously stolen data could serve as an additional means of applying pressure.

Investigations reveal that such cooperation is becoming increasingly complex. An attack on a network can therefore involve different actors, who take on different roles, whereby the distinction between perpetrating acts and providing services becomes significantly blurred. Also, actors can choose different malware families in different circumstances, in a plug-and-play manner. This makes its detection, but also its mitigation, particularly complex.

Damage as a blind spot

The total economic damage of ransomware, in terms of ransom paid, loss of business continuity, consequential losses and recovery costs of all attacks added together, is difficult to determine. Estimates of the global damage run into billions of euros annually, with a sharp increase in recent years due to an increase in both RaaS and Big Game Hunting attacks. The cost of damage to the Netherlands is not known. This blind spot has several causes. In addition to the highly transnational nature of cybercrime, which makes it complicated to gain an impression of the damage to the Netherlands, the willingness of victims of cybercrime to report and notify is structurally low.

However, several indicators show that the economic damage of ransomware will be considerable for the Netherlands too. According to the company Coveware, the estimated average ransom demand peaked at around EUR 200,000 in the third quarter of 2020. This is the average across all attacks worldwide: both RaaS attacks where the demand may be a few thousand euros, and Big Game Hunting attacks where the demand may be in the millions. In 2020, a record amount of 25 million euros may even have been demanded in the US or Europe. According to some estimates, in around 70% of all ransomware attacks, ransoms are paid by the victim, although the Police cannot verify this figure. The Police do note, however, that in the Netherlands too, both demanded and paid amounts are now running into millions of euros.

However, the total cost of overcoming a ransomware attack is often higher than the amount of ransom demanded. The Not-Petya ransomware attack in 2017 shows how extensive the total damage of a very thorough attack (in this case by a state actor) can be. For example, for the logistics company Maersk, which was also hit hard in Rotterdam, this amounted to more than 200 million euros.

Ransomware and national security

Ransomware attacks pose a risk to national security when it comes to the continuity of critical processes, the leaking and/or publication of confidential or sensitive information and impairment of the integrity of cyberspace; elements that are mentioned in the Integrated Risk Analysis for National Security and the Threat Assessment for State Actors. This is especially true of the threat posed by thorough, combined attacks in the Big Game Hunting category. National security is at stake when the target of such an attack is part of the critical national infrastructure (including the central government and all identified critical processes) and the attack disrupts the continuity of critical processes. A ransomware attack can, for example, affect the office automation of such an organisation. If access to the process automation is via the office automation, this enables the attacker to also reach the critical processes to install ransomware there.

Although targeted ransomware attacks on critical processes have not yet occurred in the Netherlands, they are already happening abroad. In the United States, for example, federal government agencies, the Police and the energy sector have been affected. In addition, ransomware attacks in both the United States and the European Union during the coronavirus pandemic severely hampered hospitals, COVID-19 research institutions and a vaccine distribution centre.


The combination of ransomware with the publication or resale of sensitive information stolen during the attack is also becoming increasingly common in the Netherlands. The attack on the Netherlands Organisation for Scientific Research (NWO) in early 2021, where internal documents were published on a leak site set up especially for this purpose, also shows that this could affect the position of the Netherlands as an innovation country.

Ransomware attacks on local government authorities, such as the attack on the municipality of Hof van Twente in December 2020, are a deliberate attack on the integrity of the government's cyberspace. This may affect the continuity of government services and public trust in them.

Breaking the ransomware kill chain

The ransomware kill chain underlines the fact that a ransomware attack is not an isolated event but is often part of a wider process. Cybercriminals make a clear cost-benefit analysis of their victims at every stage of this process. This is why the Police and the NCSC advise victims of ransomware attacks not to pay, as ransom payments maintain a revenue model for criminals. Viewing ransomware not only as a technical problem, but also as the economic side of a cybercriminal attack, makes room for a more holistic approach to the problem. Each stage of the ransomware kill chain offers opportunities to intervene, both offensively and defensively. Offensively by fighting the main perpetrators and service providers internationally, such as taking down the Emotet botnet and tracking down the criminals responsible. Or by enabling victims to decrypt their files for free, as is possible with NoMoreRansom. Defensively by boosting resilience for all phases of the kill chain and thus limiting the attackers' opportunity to strike. This is sometimes possible with simple steps, such as applying two-factor authentication.

The most promising solution therefore lies in structurally increasing the costs for the criminals in relation to the benefits of ransomware. This is only possible if the Police, the NCSC and the Public Prosecution Service, together with public and private partners and (potential) victims, take a stand by proactively working together and by sharing information and insights in a targeted manner.

 [Back to Table of Contents](#)

.....
*Interwovenness with cyberspace
is vulnerable*



5 Violation of cyberspace poses a risk

Violation of (the security of) cyberspace poses a risk to national security. After all, important elements for the functioning of cyberspace are vulnerable to system failure and/or misuse. This violation is not a theoretical possibility; it is actually taking place. Recently, sophisticated attacks in ICT supply chains with a global impact once again came to light and vulnerabilities in globally used products were exploited. Boosting resilience to this is a limited possibility for individual states and organisations.

Cyberspace security affects national security

Digital processes intertwined with, and dependent on, cyberspace

All our digital processes are strongly intertwined with and dependent on global cyberspace. Digital processes, such as those of providers of critical national infrastructure, but also those of large and small organisations and members of the public, use the services and products of globally operating companies. Examples include products enabling remote working, managing and sending emails and storing and processing information with a cloud provider. This intertwining also applies to the technical infrastructure of the Internet, including undersea cables.

The fact that digital processes can make use of cyberspace and are intertwined with it has brought many benefits and continues to offer opportunities. On the other hand, it also poses a risk. The downside of this intertwining is complexity, dependence and vulnerability to misuse and system failure. Cyber incidents can therefore strike at the heart of our society and paralyse it for a short or long time. The security of cyberspace is therefore inextricably linked to national security.

The concept of cyberspace

Cyberspace is the complex environment resulting from mutually interconnected digital processes, supported by globally distributed physical ICT and connected networks.

Three perspectives can be distinguished:

1. Digital processes (process layer). This concerns the way in which organisations and people use cyberspace, and therefore the functionality of cyberspace for society and the economy.
2. ICT, networks and protocols (technical layer). This layer facilitates digital processes and includes diverse and coherent forms of hardware, software and networks. The Internet, as a network of networks is, by and large, that layer.
3. Risk management and/or governance (governance layer). This is about how digital processes and the technical layer can and should be controlled.

This chapter concentrates on the technical and process layers.

'Cyberspace' is a complex concept, with no consensus on the key elements for its functioning. From a technical perspective, TNO has identified six key elements for the functioning of the Internet. The Scientific Council for Government Policy focused on some of the so-called protocols and argued that the Internet has a global public core that transcends the interests of individual states and individuals. Furthermore, critical processes that help shape cyberspace and some global ICT supply chains are important elements. For example, many organisations use cloud services from Amazon and Microsoft and software suites such as Microsoft Office.

Important elements for the functioning of cyberspace

Important elements for the functioning of the Internet from a technical perspective (TNO)

1. Domain Name System (DNS): this is a system and network protocol that translates domain names into text (readable by humans) and IP addresses (usable by machines) and vice versa.
2. Border Gateway Protocol (BGP): this is the main routing protocol of the Internet.
3. Network Time Protocol (NTP): this protocol is widely used to control time synchronisation between computers or to control a network time standard (Network Time). GPS receivers are generally used as time sources for the NTP.
4. Physical internet infrastructure
 - Undersea cables and fibre optics: the physical cable infrastructure upon which the Internet depends consists of large undersea cables and land-based cables (mainly fibre optics).
 - Large Internet Exchanges: Internet Exchanges are a network platform for Internet Service Providers and other connected parties to exchange IP traffic.
 - Large data centres: there are increasing numbers of large data centres from which important (cloud) services are provided.
5. Trust services: many digital processes require data traffic to be authenticated by a trust service. This is done with the help of digital certificates issued by so-called Certificate Authorities. Such trust services may include authentication^{IV}, digital signing and encryption.
6. Elements crucial to the critical national infrastructure: this includes, on the one hand, the local physical infrastructure managed by network operators, which provides connectivity to users and, on the other hand, specific services, applications, peering connections^V or servers that are important to specific critical infrastructures.

Important elements that form the public core of the internet (Scientific Council for Government Policy)

7. Transmission Control Protocol (TCP): TCP ensures that the data arrives as it was sent and that any communication errors, both in the data itself and in the sequence of the data, can be caught.

8. Internet Protocol (IP): handles the addressing of internet traffic to ensure it arrives at the intended destination.

Other elements in the process layer considered to be important

9. The (Dutch) critical processes 'Internet and data services', 'Internet access and data traffic' and 'Voice services and SMS'. These processes help shape cyberspace and are therefore important elements for the way in which organisations and people (can) use cyberspace.
10. Global ICT supply chains: ICT supply chains consist of organisations that produce and sell hardware, software and (information) services, for example ICT service providers or software suppliers. Those that are important for the functioning of cyberspace and for which cyber incidents could affect the national security of the Netherlands have not been identified.

Technical layer of cyberspace vulnerable to system failure and misuse

Important elements for the functioning of cyberspace and the technical layer thereof are potentially vulnerable to system failure and/or misuse. Some examples are known of breaks in undersea cables that carry intercontinental internet traffic. These have led to (temporarily) reduced availability in the region where it occurred. An example of misuse is the interception of data traffic via undersea cables for intelligence gathering by state actors. CSAN 2020 mentioned changing DNS settings as an attack technique. This allows incoming network traffic from an organisation to be temporarily diverted and intercepted for espionage purposes, for example.

Violation of the technical layer can have an impact on national security. Suppose a core protocol were to be manipulated or some submarine cables sabotaged. This can then quickly and on a large scale - through the so-called cascade effect - affect some national security interests: economic security, physical security and social and political stability. This can also affect the confidence of members of the public and organisations in cyberspace and digitisation. Trust in the operation of cyberspace is essential, because that is what trust in digital processes is based on and because those processes play a key role in contemporary society and the economy.

^{IV} An act, process or method for verifying, for example, the identity of an organisation or a financial transaction.

^V Peering is a process where two Internet networks connect and exchange data traffic. Peering allows parties to handle data traffic directly without having to pay a third party. Retrieved from: <https://www.netnod.se/ix/what-is-peering>.

Boosting resilience against system failure and misuse of elements of the technical layer is a limited possibility for individual states and organisations. One reason is that cyberspace is an ecosystem consisting of many components and in which many parties play a role. CSAN 2020 explained that there are various reasons why cyberspace security does not come about automatically. The risks to the entire cyberspace and their impact on society are also difficult to fathom. However, the design of the Internet does take into account vulnerabilities such as component failures. This ensures a high degree of redundancy and flexibility in the infrastructure. The design of the protocols also takes account of the failure of parts of the infrastructure.

Exploitation of vulnerabilities in software and hardware worries

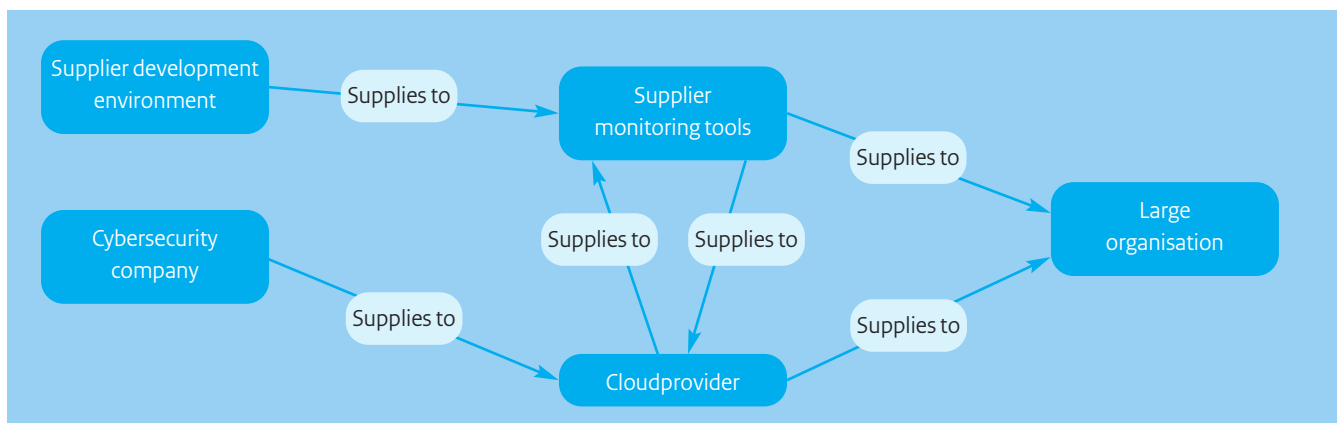
The exploitation of (zero day) vulnerabilities in widely used software or hardware causes concern because of the scale of the impact. For example, since the beginning of 2021, an actor has been exploiting (then unknown) vulnerabilities in Microsoft Exchange Server. These vulnerabilities potentially affected hundreds of thousands of organisations worldwide. When Microsoft announced the vulnerabilities on 02 March 2021, simultaneously with patches to remedy them, other actors also exploited these vulnerabilities at organisations that had not installed the patches (on time) (see Core CSAN). The NCSC stated that the consequences of the vulnerabilities in Microsoft Exchange Server were significant for Dutch organisations and companies. The NCSC found that as a result of these vulnerabilities, data was stolen, malware was installed, backdoors were built in and mailboxes were offered for sale on the black market. Malicious parties could possibly also have penetrated other systems via the vulnerabilities in Microsoft Exchange server. On 20 April 2021, Pulse Secure warned of an actively attacked zero day vulnerability in the company's VPN software that allowed remote attackers to take over vulnerable VPN servers. A security update was not yet available and, according to Pulse Secure, the security hole posed a very great risk to organisations. However, a workaround was published, as well as a tool that allowed customers to check whether their VPN

server had been compromised. Pulse Secure is used worldwide and the vulnerability makes many organisations vulnerable to exploitation by malicious parties.

Misuse of global ICT supply chains is common

As far as the process layer is concerned, the way organisations and people use cyberspace, it is misuse of global ICT supply chains that is of particular concern. The last three CSANs have highlighted the threat posed by an attack on ICT supply chains, termed 'chains' for convenience. Such an attack targets one or more vulnerabilities in chains rather than a specific process or organisation. An actor can affect many processes or organisations through weaknesses in chains. Conversely, these are intertwined with numerous chains and are therefore vulnerable to attacks through and within each of these chains. Those connections and thus vulnerabilities can be far-reaching (see Figure 2). Even in the highly simplified representation below, an actor who wants to attack a process of a large organisation can try to do so via the processes of four other organisations. For example, an attacker could try to attack a cloud provider via a monitoring tool provider and then a large organisation via that provider. Large-scale system failure within or of chains is also conceivable. A small number of tech companies have a dominant market position for certain types of service. The chance of system failure may not be very high, but if there is a failure, it will affect the digital processes of many states and organisations.

Figure 2: Simplified visualisation of an ICT supply chain



At the end of 2020, the so-called SolarWinds campaign^{VI} was discovered (see also the Retrospective). Here, an actor compromised software in ICT supply chains in various ways. Where attacks appeared to be targeted in the past, they appear to be widely used by the actor. This campaign potentially had a much greater impact than previously recognised supply chain attacks. The vulnerability in SolarWinds' Orion product, which was initially introduced by the actor, has not only been exploited at various US government agencies. Several cybersecurity and tech companies with global customers, such as FireEye, Mimecast and Microsoft, have also reported being compromised via the vulnerable version of Orion. Had the compromised version not been discovered, the actor could have affected many more organisations globally.

Supply chain attack on Codecov development environment

Codecov, based in San Francisco, reported in a statement that one or more hackers began tampering with software used in the tech industry on 31 January to test code for errors and vulnerabilities. The attacker(s) managed to gain access to Codecov's development environment and succeeded in hiding malware in a company script. In this way, the attacker(s) were able to steal passwords, tokens and keys from customers. Codecov warned that the attacker(s) could potentially export information stored on customers' CI environments^{VII}. The hack was discovered on 1 April 2021 when a customer noticed something was wrong with the script. Codecov states on its website that it has 29,000 customers, including Procter & Gamble Co, web hosting company GoDaddy Inc, The Washington Post and Australian software company Atlassian Corporation PLC. How many companies actually fell victim to the Codecov hack is not known. Security experts involved in the case stated that the scale of the attack and the skills required are similar to the SolarWinds attack (see the Review). Other companies could potentially be compromised via Codecov customers. The attackers apparently went to extra lengths to gain access to other software developers and technical services companies through Codecov.

Violation of certain global ICT supply chains can have an impact on national security by, for example, causing critical processes to become unavailable or to malfunction for longer or shorter periods of time. In such a scenario, organisations can no longer perform critical tasks such as distributing energy, carrying out financial transactions or providing education (or their performance may be more limited). Sensitive or vulnerable personal, economic or political information could become accessible to malicious parties. This could harm the Dutch economy or put the Netherlands at a disadvantage in international negotiations. Besides this direct impact, violations of cyberspace also have a wider impact. For example, a great deal of capacity and money must be devoted to investigating misuse and remedying it. In some cases, an entire infrastructure of organisations must be rebuilt. In the meantime, the extent to which actors are still present within the infrastructure of organisations and whether misuse is still possible is unknown. This may mean that analogue processes, which are often lacking or which may result in higher costs, must be used again. Violation can also affect the trust of members of the public and organisations in digital processes and possibly hinder further digitisation.

Boosting resilience against violation of ICT supply chains is limited in practice. Digital processes are intertwined with and make use of various complex chains. There is a lot of 'low-hanging fruit' for attackers that organisations are not always aware of until things go wrong. If there is any risk assessment of third parties, it does not guarantee that they will not be misused indirectly. Moreover, nobody bears full responsibility for the security of the entire chain and the chain is not transparent. Within this framework, cybersecurity expert Bruce Schneier said: 'We can't trust anyone, yet we have no choice but to trust everyone'.

 [Back to Table of Contents](#)

VI Although this campaign is referred to in the media as the 'SolarWinds campaign', this is not an accurate description because almost a third of the organisations affected by the actor had no direct connection with SolarWinds. See <https://www.securityweek.com/cisa-says-many-victims-solarwinds-hackers-had-no-direct-link-solarwinds>.

VII CI is short for continuous integration. 'Continuous Integration is a software development process where developers integrate the new code they've written more frequently throughout the development cycle [...] Continuous Integration helps streamline the build process, resulting in higher-quality software and more predictable delivery schedules.' <https://www.ibm.com/cloud/learn/continuous-integration>.

.....
*Influencing, interference, espionage and
information confrontation widely used*



6 Geopolitics influences threats and interests

Domestic relations and relations between states determine the interests that states promote and the objectives that they pursue. This creates a geopolitical force field that is in motion and also makes itself felt in cyberspace. State actors use their instruments to promote their interests there as well. And sometimes that promotion of interests poses a threat to the national security interests of others, as evidenced by the Threat Assessment for State Actors from the AIVD, MIVD and NCTV.

The threat is evolving

The threat posed by state actors is nothing new; it has been developing for some time. Sometimes it becomes more vague, sometimes more manifest. This is not only due to geopolitical shifts, such as the emergence of new powers that question the post-war international order or the renewed assertiveness of established powers. The tools also change. This makes the threat emanating from state actors towards Dutch society diverse and complex. The increased digitisation and technological possibilities increase the risks involved.

Different states engage in a wide range of activities in pursuit of their interests. They can use all means available to them within their government's remit to do so. Their activities may affect our national security. The threat comes both from state actors with a different strategic agenda and from state actors with a different political system to the Netherlands. The threat can manifest itself directly or through proxies; this term refers to third parties used by state actors. In recent years, concrete manifestations of threats have been observed from various states. Influencing and interference activities, espionage and information confrontation are common practices. In information confrontation, the information domain, including media, social media and platforms, is seen as a battle arena and information is used as a weapon to inflict harm. State actors also use economic instruments to achieve geopolitical goals. Even activities that few state actors engage in, such as preparations for and actual sabotage, can have potentially serious consequences for national security.

Motives of state actors vary

The motives of state actors for deploying resources in or against other states vary. To a large extent, it is a matter of promoting domestic political and security interests. Think of combating dissidents living abroad. An important driving force here is the desire to preserve the status quo in the country of origin: including the existing state structure, role and position of the head of state and role and position of the nationals (both at home and abroad). Although activities related to this are not directly directed against the Netherlands or our allies, they can certainly harm our interests.

Other motives are often financial and economic. Here, too, the preservation of the status quo in the country of origin plays a major role. The diaspora (people living outside the country of origin) is a source of income, making investments (such as the purchase of real estate) and providing financial support to family members left behind. Notable examples are those states for which engaging in illegal digital activities has become a revenue model. For example, North Korea derives a significant proportion of its state revenue from illegal digital activities such as ransomware attacks against international companies and cyber theft. Economic espionage also plays a large part, with which state actors aim to improve their own competitive position, for example, or to acquire high-quality knowledge and technology without having to incur the costs of research and development themselves. Illustrative of this is Chinese economic espionage, which primarily focuses on technology theft and insider information on proposed investments.

In the third group of motives, foreign relations play a more emphatic role. This involves, for example, strengthening the strategic-military position in relation to other states. For example, Iran, Syria, North Korea and Pakistan are looking to the Netherlands and other Western countries for the knowledge and goods they need to develop their programmes for weapons of mass destruction and delivery systems. Other motives include: obtaining political information about government positions and decision-making processes of other states; or influencing political-administrative processes in other states. These motives may lead to the development of all kinds of activities that harm Dutch interests, such as espionage, but also covert political influence, influencing and intimidating the diaspora, sabotage and misuse of the Dutch ICT infrastructure. Previous CSANs have already warned of increasing activities aimed at facilitating the sabotage of critical infrastructures in Europe (in the future). Suppliers of critical processes have also been successfully attacked in recent years. By implicitly or explicitly threatening disruption or sabotage, actors can exert economic, political, diplomatic or military influence on the target. The threat of possible disruption and sabotage is therefore a means of influencing decision-making processes.

Cyberspace offers a wealth of options

Cyberspace is particularly suitable for promoting the interests behind these diverse motives. Firstly, because with increased digitisation and the Internet of Things, almost every target is digitally accessible and access to targets is also relatively easy and low-threshold. In addition, attribution to a state actor is difficult, so there is a low risk of incurring damage when using digital resources. Moreover, it is significantly cheaper and less risky than using other means, as it is not particularly time- and labour-intensive, and tools and methods can be reused. Finally, digital operations are more flexibly scalable than physical operations and the return from them has grown significantly. Thus, the cost-benefit analysis is favourable.

Virtually any country with basic capabilities and the intention of digital penetration will be able to do this successfully at various organisations in the Netherlands. This says something about resilience, which still falls short in various organisations (see also the Core CSAN). Studies reveal that states such as China, Russia and Iran have offensive cyber programmes targeting the Netherlands. This shows both the capacity and intention to penetrate Dutch organisations. In fact, the cyber capabilities, knowledge and expertise of China and Russia are so extensive that there is a good chance they will succeed in penetrating anywhere digitally. In open sources, cybersecurity companies report an increase in offensive cyber activities by states not previously known for their cyber capabilities, such as India, Vietnam, Kazakhstan, Lebanon, Morocco, Ethiopia and Sudan. These states partly develop these capabilities themselves or outsource cyber operations to third parties. For example, the emergence of new cyber actors goes hand in hand with the rise of 'hackers for hire', advanced hacker groups that hire out their (often espionage) services to governments or wealthy clients. The activities of new cyber actors and hacker-for-hire groups can also affect Dutch interests. For example, in a conflict situation, a country or actor group can suddenly, or also, start focusing on the Netherlands.

An important question here is to what extent this 'democratisation' of cyber capabilities also affects the geopolitical intentions of state actors. The fact that states initially did not have capabilities in cyberspace but now do, may lead them to behave differently. After all, it offers them opportunities they did not have before, such as monitoring dissidents living abroad or cyber attacks on other states with which they are in conflict. It is conceivable that the growing range of instruments available will also lead to a reconsideration of one's own geopolitical power.

Means and targets

State actors have a wide range of means at their disposal to achieve their objectives, with each actor having its own specific goal and modus operandi. Some of them are not necessarily illegal or even undesirable. And not all state actors have the same capabilities.

Means used by state actors: seven categories ^{VIII}

1. Influencing and interference (including disinformation). This includes hacking and leaking; covertly influencing individuals, democratic processes, political decision-making; using coercion (such as threats, blackmail, extortion or physical violence) against individuals; influencing and censoring scientific research.
2. Espionage, both cyber and physical, including economic espionage.
3. (Cyber) preparatory acts for and actual disruption and sabotage.
4. Military activities, such as intimidation and show of force through arms races, large-scale exercises, military interventions in third countries, deployment of unrecognisable troops.
5. The use of economic instruments, such as takeovers and investments, but also the exploitation of strategic dependencies as a means of exerting economic pressure.
6. Diplomatic and international-political activities, for example, the use of obstructive power in international forums to block unwelcome decisions.
7. Legal activities and/or lawfare, in which (inter)national law and legal systems are used to gain the greatest possible personal advantage, even if this is very much against the spirit of the law.

The first three categories lend themselves perfectly to the use of digital resources. Influencing and interference largely take place in the information domain, which is digitalised in the form of, for example, online platforms and social media. This facilitates the use of means of influence such as the creation and/or dissemination of disinformation, media campaigns, the dissemination of information to cause damage or harm people, or hack and leak actions. That the use of digital resources for espionage and (preparations for) sabotage is perfectly suitable and attractive no longer needs to be demonstrated. In its 2020 Annual Report, the AIVD concluded that espionage is a threat to Dutch economic security.

A state actor can use its resources against a wide range of possible targets: from local associations to international security organisations and from a single individual to entire communities.


^{VIII} The order in this box does not imply any ranking of the different means.

^{IX} A more detailed description of targets and how they are affected can be found in the Threat Assessment for State Actors published by the AIVD, MIVD and NCTV in February 2021. The order in this box does not imply any ranking of the different targets.

Targets of state actors: fifteen categories ^{IX}

1. Diaspora, i.e. population groups that originate from another country and are still seen and treated as subjects by the country of origin.
2. Faith communities.
3. Groups and/or individuals susceptible to polarising messages, such as groups with strong anti-sentiment (e.g. against the Dutch government).
4. Targets of opportunity: people who consciously or unconsciously allow themselves to be used.
5. High potentials: people with the potential to reach knowledge or influential positions.
6. Institutions and officials of our democratic constitutional state, at national and local level.
7. Democratic processes, such as elections and referendums.
8. Advisory bodies, which have a role in political decision-making through research and advice.
9. Educational institutions.
10. Research community, knowledge institutions and think tanks.
11. Civil society, ranging from media to sports associations.
12. International organisations based in the Netherlands.
13. The private sector (and top sectors).
14. Critical national infrastructure (plus suppliers).
15. International frameworks that are crucial for the Netherlands, such as the EU, NATO and the UN.

A prominent target type is the critical national infrastructure, which includes critical processes, services, suppliers and central government.^X What is striking is that digital sabotage (including preparatory acts) is mainly used against this type of target. It is important to note that, as yet, no manifestations of this have been seen in the Netherlands, but they have been seen in other Western and even European countries. In particular, there is a growing interest in exploiting vulnerable links in supply chains. Extensive digitisation and the limited existence of fall-back options increase vulnerability.

 [Back to Table of Contents](#)

^X The definition of critical national infrastructure is under development. The description of this target type used here is based on the definition used at the end of 2019 and included in the Threat Assessment for State Actors from the AIVD, MIVD and NCTV. The critical national infrastructure target type has been supplemented with suppliers, because for some years now it has been observed (in the CSAN among others) that suppliers are used as stepping stones to targets within the critical national infrastructure. There is a growing interest in exploiting vulnerable links in supply chains.

.....
*The boardroom bears responsibility
for adequately handling digital risks*



7 Risk management instrumental in boosting resilience

Previous CSANs have mentioned inadequate resilience a lot. Resilience should be seen as the ability to reduce relevant cyber risks to an acceptable level. Looking at the incidents that have affected the Netherlands, resilience continues to lag behind the growing interests and shifting threat this year too. Experts also point to major differences in resilience between and within sectors and chains. Organisations that seem to be in a better position have, in addition to taking basic measures, also focused on a risk-based way of working. They can offer insights into making the Netherlands more resilient in general. This shows that, in addition to basic measures, attention to risks is essential. There are a number of widely applicable basic principles that can also be applied by smaller organisations. It is ultimately up to public administrators and leaders of organisations, whether in the private sector, central government or politics, to manage risks.

Risks require constant attention

Both the interests of organisations and those of attackers are subject to change. This means a clear picture of the shifting threat landscape and constant attention to risks is essential. After all, resilience is the ability to reduce relevant cyber risks to an acceptable level. A broad view of risks is important to be able to say that organisations, chains and states have a sufficient level of resilience. This broad view can be achieved through risk management.

A baseline is not enough

Given the increasing complexity and digitisation of processes, the intertwining of organisations and sectors, as well as a growing threat, implementing basic measures is important, but not sufficient. Basic measures, including those mentioned in the NCSC's publication *Guide to Cybersecurity Measures (Handreiking Cybersecuritymaatregelen)*, ensure a minimum level of cybersecurity

(or security hygiene). In addition, better tools are needed to anticipate sophisticated attackers and more complex problems. Organisations and sectors that appear to be more resilient than their counterparts not only invest in basic measures, they also take a critical look at the greatest risks. Security specialists, supervisors and legislators therefore emphasise the importance of risk management as the instrument for actually increasing resilience in practice. Unfortunately, many organisations still see risk management as a lengthy and costly process, rather than something to be tackled periodically.

It is more than just risk analysis

In recent years, awareness of risk management standards seems to have increased. The translation of these general frameworks into sector-specific implementations has also been further developed. This is not just about identifying relevant risks. In fact, risk analysis is part of risk management in general, where both prevention of problems and resolution play a role. Some of the key activities for

managing risks are: identification of relevant risks, prevention by implementing measures, detection of repulsed and successful attacks, mitigation of the impact of a successful attack, and repair to restore full operation of a process. Communication with stakeholders, including feedback to management, plays an important role in evaluating the effectiveness of the process. In addition to the aforementioned activities, overarching aspects are increasingly evident in a broader view of risk management. Regulation from the market and government - such as insurance, certification and liability - plays an increasingly important role. This also applies to governance, realistic testing, situational awareness and learning from mistakes. These different facets of risk management should reinforce each other: risk management is a continuous process with the aim of ensuring that risks are clearly and unambiguously identified and actually reduced.

'Prevention and cure' as an adage

A balanced approach to cyber risks is not just about reacting to incidents or rolling out measures to stop attacks. Instead, a nuanced view of the problem is needed. It must be accepted that there is no such thing as airtight security and that there will always be successful attacks. This does not mean that digital dyke reinforcement is of no use. Such activities can indeed help to parry attacks and reduce the impact of successful attacks. Detecting attackers at an early stage and responding quickly, can limit the damage. At the other end of the spectrum, the 'security by design' and 'privacy by design' mentality can also be used. The earlier security issues are included in the development process of a process, system or service, the cheaper and/or the more impactful the measures taken will normally be. The challenge is to find the right balance in this playing field so that risks can be addressed at an acceptable cost, both in terms of money and in terms of balancing other interests such as freedom, accessibility and progress. The 'usable security' field shows that interests do not have to be mutually exclusive. If problems are identified in good time in consultation with end users, there is a good chance that an appropriate trade-off can be made.

Basic principles can be applied widely

Although the establishment of a comprehensive risk management system in a large organisation may take several years, the underlying principles are also relevant for smaller organisations. After all, risk management can be implemented in many different ways. It is mainly a question of seeing what works in the given context. Therefore, each organisation is free to design its own approach to risk management in line with existing obligations. The following fundamental principles may be helpful in this regard.

Resilience is a team effort

Traditionally, the management of technology-related risks has been entrusted to the ICT department. This widens the gap between technical experts and the business. Instead, risk management can be seen as a team affair. Management of cyber risks should be done in consultation with the business, involving parties such as business continuity managers, risk managers, process owners and domain experts. Examples of where this has not happened show that basic problems can otherwise fall between two stools. Furthermore, in addition to the importance of good cooperation between disciplines, cooperation between the different layers of an organisation is essential. The exploration and management of strategic, tactical and operational risks should be well coordinated.

Scenarios provoke thought

Risks often remain abstract. For this reason, it may be useful to translate them into scenarios. Examples of such scenarios are included in Chapter 8, Threat Scenarios. This kind of scenario-driven way of working makes things tangible, and it makes it easier to build bridges between different disciplines. A workshop to introduce people to scenarios could start with everyday examples, such as ways of breaking into a house. Based on these relatively simple scenarios, more complex examples can be given, such as scenarios involving cybercrime. In a next step, even the perspectives of different disciplines could be added. Apart from being used for risk identification, these scenarios can also be used during the other stages of the risk management cycle. They can be used, for example, in process audits, system testing and incident response exercises.

Money and uptime are universal benchmarks

In order to be able to compare different scenarios, it is important to agree on a common interpretation of the concept of risk and to use the same indicators for multiple risk analyses. This allows risks to be compared in an informed way. An example of a set of indicators that is fairly universal is money (or financial impact) and continuity (or availability). By also using these indicators for other types of risks, cyber risks can be put on the same footing as, for example, operational risks. In this way, the crown jewels of an organisation can be identified by looking at what has the most impact on revenue and business continuity. These crown jewels can then be given extra attention, and the security budget can be used intelligently. In this way, the parts of an organisation that actually need it are made more resilient. Unfortunately, however, there are also organisations that carry out risk analyses that leave something to be desired: risks are often vaguely and sweepingly described, so that they cannot be adequately explained. This makes it more difficult to weigh up the effectiveness of measures to protect the performance of a country or organisation's core tasks. Security is then quickly seen as a cost item instead of an integral part of business operations.

Testing exposes problems

A pitfall with regard to risk management and cybersecurity is to have everything perfectly in place on paper but dropping the ball in practice. It is therefore important to actually test processes and systems as they run on the shop floor and in the field. These tests can be based on the scenarios identified earlier. Interim shifts in the threat assessment and the interests to be protected should not be forgotten. Testing can be done in many different ways, from a simple tabletop exercise to an extensive threat-based red teaming exercise. When choosing the scope and the type of test, it is important to also adopt a risk-based approach. In a more general sense, the test plan should be linked to the broader risk management cycle. The effectiveness of measures needs special attention. Monitoring whether measures have the intended effect can reveal whether the costs outweigh the benefits. In addition to the experiences of experts, insights from (academic) research can also be taken into account.

Learning from and with each other

Risks manifest themselves differently in different organisations. This is partly due to differences in resilience, but it is also largely a characteristic of the risks themselves. A risk will not normally materialise in all cases. This can make it difficult to see relevant risks and the effectiveness of measures. To deal with this, it is wise to talk to other organisations. Knowledge and experience can be exchanged within the framework of ISACs (Information Sharing and Analysis Centres), with the chain partners of a critical process, and in other partnerships. For example, within a private consultation, organisations can share stories about incidents that have happened to them. The exchange and even the setting of standards are also possible. In addition to exchanging knowledge, cooperation can also include joint exercises to test and improve response capacity. This helps to find each other quickly and anticipate each other's needs when the need is great and there is no time for extensive consultation. The underlying idea in all of this is not to compete in the area of security, but rather to cooperate.

The ball is in the directors' court

Risk management without buy-in from the directors will most likely fail: CISOs who try to manage security on their own sooner or later discover that the organisation does not feel ownership of the problem. It is essential that directors are closely involved in risk management. They are responsible for identifying the strategic interests within an organisation and for (mandating) the acceptance of residual risks. The right bodies must be in place and appropriate responsibilities must be assigned for this. Line managers, or the owners of digital processes, can take daily responsibility for the tactical and operational risks. In addition, directors themselves need to keep abreast of the most significant risks. This also applies to political leaders, who need to keep an eye on cyber risks to national security, in order to be able to make informed decisions between various and divergent interests.

Risk visibility and control is necessary

Public administrators and leaders of organisations are ultimately responsible for dealing adequately with cyber risks. Strategic as well as tactical and operational risks can be secured by means of targeted control and progress monitoring. Clear reporting lines should be set up for this purpose. CISOs should report directly to the board and independent internal and external audits are also important. Of course, the supervisory board and the regulators play an important role in this. They have the responsibility to check whether directors and line managers have an adequate view of relevant risks and whether they act appropriately on them. This requires monitoring bodies having a keen eye for pertinent interests, threats and measures. Insight into the information that is processed within digital processes is a crucial factor. Organisations themselves do not always have a view of their own resilience, and the absence of an organisational structure that maintains a grip on information also plays a role. The tactical layer can, in addition to the daily responsibility for money and personnel, also be responsible for the information that belongs within its own department (and the risks associated with it). Within the tactical layer, information owners can be appointed who bear responsibility, are given the means to do so, and are held accountable by directors for fulfilling this responsibility.

Investing in people is the foundation

Risk management is a specialism. This is why public administrators and leaders of organisations - and people who have the day-to-day responsibility for digital processes and the associated risks - cannot be expected to be experts in this field. Instead, they should ensure that they have put the right people in the right place by investing in new recruits and in training current staff. This requires a structured personnel policy, as well as a training programme anchored in the organisation. In addition to the experts in the field of cybersecurity risk management, the rest of the organisation must also have a minimum knowledge base to be able to properly discuss important risks to the organisation and how to deal with them. This is mainly about the how and why of the principles behind risk management

(e.g. through a workshop built around organisation-specific scenarios). When appointing and training people, a balance must be found between the various facets of risk management (see the section 'It's more than just risk analysis').

The Government also has a role

What is true for the leaders of organisations is also true for the public administrators of countries. To cope with digital risks, it is important to identify and address them in a systematic way. At the national level, these include structural problems such as growing dependence on foreign software and hardware manufacturers and service providers. Problems such as the diminishing diversity of technological solutions and suppliers may also pose a systemic risk. Furthermore, the Government has a role in addressing market failures and other collective action problems, including the issue of risk management in chains of parties that do not share the same interests and where transparency is lacking. For example, the security of many Internet-of-Things devices has left much to be desired for some time. The need for regulation is therefore gaining wider recognition, but a dynamic and complex environment makes it difficult to measure national resilience and predict the effectiveness of measures.



.....
*Large-scale increase in use of
cloud services comes with risks*



8 Threat scenarios

The previous chapters address digital threats, resilience and interests that can be in jeopardy when cyber incidents occur. But what does that mean for you or your organisation? To help answer that question, this chapter describes three related scenario sections on cloud system failure and misuse. This particular theme was chosen because of the importance of the cloud within cyberspace. There has been a large-scale increase in the use of cloud services, which comes with risks. You can use these scenarios to assess within your organisation whether events such as those described in the scenario could happen to you, what preparations you have made and how you can improve your cloud strategy. The scenario was prepared by TNO on behalf of the NCTV.

Cloudburst scenario

This scenario has three scenario parts that follow each other but can also be read separately.

Scenario part a: the Cloud comes back online quickly

Description of events

Extreme weather causes major problems in the Netherlands. Heavy flooding occurs at several locations and is accompanied by power outages. As a result, Nubes Link-Exchange (NLeX)^{XI}, a major cloud exchange provider, is experiencing significant disruption to its connection to one of the Dutch data centres of CirroCumulus Networks^{XII}, a major cloud service provider (CSP). NLeX provides direct, private connections between customers (governments and businesses) and the CirroCumulus Networks cloud network, without the intervention of an Internet Service Provider (ISP). Due to the malfunction at NLeX, none of the customers in the affected region will be able to connect directly to their CirroCumulus Networks cloud environment.

Some of the affected organisations are prepared for such a temporary unavailability and have taken extra (fallback) connectivity services as laid down in their contract with NLeX and CirroCumulus Networks. This part of the affected organisations will be switched via NLeX from the direct connection to CirroCumulus Networks to a connection via the (public) Internet, provided by an Internet Service Provider (ISP). There is hardly any disruption for these organisations. The other part of the affected organisations

have not purchased any additional (fallback) services and temporarily lose the connection to their cloud environment as provided by CirroCumulus Networks. After appropriate action by NLeX, their services can be resumed after about two hours.

The impact of the temporary system failure varies per affected organisation, as it depends on the set-up of their infrastructure (variations in the use of public, (virtual) private, hybrid cloud and on-premises solutions). Organisations with a lot of on-premises infrastructure are less affected by the system failure than those whose services are housed in the cloud environment.

Interpretation

In recent years, more and more parties have opted for a direct connection to the cloud environment that does not go through the public Internet but connects them to the Cloud as directly as possible (with as few parties as possible in between). Reasons for choosing this are speed (less delay), confidentiality and reliability (fewer links). Practical examples include cloud connectivity services Direct Connect (AWS) and Express Route (Microsoft). In all cases, it is important to consider how dependent an organisation wants to be on a cloud service provider and what the risks and benefits are for your organisational processes. These are important considerations when deciding on your own cloud strategy. Organisations that work a lot with sensitive information often

XI Any resemblance to an existing company is purely coincidental and not intended.

XII Any resemblance to an existing company is purely coincidental and not intended.

choose to process this data only in a protected (private) environment. This can be a private cloud environment at a CSP or their own in-house on-premises infrastructure. Some organisations choose to make partial use of a public cloud service and partial use of a private solution (cloud or on-premises). With such hybrid cloud solutions, sensitive information can be properly protected, but for less sensitive processes, the economies of scale of a public cloud infrastructure can be utilised. In practice, many combinations and configurations are used. Additional measures increase security or availability but come at a price and require specific expertise. It is important for an organisation to make an informed decision about this. For the safe purchase of cloud services, the NCSC published Fact Sheet 5 - Recommendations for Securely Purchasing Cloud Services in 2020.

Key terms

Cloud exchange provider: provides on-demand (direct) connections to cloud service providers, where digital traffic is not necessarily routed via the Internet. They are therefore an intermediary that connects many customers directly to cloud service providers without the intervention of an ISP.

Cloud service, also called cloud computing service: digital service that allows access to a scalable and elastic pool of shareable computing capacity.

Cloud service provider (CSP): provides on-demand services to customers in the form of a platform, infrastructure, computing capacity, storage or a specific service, without direct active management by a customer or user.

Internet Service Provider: provides facilities to organisations to connect to the Internet, whether or not in combination with Internet services. Internet connections are typically not made on-demand and are installed for long-term use.

Public cloud: here, customers share the infrastructure available for rental with other customers. A CSP manages this infrastructure and can provide customers with the necessary resources against payment.

Private cloud: here the infrastructure is exclusive to a single customer, where the physical location of the resources is either on the customer's premises (on-premises) or on the premises of a CSP but separate from other customers. An organisation can set up its own private cloud environment, or contract a CSP to do it for them.

Hybrid cloud environment: this combines a public cloud service provided by a CSP with either a private cloud environment or private (owned or leased) capacity in a data centre, where the two environments are separate but can communicate with each other and share data and applications. This is sometimes chosen because organisations want to have access to sensitive data, which they consider too risky to store in a public cloud environment. At the same time, they want to use the computing power of the public cloud to run applications.

Key questions for the reader

1. Are you familiar with your organisation's cloud strategy and the considerations made for this?
2. Has there been an informed decision about which cloud service to use to support which organisational processes?
3. Are you aware of how the connectivity to the cloud service has been realised and has an informed choice been made from the possible cloud connectivity options?
4. Do you have a clear picture of the impact on your organisational processes if the cloud service or the connectivity to it fails?
5. What alternatives or mitigating measures do you have in place if the cloud service is temporarily unavailable?

Scenario part b: there is no sky without clouds

Description of events

A few weeks after extreme weather caused a temporary disruption of cloud exchange provider NLeX, the CSP Cirrocloud Networks identifies a suspicious peering connection at one of its customers. The discovery is made based on the Monitoring & Detection (M&D) service that this customer has also purchased from the CSP (which is adept at anomaly detection). It seems that data from the customer's cloud environment is being siphoned off to an unknown location outside the customer's (virtual) network. Further investigation reveals that there is indeed an illicit connection. As such a peering connection can only be established with the correct credentials, further investigation is underway. An actor has apparently gained access to the customer's cloud environment and has been able to generate false credentials and establish a connection with them. This is initially handled as an incident targeting this customer. Because there is a suspicion that the customer's stolen data also contain personally sensitive data, this is reported to the Dutch Data Protection Authority.

One week later, a similar case comes to light through the same M&D service for another client from the same Dutch region. Cirrocloud Networks starts investigating the matter further and is also starts monitoring the connections of their other customers in this region as a precaution. This reveals that the problem affects a number of customers. However, it is clear that the problems are limited to customers in this region. After a few days, the media reports on this, with various speculation about the motive of the malicious actor and the damage caused. The media reports name some of the companies that have been affected and have already been notified by Cirrocloud Networks. The cloud service provider has shared technical threat information (IoCs) with their customers, the CSIRT-DSP and the Telecom Agency. The CSIRT-DSP, together with the NCSC has further shared the threat information with trusted intermediary organisations Objectively Known To Task (OKTTs) and offers an action framework for the detection of possible anomalies in their network environment.

Further (forensic) investigation is being conducted by CirroCumulus Networks and a forensic investigation company hired by an affected customer. This reveals that the intrusion can be traced back to the temporary re-routing of the direct connection by NLeX a few weeks earlier when a storm caused a system failure that made NLeX's service temporarily unavailable. When NLeX temporarily switched the direct peering connection of a number of CirroCumulus Networks customers to an internet connection, a (human) error was made in the confusing, time-sensitive situation, which led to a vulnerability. A malicious actor had surreptitiously exploited this vulnerability, as the malware found in a customer environment appears to have been installed since the time of the extreme weather situation. As more customers may have been affected, CirroCumulus Networks is notifying all its customers in the affected region as a precaution.

It appears that several, but not all, CirroCumulus Networks customers who were temporarily switched from a direct connection to an internet connection by NLeX during the storm have indeed experienced suspicious activity. There is still much uncertainty about the exact scope of the data that has been stolen, but it is clear that in addition to personal (customer) information, the data of some customers also includes business-sensitive information and sensitive information from some government departments. This information is additional fuel on the fire in the (social) media. Varying speculation from cybersecurity experts make it unclear which organisations have been affected, which have not, and what the consequences of the succession of incidents are. Questions are also asked in Parliament, such as whether the Netherlands has become too dependent on cloud services and whether customers using the services of the CSP, the cloud exchange or the CSP itself are responsible for the damage suffered.

Interpretation

Many organisations see moving operations to a public or hybrid cloud environment as a way to increase protection against cyber attacks. For cloud service providers, it is extremely important to ensure the security of their services, and they therefore have a lot of expertise and capacity in the field of cybersecurity. However, this does not mean that cloud environments are infallible. Mistakes can be made and malicious actors are lurking everywhere to exploit vulnerabilities.

Incidents such as Solarwinds have shown that organisations can be vulnerable if they depend on an increasingly complex network of software product suppliers or outsourced ICT services.

Organisations do not always have a good overview of all the parties that are part of this network, which makes control difficult. An attack on a component in the chain of ICT services can therefore indirectly impact an organisation (supply chain attack, see also the threat scenario of CSAN 2020).

Key term

(Private) peering connection: a method of routing traffic between devices in two different networks without having to use a third party (ISP) to route the traffic. For example, large organisations use private peering connections to exchange data between different locations in their organisation. For communication with other organisations, organisations use a public peering connection, usually through an ISP that in turn has peering connections with other ISPs. Peering connections between ISPs are often realised in an Internet Exchange. The interconnection of all peering connections forms the Internet.

Key questions for the reader

1. Do you have monitoring and detection capacity available or purchased as a service? Are you aware of what exactly is being monitored and what types of threats are and are not being detected?
2. How are the responsibilities allocated between you as the customer and the cloud service provider in the event of an incident? What are the individual and collective responsibilities in this regard? And are they sufficiently coordinated with each other?
3. Are you familiar with or do you use an assume breach strategy? In other words: if it is assumed that your organisation will one day be confronted with a cybersecurity incident, what is your action framework?

Scenario part c: operation dust cloud leads to scorched earth

Description of events

A large group of Dutch customers of CSP CirroCumulus Networks suddenly have no access to their cloud environment. Media reports immediately point to a major infrastructure failure at CirroCumulus Networks and do not exclude the possibility of an attack. It is of note that this occurs at a time when reports of suspicious activity in the cloud environment of several CirroCumulus Networks customers have already come to light. A spokesperson for CirroCumulus Networks indicates that service was indeed disrupted by problems in one of its data centres and that they are working to find the cause and solution. Meanwhile, unrest among CirroCumulus Networks customers is growing, fuelled by media reports. Are their systems and data still reliable and secure? What's going on?

A few hours later, CirroCumulus announces that there is an advanced attack against one of the company's data centres in the Netherlands, which has affected some of the Dutch customers. The situation is now under control and CirroCumulus Networks is doing everything possible to restore service as soon as possible. This can take from a few hours to a few weeks, depending on the specific situation of the affected users.

In the days that follow, more information about the incident slowly comes to light. It seems that attackers were able to generate a huge amount of traffic from the inside, via a botnet of virtual machines. This internal DDoS attack overwhelmed the virtual machine manager (VMM) and caused it to fail. The VMM is software that controls the virtualisation of the hardware (servers in a data centre) and distributes the available resources such as memory and CPU among the connected users (customers' virtual machines). Because the VMM crashed, all virtual machines connected to the VMM and in use at the time have been lost.

The VMM has been reset to restore service. CirroCumulus Networks will discuss with all affected customers whether their virtual machines can also be reset or whether further analysis is required to determine whether data that was being processed at the time of the crash should and can be restored. This depends on the configuration of a user's cloud environment and the type of work the customer performs on the affected virtual machines. For customers for whom (part of) the virtual machines are reset, the availability of their cloud environment is restored a few minutes or at most a few hours after the VMM is reset. For users where further investigation is required, this may take days or even several weeks.

In reporting on the incident, much attention is also paid to how this attack could have taken place. To make the virtual machines function as a botnet, the attackers placed malware on the virtual machines. This means that they must have had access to these virtual machines. This leads to speculation about a connection with a recent CirroCumulus Networks user incident, where attackers were able to exploit a vulnerability during a recovery operation after an extreme-weather system failure. These attackers then gained access to the cloud environment of several users, presumably to exfiltrate data. It now seems that the same perpetrators started preparing this internal DDoS attack at the same time. According to experts, now that their activities have been discovered, the attackers may well have launched this DDoS attack to hamper the investigation and cause as much damage and disruption as possible.

Interpretation

For cloud services, DDoS attacks are seen as a concrete risk. One example is an attack on Amazon's cloud services in 2019. Since then, much attention has also been devoted to measures to counteract DDoS attacks, aimed at identifying and repelling improper traffic. However, when the attack is carried out with legitimate traffic (e.g. from the service's customers), identifying and stopping the flow of traffic is much more difficult. DDoS attacks on cloud environments can either come from outside (for example, an external botnet attacking a set of virtual machines in a cloud environment) or from within (an internal botnet of virtual machines attacking a target within the same cloud environment). Internal attacks in particular are seen as a serious risk, as they can disrupt the entire virtual infrastructure.

The consequences of virtual machines going down - due to the VMM crash - are similar to a computer crashing. The data that is currently being processed and has not yet been saved is lost. How much data loss there is depends on the settings of the virtual machine. For complex calculations or data processing that may take hours or days, a crash is much more drastic than losing the last few sentences in a word processing document. The way in which data is stored also influences the impact of such an incident. For example, it is possible to replicate data in different locations. These are matters that are not automatically taken care of by a cloud service provider and that a user should therefore think about when setting up the (cloud) network infrastructure.

Key terms

Virtualisation: one of the core technologies of cloud services. With virtualisation, a virtual (simulated) computer environment is created, whereby one physical computer environment is divided into several virtual computers, also called virtual machines. Cloud Service Providers have physical servers in a data centre and the cloud environment of the customers is built via virtualisation. As a result, these parties do not need to have their own physical server.

Virtual Machine Manager (VMM) or Hypervisor: a software program (comprising several modules) that sits between the CSP's physical server (physical hardware and host operating system) and the customers' virtual machines (guest operating system). It enables virtualisation and regulates performance by distributing memory, CPU and other resources to virtual machines.

Key questions for the reader

1. When designing your cloud environment, did you take the failure of this infrastructure into account (design for failure)?
2. What activities does your organisation perform in the cloud environment and how sensitive are these processes to interruption?
3. How is the data processed in the cloud environment stored? For complex or sensitive data processing, has replication at multiple data centre locations or 'availability zones' been considered? Please note: Replication can ensure that important data is not lost in the event of disruption at one location but remains available at another location.
4. Do you know the basis upon which your organisation chose a public, private or hybrid cloud environment? Does this include the complex data processing and sensitive or unique data that plays a role in your organisational processes?

 [Back to Table of Contents](#)

Appendix: Creating the CSAN

The Cybersecurity Assessment Netherlands was drawn up by the National Coordinator for Counterterrorism and Security (NCTV) and the National Cybersecurity Centre (NCSC). It is defined annually by the NCTV. They are grateful for the information, insights and expertise of government agencies, organisations in critical processes, science and other parties.

There are three phases in the creation of the CSAN: 1) analysis, 2) writing and peer review and 3) validation.

Re 1 Analysis

The NCTV collects and analyses relevant information on incidents, trends and shifts in the triangle of interests, threat and resilience. When doing so, the following questions are answered:

Retrospective: what relevant incidents took place in the Netherlands during the period March 2020 to March 2021? What type of incidents were involved? What caused them and what damage did they cause/impact did they have?

Interests: what interests can be affected when cyber incidents occur? What can the impact be?

Threat: what digital threats could affect national security? From whom or what do these threats emanate? Against which targets are they directed? Which modi operandi are used by actors? What vulnerabilities are exploited by actors? Have any shifts in the threat become apparent?

Resilience: what is the degree of resilience of the Netherlands against these digital threats? What concrete initiatives for boosting resilience are there?

Outlook: what broader developments are expected to affect cybersecurity in the coming years? Which developments can be game changers?

External partners are asked to provide input in the analysis phase. In November 2020, a written expert consultation took place, in

which government agencies, organisations in critical processes, the research community and other parties were asked to answer the following questions:

- What events, incidents or developments in the field of cybersecurity in the past year in relation to the Netherlands are striking in your opinion and why? How does this affect interests, threats and resilience?
- What shifts do you expect in the perception of: a) interests, b) threats and c) resilience in relation to the Netherlands in the coming year and why?

In the period November 2020 to February 2021, a number of parties from the financial sector (including EquensWorldline) and the Justice and Security Inspectorate also provided input for the theme of Resilience. This input has been incorporated into the Risk Management chapter. The analysis questions were answered based on the information collected and the risks to National Security were formulated. The NCTV then formulated a Core CSAN outline. The core contains the most important 'leitmotifs' for the latest Cybersecurity Assessment and identifies the themes that deserve further elaboration, for example because they imply a shift in the existing perspective or have not been addressed previously in the CSAN. The themes were then tested with a number of partners.

Re 2 Writing and peer review

Subsequently, both the Core CSAN and the themes were drafted by authors within the NCTV (Core CSAN, Chapters 1, 3, 5 and 6), the NCSC (Chapter 7), the Police (Chapter 4) and TNO (Chapter 8). Chapter 2 (the Retrospective) was written by NCTV and NCSC. The complete text was peer-reviewed several times within the NCTV and the NCSC. All chapters have been produced under the editorial final responsibility of the NCTV.

Re 3 Validation

The CSAN has an extensive validation process, in which the draft text is submitted to external partners for comments. These are the partners who were also asked to provide input in the analysis phase. After the collected comments have been processed, the final text is prepared and adopted by the NCTV.

After the publication of the CSAN, an extensive internal and external evaluation takes place. The feedback collected is then incorporated into the following year's CSAN process. The evaluation has led to concrete changes in the past, such as the inclusion of a scenario chapter (since 2020) and the refining of the terms used (2021, in cooperation with Prof. Bibi van den Berg and Em. Prof. Jan van den Berg). As a result of the evaluations of previous years, the NCSC has decided to issue the 'Guide to Cybersecurity Measures' in mid-2021.



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](https://twitter.com/nctv_nl)

June 2021