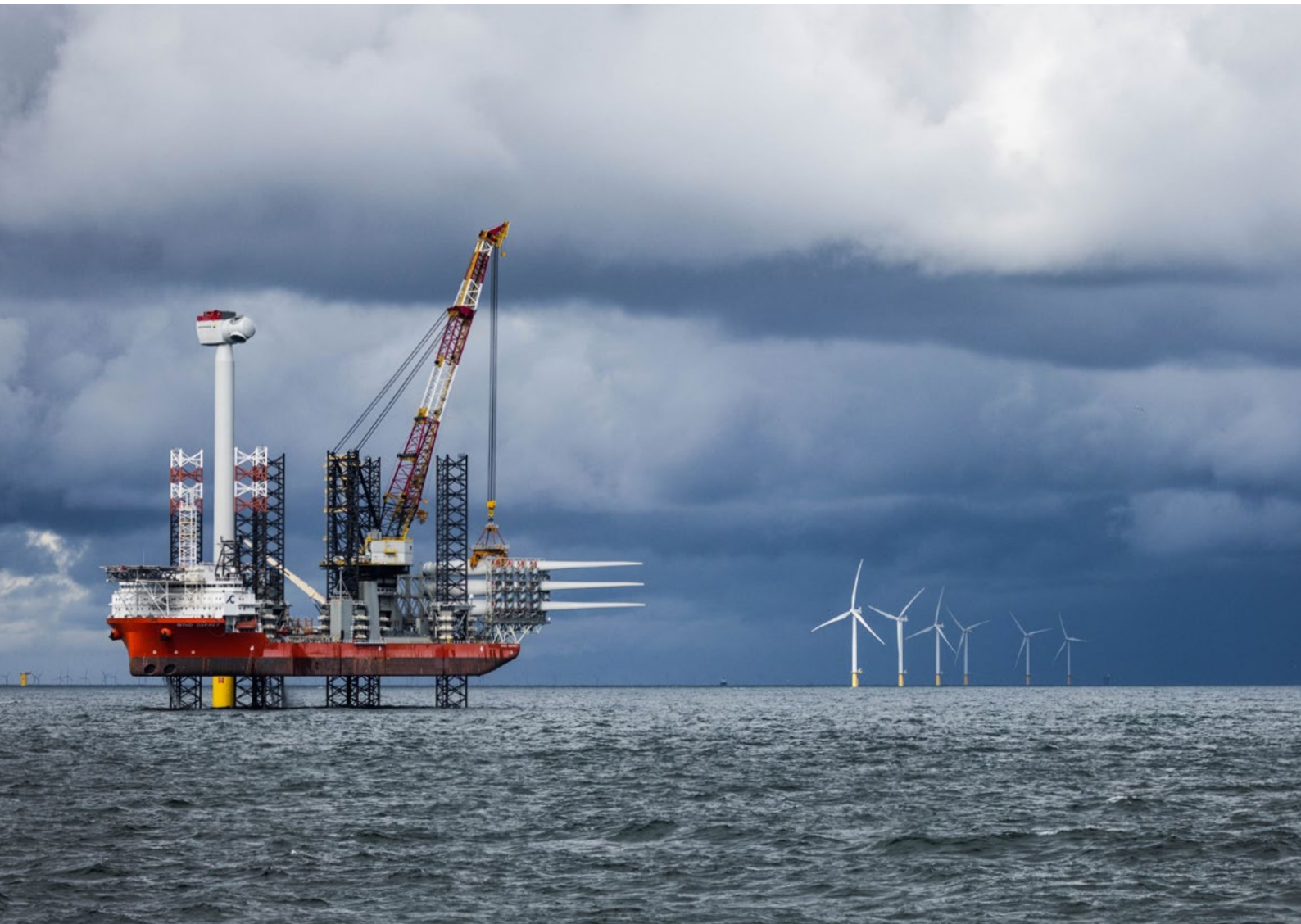
National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

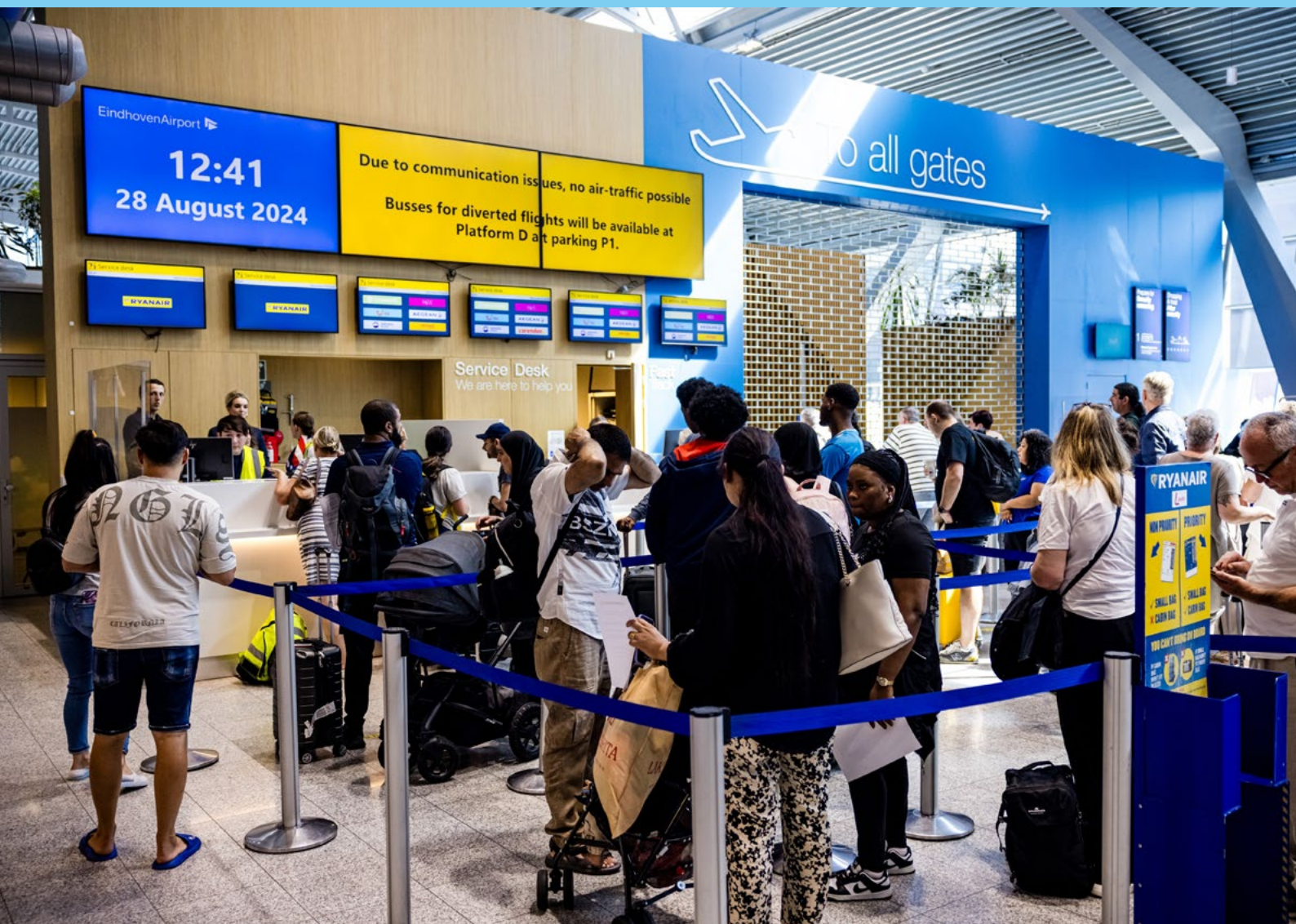
Cybersecurity Assessment Netherlands 2024



Cover image: State actors are intensifying their activities and expanding their capabilities, using various means from a broader toolkit. Vital infrastructure in the Netherlands, such as wind farms, can become the target of digital espionage or sabotage.

Contents

Travelers at Eindhoven Airport are stranded due to a major outage that has completely paralyzed air traffic to and from Eindhoven Airport. It turned out to be a software error on an ICT network of the Ministry of Defence. The outage also affected the communication and alarm system of emergency services, making it more difficult for them to communicate with each other. The outage was not resolved resolved until the end of the day.



Turbulent times, unforeseen effects

Digital risks are dynamic and influenced by many factors, which may not always be digital in nature. Particularly in recent years, turbulent geopolitical times have had a significant impact on the digital threat landscape. The Netherlands has been a target of cyberattacks or experiences the impact of cyberattacks that ripple through the digital ecosystem. Additionally, disruptions can lead to large-scale outages. Digital risks are complex and highly interconnected. All of this can result in unforeseen effects. Consequently, the risk to national security may increase. To address digital risks effectively, it is crucial to adopt a comprehensive approach to risk management.

Main findings of CSAN 2024

1. The digital threat against the Netherlands is significant and diverse, with cyberattacks primarily originating from state and criminal actors. In these turbulent geopolitical times, state actors are intensifying their activities and expanding their capabilities, employing a broader toolkit. Criminal actors carry out large-scale attacks and act opportunistically. Widespread disruption of digital processes also poses a threat.
2. Digital risks require a comprehensive approach to risk management. They are dynamic and influenced by many different factors. The broader digital ecosystem, including monocultures within it, and the high degree of digitalisation cause risks to become interconnected.
3. The security of digital processes is and remains essential in our society and is therefore inextricably linked to national security. The importance of digital security competes with other interests.

The digital threat against the Netherlands is significant and diverse

State and criminal actors pose the greatest threat to the Netherlands when it comes to cyberattacks. New methods of attack include exploiting edge devices, such as VPN servers and routers. Attacks via edge devices are attractive because monitoring and detection are extremely complex.

State actors intensify activities and broaden capabilities

Multiple state actors are intensifying their cyber activities. Russia and China, for instance, are stepping up their efforts. Some other countries are also investing in their cyber programmes, leading to the emergence of new cyber powers. In addition to intensifying cyber activities, several countries are also broadening their capabilities: they are adding new methods to their existing arsenal or using other means, including non-digital. Beyond using other tools from a broader toolkit, the deployment or involvement of non-state actors is part of this expansion. In 2023, for example, 'hacktivist' collectives carried out a larger portion of Russian digital espionage, sabotage and influence activities. Sometimes these were what are known as cover operations, sometimes they were actual hacktivist groups acting in line with the Russian state. The Chinese offensive cyber programme is partly based on cooperation between businesses, universities and Chinese intelligence services. The dividing lines between organisations are unclear: individuals sometimes fulfil both a scientific role and a role in the Chinese security apparatus, while working with Chinese state or other companies.

Cybercriminals remain capable of causing damage to digital processes

Cybercriminals remain capable of causing extensive damage to digital processes. The use of ransomware in particular, can have significant consequences for national security. Notably, some ransomware actors focused solely on exfiltrating data. Instead of encrypting data and blackmailing victims, they did this by threatening to publish the data.

Large-scale outages also pose a threat, especially due to monocultures

In addition to cyberattacks, large-scale outages also pose a threat. Outages of digital processes can have various causes, including technical problems and unintentional human actions. In the summer of 2024, two large-scale outage incidents occurred due to a software error, severely hindering hospital care, aviation, government functions and more. The incidents demonstrated the potentially far-reaching and unforeseen consequences of a digital monoculture, in which many organisations depend on a small number of providers.

Cyber incidents are in line with the threat assessment

The cyber incidents described in the Annual Review are in line with the previous threat assessments. For instance, some incidents can be placed in the context of geopolitical tensions. These mainly concern the war against Ukraine, the conflict between Israel and Hamas, and tensions between the West and China. Globally, providers of vital processes have experienced disruption from cyberattacks. Notably, this included preparatory activities in the US for digital sabotage by a hacker group linked to China. In 2023, there were no reports of information security incidents in the Netherlands above the threshold values. Ransomware attacks again made headlines, including data breaches combined with extortion. Several Dutch healthcare institutions were hit by cyberattacks. As far as is known, these attacks had no impact on the care provided. Organisations also faced the consequences of cyberattacks on other organisations. Various disruptions to digital processes also occurred due to human or technical failure, such as those resulting from the global outage of Microsoft systems caused by an incorrect update of CrowdStrike software. In the Netherlands, various digital processes were disrupted by a software error on a Defence network.

Digital risks do not exist in isolation but are influenced by many different factors

As in previous years, we have seen various factors affecting and complicating digital risks. Even developments that seemingly have nothing to do with cybersecurity can have a lasting impact on digital threats and resilience. This applies, for example, to geopolitical and technological developments. A future powerful quantum computer, a technological development, already poses a risk to national security. Encrypted data that is intercepted and stored now could potentially be decrypted later using a quantum computer.

Global data trading is an example of a non-digital factor that influences digital risks. Some companies enrich the obtained sensitive personal data with other data, create user profiles and sell them. The large scale and precision of this data trade and its potential misuse can harm national security.

Another example is the shortage of cybersecurity experts in the Netherlands. This shortage can ultimately impact the digital resilience of the country. Additionally, it might become interesting for malicious actors to identify which organisations have the largest shortages – and potentially the weakest defences.

Digital risks require a comprehensive approach to risk management

Digital risks are influenced by many factors, including non-digital ones. Moreover, digital processes are highly interconnected and intertwined, collectively forming a broader digital ecosystem. An incident at one organisation can ripple through to many others, as demonstrated by CrowdStrike's faulty software update and the software error on a Defence network. Non-vital organisations can serve as an attractive springboard for malicious actors to reach vital organisations. State actors may carry out cyberattacks in combination with other, including non-digital, means. Individual cyberattacks can also be deployed in conjunction with each other. This combination can have a significant impact.

A comprehensive approach to risk management suits the diverse and dynamic nature of digital risks; it is also appropriate for managing the potentially unforeseen effects of an incident. In this context, it can be useful to assume that there is already a malicious actor in your network (assume breach) when setting up and managing a network. Furthermore, basic measures still form an effective barrier against many types of cyberattacks. The basic principles, established by the NCSC and the DTC, can serve as a starting point for this purpose.

Security of digital processes is essential and inextricably linked to national security

Digital processes form the nervous system of society, and the security of these processes is essential. Digital security is therefore inextricably linked to national security. It is also needed to maintain trust in digital processes. If that trust disappears, it can cause major problems in our digitalised society.

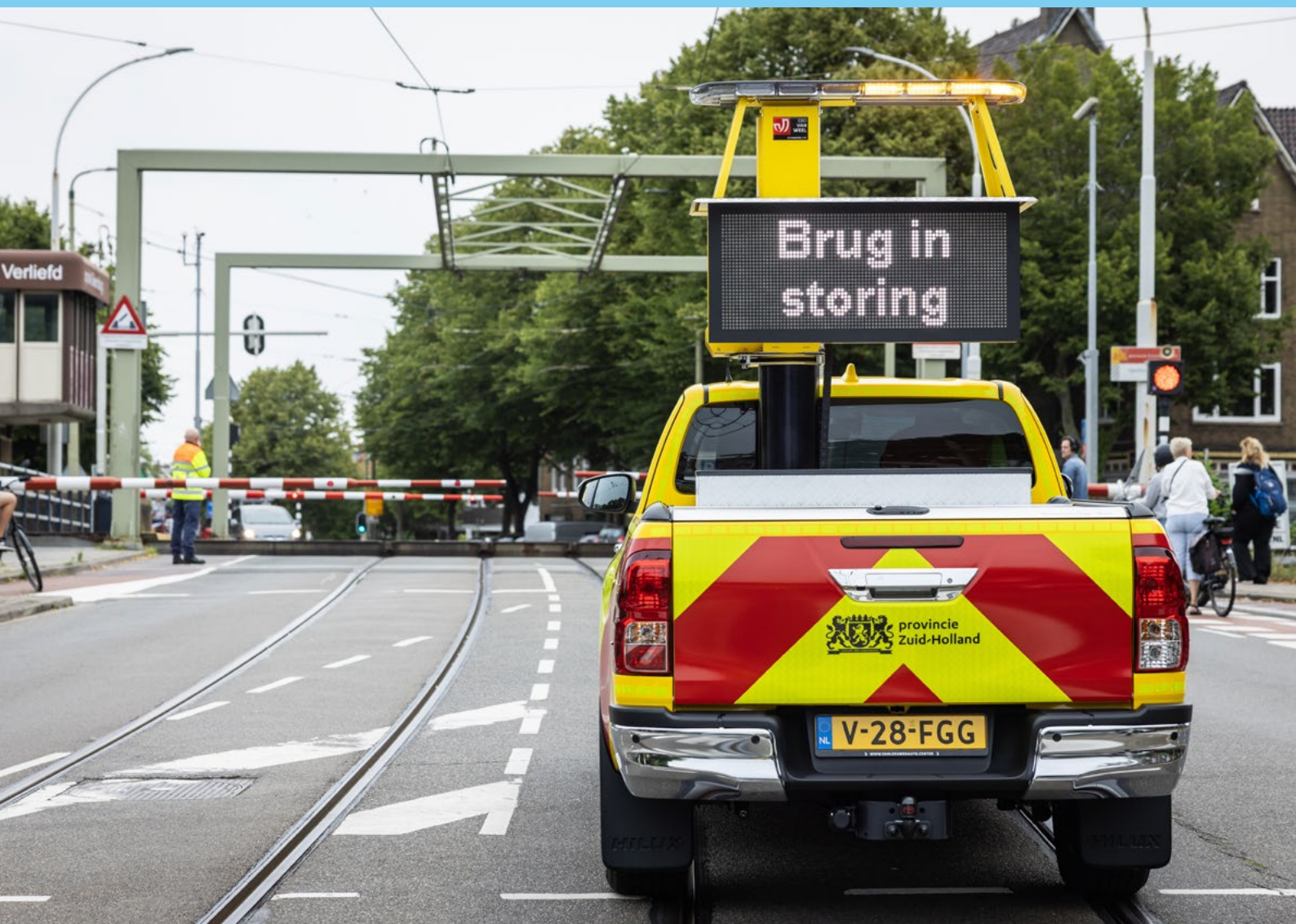
A significant development is that the importance of digital security is becoming anchored in new European and Dutch laws and regulations. However, it takes time before legislation actually leads to changes in digital resilience and influences digital risks. This not only relates to the design of legislation but also to awareness and preparation among companies, implementation organisations and supervisory authorities.

Structural and newly described challenges for digital security [I]

Structural challenges for digital security, also described in previous editions of the CSAN	New challenges for digital security, not described in previous editions of the CSAN
Geopolitical and technological developments influence threats	• State actors intensify activities and broaden capabilities. They use a broader toolkit, of which cyberattacks are 'merely' a part. • A future powerful quantum computer already poses a risk to national security.
State and criminal actors account for the lion's share of cyberattacks	• Actors seek new ways to carry out cyberattacks. Living-off-the-Land and targeting edge devices are characteristic modus operandi in 2023. • State actors intensify activities and broaden capabilities.
Any organisation can be a target for malicious actors	• Large-scale effects due to digital monocultures
Security of digital processes is and remains essential in a digitalised society	• Digital security is a prerequisite for trust in digital processes
Digital risks require a comprehensive approach to risk management	• Physical and digital incidents should be viewed in conjunction with each other. • State actors use a broader toolkit, of which cyberattacks are 'merely' a part. • Large-scale trade in sensitive personal data poses a threat to national security. • Large-scale concentration at major cloud providers poses a risk. • Large-scale effects due to digital monocultures
Legislation consolidates, implementation underway	• The importance of digital security is becoming further anchored in laws and regulations.
Non-digital developments influence digital security	• Large-scale concentration at major cloud providers poses a risk • Large-scale effects due to digital monocultures • Resilience at risk due to scarce cybersecurity capacity • Large-scale trade in sensitive personal data poses a threat to national security
Strategic themes still apply.	• Some additional challenges for risk management: • States intensify activities and broaden capabilities, and state cyberattacks do not stand alone but are part of a broader toolkit. • Actors seek new avenues to initiate cyberattacks. • The large-scale concentration at the three largest cloud providers. • Global online data trade. • The need for trust to want to use, and continue using, digital processes.

I The left column of the table corresponds to findings from Chapter 4, while the right column corresponds to findings from Chapter 3.

Infrastructure in het Netherlands, such as bridges and highways, have long been dependent on technical systems for operation and security. This also causes increasing vulnerability to cyber incidents. The past few years various locks, bridges and tunnels were temporarily closed because operating and security systems were not working properly. This caused long traffic jams.



1 Introduction

Purpose and scope

The Cybersecurity Assessment Netherlands, 2024 (CSAN 2024) provides insight into the digital threat, the interests that may be affected by this, digital resilience and, lastly, the digital risks. It also aims to provide an insight into possible changes in the strategic themes detailed in the CSAN 2022. These themes formed a substantive basis for the Netherlands Cybersecurity Strategy 2022–2028. CSAN 2024 built on these themes and describes developments within them. The CSAN provides a substantive basis for evaluating the action plan derived from it.

The emphasis is on national security. Digitalisation offers many opportunities, but it also lends itself to all kinds of exploitation, and outages may occur. The CSAN does not focus on the opportunities offered by digitalisation. It does, however, focus on disruptions of critical and other processes with a digital component.

The CSAN is intended primarily for strategic planning and policy-making at national level. It aims to provide insight to the government, the members of the Senate and the House of Representatives, civil servants, policymakers, other administrators and departments, and other interested parties into the digital risks for the Netherlands. Cybersecurity companies and professionals use the CSAN as a reference framework for their own management or customers. The CSAN is also intended as a tool for risk management, aimed specifically at the identification and analysis of risks, which is one of the steps in a risk management process. Finally, the CSAN is also available to the general public.

Reading guide

This CSAN consists of the preceding chapter, which articulates the main messages, and four in-depth chapters. This structure aims to allow readers from different target groups to browse through the CSAN and focus on topics that align with their professional role or interest. The in-depth chapters cover the following themes:

- Chapter 2, the Annual Review, provides a summary of relevant incidents in the Netherlands from March 2023 to June 2024 and their interpretation.
- Chapter 3 describes new challenges, changes in existing challenges or new insights that have been deemed relevant for strategy and policymaking.
- Chapter 4 provides insight into structural challenges for digital security. These challenges have been addressed in previous Cybersecurity Assessments in recent years and, with minor nuances, are still fully applicable. Unlike the other chapters, there is no explicit accountability of sources. After all, these challenges have already been published in previous editions of the CSAN.

Appendix 1 contains an account of how the CSAN was created. Appendix 2 contains A methodological explanation of the figures used on ransomware attacks. Appendix 3 contains the five basic digital resilience principles, prepared by the NCSC and DTC. Appendix 4 contains the sources and references.

Explanation of key concepts

The terms 'cyber' and 'digital' are used sparingly due to the interwovenness of the physical and cyberspace and for the sake of readability. The main concepts in the CSAN are defined as follows[1]:

- **Interest:** values, achievements, material and immaterial matters that may be damaged in the event a cyber incident occurs and the weight assigned to their defence by society or a party. The CSAN focuses on national security interests.
- **Cyberattack:** intentional activity by an actor aimed at disrupting one or more digital processes using digital means.
- **Cyber incident:** a (coherent set of) events or activities that can result in the disruption of one of more (digital) processes
- **Cybersecurity**: the set of measures to reduce relevant risks to an acceptable level. The measures may be aimed at preventing cyber incidents and, in the event cyber incidents occur, discovering them, limiting damage and facilitating repair. What constitutes an acceptable level is the outcome of a weighing of interests.Digital process (hereafter: process): a process that is carried out in whole or in part by the complex and mutually-related interaction between people and the many components of hardware, software and/or networks. The concept includes fully-automated processes such as process control systems.
- **Cyberspace:** the complex environment that is the result of interwoven digital processes, supported by worldwide distributed physical information and communication technology (ICT) devices and connected networks. Cyberspace is approached from three perspectives or layers: 1) digital processes carried out (or initiated) by actors; 2) the technical layer (of ICT and OT) that enables the digital processes; 3) the risk management and/or governance layer that controls the two other layers.
- **Threat:** the intentional or unintentional danger that could result in a cyber incident or a combination of simultaneous or consecutive cyber incidents.
- **Risk:** the (combination of the) probability that a threat results in a cyber incident and the impact of the cyber incident on interests, both in relation to the current level of digital resilience.
- **Outage:** a situation in which one or more digital processes are disrupted due to natural or technical causes or as a consequence of human error.
- **Disruption:** the impairment of the availability, integrity or confidentiality of information (processing), which means a disruption to the technical layer of cyberspace.
- **Resilience:** the ability to reduce (relevant) risks to an acceptable level by means of a set of measures aimed at preventing cyber incidents and, in the event cyber incidents occur, discovering them, limiting damage and facilitating repair. What constitutes an acceptable level is the outcome of a weighing of interests and the political and/or administrative decisions based thereon where it concerns (inter alia) selecting the correct technical, procedural or organisational measures.

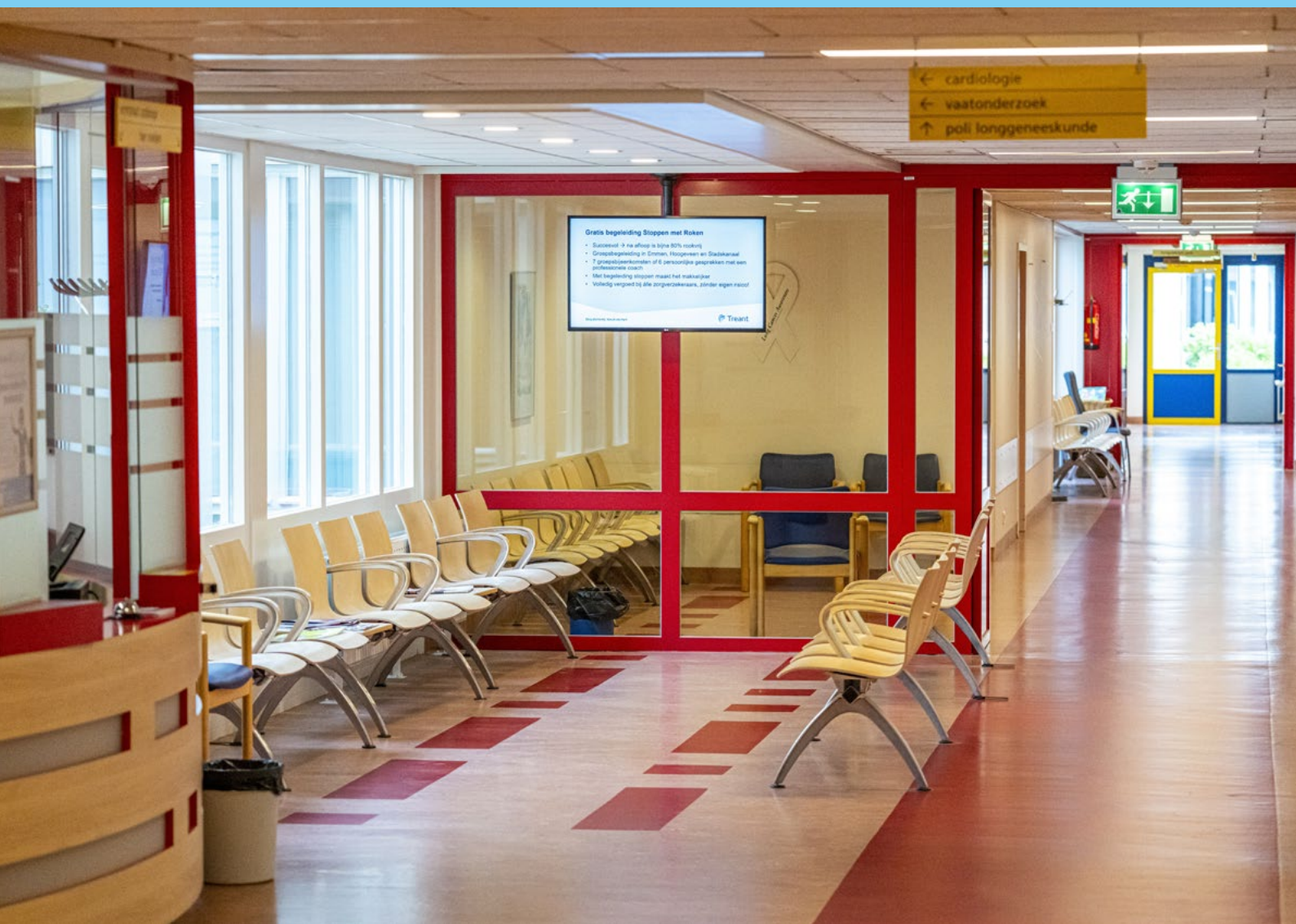
Different types of attacks

From an analytical standpoint, various types of attacks can be distinguished. Below are some types described in alphabetical order:

- **DDoS attack (Distributed Denial-of-Service):** an attack on the capacity of online services or the supporting servers and network equipment. As a result of this attack, digital services become poorly accessible or completely inaccessible to employees or customers.[2] A DDoS attack is easy to deploy, and tracing who is behind it is difficult. On the other hand, organisations can be relatively resilient against this type of attack, and its impact is limited. An example is the DDoS attack in April 2023 against the websites of the international organisation coordinating air traffic control in Europe (see Annual Review).
- **Defacement:** an actor changes the content on web pages or adds new web pages. Sometimes the actor leaves malware behind when defacing, which can infect visitors to the website.[3] A defacement thus compromises the integrity of web pages by providing incorrect information or, in the case of malware placement, can lead to a follow-up attack on visitors. Defacements are often carried out by hacktivists, who change the content of websites in accordance with their group's message. In 2022, pro-Ukrainian hacktivists defaced Russian government websites[4] with intimidating texts. Pro-Russian hacktivists did the same to Ukrainian government websites.[5]
- **Digital sabotage:** an actor deliberately and persistently compromises the availability of digital services, processes, or systems (by destroying them in extreme cases). This is possible through preparatory actions by gaining access to and embedding themselves in ICT and/or OT systems.[II][6] Preparatory actions can take a long time (months or years), require specific technical knowledge and primarily originate from state actors. Digital sabotage can have far-reaching consequences. An example of preparatory actions for digital sabotage are the Chinese APT Volt Typhoon's activities in the US's critical infrastructure (see Annual Review).
- **Digital espionage:** an actor compromises the confidentiality of information by copying or removing it.[7] The underlying motivation is to obtain sensitive or classified data or intellectual property. Digital espionage is primarily carried out by state actors. An example is Chinese digital espionage in the Netherlands using advanced malware that the Military Intelligence and Security Service (MIVD) uncovered on a computer network at the armed forces (see Annual Review).
- **Ransomware attack:** an actor encrypts user files using ransomware (software), with the aim of later decrypting them in exchange for ransom. In extreme cases, the ransomware blocks access to the system by also encrypting system files that are essential for the proper functioning of the system. An actor can use advanced types of ransomware to encrypt local systems as well as hard drives, databases, backups, USB sticks and data in the cloud. A ransomware attack at least compromises the availability of systems and data. In targeted ransomware attacks, the actor has access to the systems, potentially endangering the integrity and confidentiality of data. Cybercriminals primarily carry out ransomware attacks.
- **Supply chain attack:** an actor deliberately compromises the confidentiality, integrity or availability of one or more components within a supply chain to gain a springboard for attacks on other organisations, which are often the primary target. Through a supply chain attack, actors can, for example, gain access to organisations' secure ICT systems and thus to their sensitive data, processes, finances and more. As the attack has a layered nature (at least two attacks) and is targeted, complex and expensive, it requires extensive capacity and planning from the actor. Although the motive for the attack is usually espionage, it can also be aimed at sabotage or financial gain. An example occurred in March 2023, where hackers likely compromised the networks of thousands of companies as a result of a supply chain attack on the business phone company 3CX (see Annual Review).

II Operational technology (OT) is also referred to within industrial networks as Industrial Automation and Control Systems (IACS).

An empty waiting room in the Scheper hospital in Emmen. The emergency department of the regional hospital was closed on July 19, 2024 due to a global computer outage. Surgeries had to be canceled. Airports, government organizations and many other companies were affected worldwide. It turned out to be caused by a faulty software update of CrowdStrike's software.



2 Annual Review

Cyber incidents in the reporting period are in line with the threat assessment. Incidents, including DDoS attacks, sabotage and espionage, as well as preparations for them, can partly be placed in the context of geopolitical tensions and shifting international power dynamics. This mainly concerns the war against Ukraine, the conflict between Israel and Hamas and China's role on the world stage. Ransomware attacks once again made headlines, often involving data breaches combined with extortion. According to the Dutch Data Protection Authority ('Dutch DPA'), at least 178 ransomware attacks occurred in the Netherlands in 2023. It should also be noted that the number of victim organisations and affected members of the public is exponentially larger. After all, cyber incidents within the wider digital ecosystem spill over to other organisations and the general public. In most cyberattacks, state actors and cybercriminals emerge as the most likely perpetrators, while hacktivists are usually behind DDoS attacks. Besides cyberattacks, there were again numerous examples of disruptions due to unintentional actions. International operations by enforcement and investigative agencies disrupted parts of the criminal infrastructure. Some internationally operating cybercriminals were also arrested, and at the Netherlands' initiative, the EU placed cybercriminals on the sanctions list.

Cyber incidents are in line with the threat assessment

Availability of digital processes affected by ransomware, DDoS and disruptions

During this reporting period, digital processes were unavailable due to ransomware attacks, DDoS attacks and disruptions. Various websites were repeatedly disrupted by DDoS attacks, including in the Netherlands. The impact remained limited, and hacktivists are mainly interested in media attention and spreading fear.

Ransomware attacks had a greater impact. In the case of the ransomware attack on maritime service provider Royal Dirkzwager, it took almost a week before systems were restored and services could resume. Additionally, there were various disruptions due to human or technical failure, such as the global outage of Microsoft systems caused by a CrowdStrike update. This outage had a major impact worldwide, including in the Netherlands, air traffic and healthcare experienced problems. In August, a national malfunction followed when there were issues with a Defence network. Government organisations and Eindhoven Airport experienced major hindrance in the process.

DDoS attacks against Dutch organisations stem from geopolitical tensions

Geopolitical tensions have led to DDoS attacks against Dutch organisations, among other things. This reporting period saw several incidents in which DDoS attacks disrupted digital processes, albeit briefly. Some of the attacks were claimed by pro-Russian actors who presented themselves as hacktivists. The conflict in Gaza has also led to DDoS attacks. For example, the Centre for Information and Documentation Israel (CIDI) was the victim of persistent DDoS attacks in October and November 2023. It is unknown who is responsible for these attacks. Although DDoS attacks are limited and symbolic in nature, they can temporarily affect the availability, information provision and/or services of the affected website(s).

State actors carry out cyberattacks, including in the Netherlands

Countries with offensive cyber programmes also carried out cyberattacks during this period, including in the context of the war in Ukraine. State cyberattacks also came to light in the Netherlands. For instance, a cybersecurity company saw hackers carry out multiple cyberattacks on Dutch telecom and media companies, presumably to gather personal information. Additionally, the Ministry of Defence announced that it had found Chinese spyware on an unclassified research network of the armed forces. About this malware, called COATHANGER, the intelligence and security services and the NCSC published a report.

Data breaches by ransomware actors

During this reporting period, there were numerous incidents involving ransomware actors globally, including in the Netherlands. These actors often did not just extort organisations by demanding ransom for decrypting files but also by threatening to publish stolen data. And some ransomware actors focused on extortion solely by threatening to publish stolen data. An illustrative example of this is the large-scale data exfiltration[III] in the MOVEit incident. In this attack, the ransomware actors did not use file encryption but stole a large amount of data after which organisations were extorted. Several Dutch companies were also victims of this. In ransomware attacks, it is not always publicly known whether ransomware was used or if the actors only stole data. Either way, double extortion still seems to occur frequently. In about 50% of the ransomware attacks investigated by the Dutch DPA, data extraction occurred in combination with encryption. This happened more often at the end of 2023 than at the beginning of 2023.[8]

At least 178 ransomware attacks in the Netherlands in 2023; number of victims many times larger

According to the Dutch DPA, at least 178 ransomware attacks occurred in the Netherlands in 2023. The Dutch DPA bases these figures on an analysis of legally required data breach notifications.[9] However, Melissa, the public-private partnership, reports at least 147 ransomware attacks on larger organisations (from around 100 FTEs) in the Netherlands in 2023.[10] Melissa based these figures on primary research data including police reports, anonymised information from cybersecurity companies directly involved in handling these cyber incidents and reports made to the NCSC.[IV]

Besides the organisations directly affected by a ransomware attack, many other organisations and customers of those organisations may also have been victims. Attacks on digital service providers (e.g. Internet Service Providers, data centres and telecom companies) can affect many other organisations – and, indirectly, the general public as well – because they depend on these services. Due to dependence on suppliers for certain products and services, there is a risk that customers could become secondary victims through the supply chain if an attack occurs on a supplier. Just one attack resulted in a data breach affecting approximately 2.5 million Dutch individuals (see below).

Attacks on suppliers cause problems further down the supply chain

A cyber attack on the supply chain not only damages the compromised company but also affects other organisations. During this period, we have seen various attacks in which a company providing digital processes, sometimes for many other organisations, fell victim to a cyber attack, after which other companies in the supply chain experienced problems. Service providers Nebu and AddComm were victims of cyberattacks in the Netherlands. Subsequently, both direct and indirect customers of these companies reported actual or potential data breaches. It might be coincidental that these specific companies were attacked, but it could also be a deliberate stepping stone to other organisations or intended to increase the pressure of extortion. This period also saw attacks by sophisticated actors that may have been intended as supply-chain attacks. For instance, 3CX software was infected with malware, potentially compromising the networks of thousands of companies. The backdoor found in the widely used Linux software, the data compression application XZ Utils, was another notable incident. Although this attack has not been definitively attributed yet, open sources assume it is a state actor. This could have allowed

III Data exfiltration, also known as data theft, is a process by which data is stolen during a cyber attack.

IV For a methodological explanation of these figures and an explanation of the difference, see Appendix 2.

the actor to compromise a large number of organisations. While this case shows that open source software can be vulnerable to backdoor insertion, it also highlights the advantage that this manipulation can be detected.

Exploiting vulnerabilities formed the starting point for some cyberattacks

The exploitation of vulnerabilities remains an important starting point for an attack (attack vector). This reporting period saw various incidents worldwide where zero-day and other vulnerabilities were exploited. Combined data from Google and Mandiant shows, for example, that 97 zero-days were exploited throughout 2023, compared to 62 in 2022.[11] An example of this is the large-scale exploitation of vulnerabilities in the Ivanti Connect Secure VPN solution. This product contained multiple vulnerabilities that were exploited by both state actors and cybercriminals. Several organisations in the Netherlands were also affected.

Healthcare organisations fall victim to cybercriminals, Dutch organisations also affected

More than once during this reporting period, we have seen healthcare organisations become victims of cyberattacks. These often involved ransomware, extortion with stolen data or both. Many of these attacks occurred abroad and had an impact on the care to be provided. Several Dutch healthcare institutions were also affected by cyberattacks. As far as is known, these had no impact on the care provided in the Netherlands. However, organisations were blackmailed with stolen data and data was leaked. This often involved sensitive personal information. Healthcare institutions were directly affected by cyberattacks. But there were also incidents at healthcare suppliers that caused problems for healthcare institutions. Z-CERT states that suppliers of healthcare institutions are more often affected than healthcare institutions themselves.[12] This was illustrated abroad by the ransomware attack on an information system of Romanian hospitals, forcing them to revert to pen and paper. There was also an attack on a service provider of British hospitals, causing operations to be cancelled. And in the US, a financial service provider was hit by ransomware, preventing American healthcare from receiving payments and pharmacies from dispensing medication. The fact that healthcare institutions are directly or indirectly affected does not mean that there is a targeted choice of targets.

Worldwide, providers of vital processes are hindered by cyberattacks

During this reporting period, there were reports of various types of cyberattacks affecting companies in vital sectors in Western countries, many of which were successful. A distinction can be made between deliberate sabotage, espionage and the preparations for them, and operations driven by financial gain. A notable example was the preparatory activities for digital sabotage by the China-linked APT Volt Typhoon in the military and civilian infrastructure of the US. In Ireland, a cyber incident occurred that actually disrupted vital processes. However, it only had a limited impact, briefly interrupting the water supply. Hackers had targeted digital equipment that controlled the water supply. Water authorities in the US were also compromised, although with no impact on operational activities. In this context, Microsoft also warned of attacks on poorly secured OT systems. Since the end of 2023, Microsoft has seen an increase in the number of reports of attacks targeting internet-exposed, poorly secured OT devices. Shortly after the outbreak of the war between Israel and Hamas, it noted an increase in the number of reports of attacks against OT systems of Israeli origin.[13] This target choice was probably based on the use of equipment from an Israeli firm and not against the affected organisations themselves. In Australia, several major ports struggled with the consequences of a cyberattack. DP World, the country's second-largest port operator, halted internet traffic as a precaution after discovering a cyberattack. In Curaçao, the internal systems and customer service of electricity company Aqualectra were hit by a ransomware attack, rendering them temporarily unavailable.

Under the current Network and Information Systems Security Act (Wbni), if an incident causes the consequences for the continuity of a service to exceed a sector-specific threshold value, a vital organisation must report the incident to the National Cyber Security Centre (NCSC).[14]Despite incidents indicating that critical infrastructure is certainly not exempt from cyber incidents, no reports of information security incidents above the threshold value were received in the Netherlands in 2023.

2023

March

Inland

- Sensitive data of Attent Zorg en Behandeling employees leaked after ransomware attack
- Personal data of 48,000 visitors of the Amsterdamse Waterleidingduinen leaked
- Data leaked from maritime services provider Royal Dirkzwager after a ransomware attack
- Data of 2.5 million customers from 190 organisations leaked after ransomware attack on software supplier Nebu

Abroad

- Emergency department of Brussels Sint-Pieter hospital temporarily closed after cyber attack
- Data theft at dozens of organisations due to exploitation of zero-day vulnerability in GoAnywhere MFT
- Supply chain attack on VoIP company 3CX by suspected North Korean hackers

April

Inland

- Ransomware group publishes data of Joris Zorg clients and employees
- Temporary suspension of provider SKP's services due to ransomware attack

Abroad

- Hackers disrupt government websites in over half of German states
- Cybercriminals steal data from Belgian municipality of Herselt using a software supplier's login credentials
- Accessibility of Eurocontrol websites affected by DDoS attacks

May

Inland

- Rechtspraak.nl and States General website temporarily difficult to access or inaccessible due to DDoS attacks
- HVC customer portal inaccessible due to cyberattack on an IT supplier

Abroad

- Critical US infrastructure compromised

June

Inland

- Large-scale data theft after exploitation of vulnerabilities in MOVEit, Dutch organisations also affected
- Websites of Dutch ports temporarily inaccessible due to DDoS attacks
- Train traffic chaos in and around Amsterdam due to IT outage

July

Inland

- Data of residents from four municipalities leaked due to software error in citizen portal

Abroad

- Operations of Norwegian ministries disrupted, data theft conceivable

August

Inland

- Accessibility of various Dutch websites impaired by DDoS attacks

Abroad

- Polish trains brought to a halt by fake radio stop signal

September

Inland

- Lyca Mobile customers temporarily unable to make calls and top up due to cyber attack

October

Inland

- Targeted cyberattack on International Criminal Court (ICC), impact unknown, data possibly stolen
- Centre for Information and Documentation Israel (CIDI) targeted in DDoS attacks

Abroad

- Strategic NATO documents stolen and posted online by hackers
- Database of European Telecommunications Standards Institute stolen

2024

November

Inland

- Nationwide outage of emergency button system for elderly and vulnerable, due to ransomware attack

Abroad

- Compromise of critical Danish infrastructure
- Australian port operations disrupted by cyber attack
- Irish village without water for two days due to cyberattack on local water supply
- Multiple US water facilities compromised, but no impact on drinking water supply

December

Inland

- Aqualectra systems and customer service unavailable due to ransomware attack

Abroad

- Iran-linked hackers claim responsibility for cyberattacks on Albanian parliament and telecom company

January

Inland

- Hackers of APT Sea Turle target Dutch telecom and media companies
- Active exploitation of vulnerabilities in Ivanti Connect Secure, Dutch companies also compromised

February

Inland

- Chinese hackers compromise Dutch defence computer system

Abroad

- Dozens of Romanian hospitals offline after ransomware attack on IT platform
- US pharmacies and healthcare payments disrupted by ransomware attack on service provider

March

Inland

- Political party websites temporarily inaccessible due to DDoS attacks
- Webex meta-data accessible due to vulnerabilities
- Mobile banking app malfunctions cause problems for users
- Data of 60,000 people leaked due to poorly secured software
- Part of RDW's online services not continuously available due to a malfunction
- Calling and internet temporarily impossible for Odido customers due to router problems

Abroad

- British hospitals cancel operations due to ransomware attack on laboratory
- IT system TeamViewer compromised by Russian hackers
- Sensitive personal information from identity and age verification service accessible online

April

Inland

- Cybercriminals steal data from chip maker Nexperia
- Russian propaganda shown on children's channel after deliberate disruption
- Secret deactivation codes of thousands of alarm systems retrievable due to software error
- Active exploitation of vulnerability in Palo Alto product

Abroad

- Backdoor discovered in widely used Linux software

May

Inland

- Various organisations report data breach after ransomware attack on AddComm
- Malware discovered at several shipping companies
- Problems with card transactions due to major nationwide card payment malfunction

June

Inland

- Political party websites temporarily inaccessible due to DDoS attacks
- Webex meta-data accessible due to vulnerabilities
- Mobile banking app malfunctions cause problems for users
- Data of 60,000 people leaked due to poorly secured software
- Part of RDW's online services not continuously available due to a malfunction
- Calling and internet temporarily impossible for Odido customers due to router problems

Abroad

- British hospitals cancel operations due to ransomware attack on laboratory
- IT system TeamViewer compromised by Russian hackers
- Sensitive personal information from identity and age verification service accessible online

July

Inland

- Air traffic, healthcare and others disrupted by global computer outage due to faulty update

August

Inland

- Government services and air traffic in Eindhoven disrupted by software error on Defence network

Notable incidents in the Netherlands 2023

March 2023

Sensitive data of Attent Zorg en Behandeling employees leaked after ransomware attack
Cybercriminals from the Qilin ransomware group leaked copies of passports, payslips, non-disclosure agreements and confidential internal communications of current and former Attent Zorg en Behandeling employees. The organisation fell victim to a ransomware attack in February. After the hack, internal IT systems and email and telephone systems were no longer accessible. The cybercriminals claimed they had stolen hundreds of gigabytes of data, part of which were published.[15]

Personal data of 48,000 visitors of the Amsterdamse Waterleidingduinen leaked
Hackers managed to obtain data of people who purchased online parking and access tickets for the Amsterdamse Waterleidingduinen between 2015 and 2021. This concerns the names and bank account numbers of 48,000 visitors, which were likely stolen earlier through a security flaw in Waternet's website. This came to light during a large-scale police investigation into computer intrusion, data theft, extortion, blackmail and money laundering.[16]

Data leaked from maritime services provider Royal Dirkzwager after a ransomware attack
The Dutch maritime service provider Royal Dirkzwager was hit by a ransomware attack from the Play ransomware group. The company needed almost a week to fully restore its systems and resume services. Customers had to take emergency measures, including physical supervision of drilling rigs.[17] Additionally, the hacker leaked confidential information from the organisation, including employee IDs, passports and contracts.[18]

Data of 2.5 million customers from 190 organisations leaked after ransomware attack on software supplier Nebu
As a result of a ransomware attack on software supplier Nebu, personal data of approximately 2.5 million individuals from 190 organisations in the Netherlands were leaked. [19] Data were leaked from five to ten market research agencies, mainly names, e-mail addresses and phone numbers. The market research agencies used Nebu's software.[20] These data contained personal information that the customers of the market research agencies had provided to them.

April 2023

Ransomware group publishes data of Joris Zorg clients and employees
Cybercriminals published stolen data of clients and employees of the Brabant care institution Joris Zorg. In December 2022, the organisation suffered a cyberattack, with hackers from the LockBit ransomware group demanding a ransom. The criminals claimed 100 gigabytes of data were stolen. They subsequently published these data in April 2023, after no payment was made.[21]

Temporary suspension of provider SKP's services due to ransomware attack
Internet and television services provider Stichting Kabeltelevisie Pijnacker (SKP) was temporarily unable to provide its services to customers due to a ransomware attack. The provider also experienced problems with its phone service.[22]

May 2023

Rechtspraak.nl and States General website temporarily difficult to access or inaccessible due to DDoS attacks
The public part of Rechtspraak.nl was difficult to access or inaccessible for several days due to a DDoS attack. The States General website was temporarily difficult to access for the same reason.[23] According to a cybersecurity company, pro-Russian hacktivists are likely responsible.[24]

HVC customer portal inaccessible due to cyberattack on an IT supplier
A customer portal of energy supplier and waste processor HVC was temporarily inaccessible due to a cyberattack on an IT supplier's data centre. For HVC, the attack meant that employees could not access the customer system and billing was delayed. Malicious actors possibly also viewed or stole customer data. Although the company suspects this is not the case, it cannot rule it out.[25] No ransom was reportedly demanded from HVC.[26]

June 2023

Large-scale data theft after exploitation of vulnerabilities in MOVEit, Dutch organisations also affected
Organisations worldwide fell victim to data theft after cybercriminals from Clop carried out a large-scale campaign by exploiting a zero-day vulnerability in the file transfer application MOVEit Transfer.[27] In the Netherlands, Landal Greenparks and Shell, among others, reported a data breach as a result of this campaign. At least a dozen Dutch organisations were reportedly affected.[28] More and more victims came forward in the months following the attacks. Security company Emsisoft estimates that more than 2,700 companies worldwide have fallen victim.[29]

Websites of Dutch ports temporarily inaccessible due to DDoS attacks
The websites of the port companies in Rotterdam, Amsterdam and Den Helder were inaccessible for a few hours due to DDoS attacks. The website of the Groningen Seaports was inaccessible for two days. A pro-Russian hacktivist group claimed responsibility for the attacks.[30]

Train traffic chaos in and around Amsterdam due to IT outage
Train traffic in and around Amsterdam was severely disrupted because ProRail's traffic control centre experienced an IT outage. The disruption also caused problems elsewhere on the railway and stranded travellers who could not spend the night at home.[31]

July 2023

Data of residents from four municipalities leaked due to software error in citizen portal
Data of residents from four municipalities was leaked due to a software error in a digital citizen portal. An incorrect button was visible in the citizen portal after a software update was installed. When this button was pressed, the system sometimes displayed a document belonging to someone else. Data of more than 29 residents of the municipality of Apeldoorn was leaked, including their name, address, date of birth and BSN (citizen service number). It is unknown which other municipalities were affected.[32]

August 2023

Accessibility of various Dutch websites impaired by DDoS attacks
In August, Dutch websites struggled with DDoS attacks, making them temporarily inaccessible or difficult to reach. Targets in early August included Maastricht Airport, the municipality of Vlaardingen and BNG Bank.[33] Attacks followed later in the month at Groningen and Schiphol airports. Only the website of Groningen Airport Eelde was temporarily inaccessible.[34] Pro-Russian hacktivists claimed responsibility for the attacks. A number of local news websites were also temporarily offline due to DDoS attacks; the party responsible for these attacks are unknown.[35]

September 2023

Lyca Mobile customers temporarily unable to make calls and top up due to cyber attack
The provider Lyca Mobile confirmed it had fallen victim to a cyber attack which had a global impact, including in the Netherlands. Due to this attack, customers were unable to top up their accounts. The attack also affected the ability to make national and international calls. The type of attack was not disclosed.[36]

October 2023

Targeted cyberattack on International Criminal Court (ICC), impact unknown, data possibly stolen
The ICC in The Hague was victim to a cyberattack. The type of attack and its impact were not disclosed. The ICC suspects it may involve espionage and undermining of its work.[37] Media reports suggested that sensitive documents were stolen.[38]

Centre for Information and Documentation Israel (CIDI) targeted in DDoS attacks
The CIDI was the target of sustained DDoS attacks in October and November. According to the online security company hired by CIDI, the attacks were of an unprecedented scale. The party responsible for these attacks is unknown.[39]

November 2023

Nationwide outage of emergency button system for elderly and vulnerable, due to ransomware attack
A ransomware attack on Tunstall temporarily disrupted the operation of an emergency button system used by elderly and vulnerable people in the Netherlands. Systems and data were encrypted during this attack. The attack was reportedly limited to the company's control room environment and did not affect adjacent systems. During the attack, criminals had access to data, but it is not known exactly what data was involved.[40]

December 2023

Aqualectra systems and customer service unavailable due to ransomware attack
A ransomware attack blocked access to the internal systems and customer service of electricity company Aqualectra (Curaçao).[41] The attack forced the company to temporarily shut down all online connections. Although the company managed to minimise the damage, hackers did steal outdated data. The hackers also reportedly demanded a ransom. The company decided not to pay, claiming that no sensitive customer data had been stolen. The water and power supplier also emphasised that the attack had not caused recent power outages in Curaçao.[42]

Notable incidents in the Netherlands 2024

January 2024

Hackers of APT Sea Turle target Dutch telecom and media companies
According to a cybersecurity company, hackers of APT Sea Turtle have carried out cyberattacks on Dutch telecom and media companies over the past year. The hackers were allegedly targeting personal data of specific groups of Dutch nationals.[43]

Active exploitation of vulnerabilities in Ivanti Connect Secure, Dutch companies also compromised
This month, Ivanti warned of two vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure Gateways that allow an unauthenticated attacker to execute commands on the VPN system. Cybersecurity researchers quickly reported widespread exploitation. Several China-linked hacker groups were said to be exploiting the vulnerabilities in Ivanti Connect Secure for cyberattacks, including on the US energy sector.[44] The NCSC confirmed that companies in the Netherlands have also been compromised through these vulnerabilities.

February 2024

Chinese hackers compromise Dutch defence computer system
The Ministry of Defence discovered Chinese spyware on an unclassified computer system of the armed forces in 2023. According to the MIVD, it was advanced espionage malware placed by Chinese hackers. The malware, named COATHANGER, was found on a standalone computer network for Research and Development, which had fewer than 50 users.[45]

April 2024

Cybercriminals steal data from chip maker Nexperia
Nexperia's data was stolen and partially leaked following an attack by cybercriminals. Initially, internal company emails were leaked, but the hackers also claimed to possess trade secrets, chip designs and customer data.[46]

Russian propaganda shown on children's channel after deliberate disruption
The broadcast of children's channel BabyTV was interrupted by signal hijacking, resulting in Russian propaganda being shown for a period on the channel in the Netherlands, Scandinavia and Portugal.[47] Following an incident in March, there was another interruption in April when Russian propaganda was displayed on BabyTV. The action does not appear to have targeted BabyTV specifically but was collateral damage from a broader effort aimed at disrupting Ukrainian channel broadcasts.[48]

Secret deactivation codes of thousands of alarm systems retrievable due to software error
A vulnerability in Carrier Global's software made it possible to remotely deactivate thousands of alarm systems for a year. The breach happened in a Carrier Global app used by alarm system installers to access data from their own customer base: MAS Mobile Classic. The software, which is used by alarm centre SMC, among others, affects at least 26,000 active Dutch security systems. Due to an error in the server software where the app stored data, the confidential information was accessible online. In addition to deactivation codes, home addresses of CEOs, Quote 500 members, celebrities, and even a former minister were accessible. SMC gave prominent individuals a separate designation, making them easier to find. According to the company, there are no indications that malicious actors exploited the flaw.[49]

Active exploitation of vulnerability in Palo Alto product
The NCSC observed active exploitation in the Netherlands of a vulnerability in Palo Alto PAN-OS. This is software that runs on all Palo Alto Networks® next-generation firewalls.[50]

May 2024

Various organisations report data breach after ransomware attack on AddComm
Service provider AddComm was victim to a cyberattack. Systems were encrypted and data was stolen.[51] Data was also taken from a select group of AddComm customers. While the affected customers haven't been named, ABN Amro, the Regional Tax Group, Dunea, Essent and various municipalities reported potential data breaches. AddComm is a communications company that handles customer communications for various organisations.[52]

Malware discovered at several shipping companies
ESET discovered malware in the systems of several shipping companies in Norway, Greece and the Netherlands. This affected both cargo ships and office systems. In some cases, the malware came from a USB stick. ESET attributes the attacks to a Chinese APT.[53]

Problems with card transactions due to major nationwide card payment malfunction
On 16 May, a major nationwide card payment malfunction caused problems in 30 to 40% of card transactions. The problem, which lasted for about three hours and led to long queues in shops, lay with one of the transaction processors. It has not been disclosed whether it was human or technical error.[54]

June 2024

Political party websites temporarily inaccessible due to DDoS attacks
On the day of the European elections in the Netherlands, several Dutch political parties reported that their websites were difficult to access due to DDoS attacks. Pro-Russian hacktivists claimed responsibility for the attacks.[55]

Webex meta-data accessible due to vulnerabilities
Journalistic research revealed vulnerabilities in the cloud version of Cisco Webex, allowing meeting metadata to be retrieved. The journalist was able to collect data from governments and companies in Germany, the Netherlands, Italy, Austria, France, Switzerland, Ireland and Denmark. She was also able to listen in on two online meetings. The NCSC has no indications that this vulnerability has been actively misused.[56]

Mobile banking app malfunctions cause problems for users
In June, mobile banking apps malfunctioned several times. On 21 and 24 June, for example, this lasted for hours affecting the banking apps of SNS, ASN, and Regiobank, all part of de Volksbank. Customers were affected differently. The cause is unknown.[57] ING also struggled with a technical glitch that week, which caused the mobile banking app to malfunction. Transfers could not be made. The problem was reportedly caused by a fire alarm in a data centre. A gas extinguishing system caused 'some systems' to shut down there.[58]

Data of 60,000 people leaked due to poorly secured software
An ethical hacker discovered a data leak at DUO, which meant the email addresses of 60,000 people with student debt were briefly visible online. These were debtors who had been approached for a survey using Survalyzer software that proved to be poorly secured. As many email addresses contained names, it was often clear who the debtors were.[59]

Part of RDW's online services not continuously available due to a malfunction
On Thursday, 13 June, a malfunction at the Netherlands Vehicle Authority (RDW) meant that some of the online services, such as vehicle registration and MOT sign-off, were not continuously available. The glitch occurred when a cleaning script was not completed on time and caused delays and disruptions as online services were starting up. The rollback mechanism that then came into effect took longer than expected. A day later, the sector was still busy catching up with backlogs.[60]

Calling and internet temporarily impossible for Odido customers due to router problems
Telecom provider Odido experienced malfunctions in various regions on 30 June, causing customers to temporarily lose the ability to make calls and use the internet. Odido announced that there was a problem with a router on the main network.[61]

The Annual Review covers the period from March 2023 to June 2024.
Given their impact, two incidents that occurred after this period have been included.

July 2024

Air traffic, healthcare and others disrupted by global computer outage due to faulty update
On 19 July, CrowdStrike introduced a software update that rendered approximately 8.5 million Windows systems unusable worldwide.[62] The error caused 'Blue Screens of Death' on Windows systems.[63] This led to significant problems globally, including in the Netherlands. Schiphol Airport cancelled flights and some hospitals scaled back care. Parts of the government were also affected, including the Ministry of Foreign Affairs and the UWV (Employee Insurance Agency).[64] Although some companies got back online relatively quickly after performing the labour-intensive workaround, some CrowdStrike customers were still experiencing problems a few days later.

August 2024

Government services and air traffic in Eindhoven disrupted by software error on Defence network
At the end of August, emergency services and various government institutions struggled with an IT outage. Emergency services encountered problems with their communication and alarm system, making it more difficult for them to communicate with each other. Civil servants from various ministries could not log in to work systems. Eindhoven Airport was also affected as it uses the same network. Planes could not take off or land there. Reports also came from various municipalities where services were disrupted. For example, driving licences and passports could not be issued. Additionally, DigiD (Dutch digital identity system) experienced a glitch. [65] The cause of the problems lay in the access provision to the Netherlands Armed Forces Integrated Network (NAFIN). This heavily secured network connects Defence locations, among others, and is also used at data centres of various ministries and police stations. An error in the software code caused a time synchronisation issue on the network. According to the Minister of Defence, there is no indication as yet that a malicious actor caused the issue. [66]

Notable incidents abroad 2023

March 2023

Emergency department of Brussels Sint-Pieter hospital temporarily closed after cyber attack
The emergency department of Brussels Sint-Pieter hospital was temporarily closed on 11 March due to a cyberattack. According to Belgian media, this resulted in blocked patient files and telephone lines. Calls to 112 were redirected to other hospitals. Patients reportedly did not experience any inconvenience and, according to the hospital, no data was stolen. Open sources do not reveal the exact nature of the attack.[67]

Data theft at dozens of organisations due to exploitation of zero-day vulnerability in GoAnywhere MFT
Dozens of international organisations reported data theft due to the exploitation of a zero-day vulnerability in GoAnywhere MFT. This includes Procter & Gamble, Hitachi Energy, Community Health Systems (CHS), Crown Resorts, Hatch Bank, the British Pension Protection Fund, the city of Toronto and Brightline. Criminals behind the Clop ransomware have claimed responsibility for the attack and claim to have stolen data from at least 72 organisations.[68]

Supply chain attack on VoIP company 3CX by suspected North Korean hackers
Hackers likely compromised the networks of thousands of companies as a result of a supply chain attack on business phone company 3CX. Malware was found in the official desktop application of the popular VoIP software 3CX. Although 600,000 thousand companies worldwide use this software, the actual impact of this large-scale attack on organisations is unclear.[69] At least two critical infrastructure organisations in Europe were reportedly affected in this manner. [70] 3CX, Symantec and others claimed that North Korean hackers were responsible for this.[71]

April 2023

Hackers disrupt government websites in over half of German states
Websites of government agencies in over half of Germany's states were targeted by DDoS attacks. As a result, official state sites, police websites and sites of the Ministry of the Interior were temporarily inaccessible. The German Public Prosecution Service stated that there were indications the attackers had a pro-Russian background.[72]

Cybercriminals steal data from Belgian municipality of Herselt using a software supplier's login credentials
Cybercriminals gained access to the servers of the Belgian municipality of Herselt using login credentials from a software supplier. They then used malware to steal 180 gigabytes of data, including residents' personal data. Systems were shut down to investigate the incident, disrupting a significant portion of municipal services for days.[73]

Accessibility of Eurocontrol websites affected by DDoS attacks
Several websites of Eurocontrol, the international organisation coordinating air traffic control in Europe, were hit by a DDoS attack. A pro-Russian hacking group claimed responsibility for the attack. According to Eurocontrol, the attack caused interruptions to the websites but had no impact on European aviation.[74]

May 2023

Critical US infrastructure compromised
The United States and Microsoft claim that hackers have infiltrated US critical infrastructure, possibly in preparation for potential acts of sabotage. The hackers, tracked as Volt Typhoon, have reportedly been active since mid-2021 and are primarily targeting critical US infrastructure.[75] According to US authorities, Volt Typhoon is a China-based group.[76] Mindful of the geopolitical tensions surrounding Taiwan, US officials stated that China aims to exploit the access it has gained to American organisations in the event of a war or conflict.[77]

July 2023

Operations of Norwegian ministries disrupted, data theft conceivable
Twelve Norwegian ministries were hacked, with the attackers exploiting vulnerabilities in Ivanti Endpoint Manager Mobile. The hackers may have gained access to sensitive data, and it is conceivable that this data has been stolen. The party responsible for these attacks is unknown. Due to the cyberattack, civil servants at twelve different ministries could not log in to their email and other applications.[78]

August 2023

Polish trains brought to a halt by fake radio stop signal
Malicious actors brought multiple trains to a halt using an unauthorised radio stop signal. The actor reportedly also broadcast the Russian national anthem and a speech by the Russian president. [79]

October 2023

Strategic NATO documents stolen and posted online by hackers
Over 3,000 NATO documents appeared online after hackers from the hacking group SiegedSec claimed they had hacked NATO. The hackers may have broken into at least four web portals, involving non-classified NATO websites.[80]

Database of European Telecommunications Standards Institute stolen
The European Telecommunications Standards Institute (ETSI), based in France, announced that hackers had stolen a database identifying its users. ETSI has more than 900 members from over 60 countries, including private companies, research institutions, academia, government and public organisations. It is unclear what information about them was in the stolen database. It is also unclear whether the attack was financially motivated or if the hackers intended to obtain the list of users for purposes such as espionage.[81]

November 2023

Compromise of critical Danish infrastructure
SektorCERT, a non-profit cybersecurity centre for critical sectors in Denmark, reported that attackers gained access to the systems of 22 companies overseeing various components of the Danish energy infrastructure in May 2023. Most attacks could have been prevented if companies had updated their firewalls. SektorCERT suspects that a state actor is responsible. According to researchers, the attacks were meticulously planned and coordinated, with the aim of gathering intelligence.[82]

Australian port operations disrupted by cyber attack
In Australia, several major ports struggled with the consequences of a cyberattack. DP World, the country's second-largest port operator, preventively shut down internet traffic after detecting a cyberattack. Media reported that hackers had infiltrated the system.[83] While ransomware was not involved, data was stolen. The disruption stranded over 30,000 containers.[84]

Irish village without water for two days due to cyberattack on local water supply
A cyber incident in Ireland briefly interrupted a local water supply. Hackers targeted digital equipment of Israeli origin that controlled the water supply. Anti-Israeli messages were reportedly displayed on the hacked equipment.[85]

Multiple US water facilities compromised, but no impact on drinking water supply
Various water facilities in the US were hacked. The Cyber Av3ngers hacked a booster station of the Aliquippa Municipal Water Authority.[86] A water facility in Pennsylvania also fell victim to a cyberattack. The cyberattacks did not lead to any disruption of water supplies or pose a threat to drinking water quality.[87] According to US authorities, the attackers targeted Israeli equipment used in these facilities. The US linked the attacks to Iranian hackers and associated them with the Israel-Hamas conflict. US and Israeli authorities attribute 'Cyber Av3ngers' to Iran's IRGC.[88]

December 2023

Iran-linked hackers claim responsibility for cyberattacks on Albanian parliament and telecom company
In the last week of 2023, the Albanian parliament and telecom company One Albania became targets of cyberattacks. The exact scope and extent of the attacks are unknown. An Iran-linked hacker group called Homeland Justice claimed responsibility for the attacks through their Telegram channel. They also claimed to have hacked a second telecom company and the national airline Air Albania.[89]

Opvallende incidenten in buitenland 2024

February 2024

Dozens of Romanian hospitals offline after ransomware attack on IT platform
Dozens of Romanian hospitals were forced to revert to pen and paper after criminals carried out a ransomware attack on a widely used IT platform. Data was encrypted at some hospitals, while others were disconnected from the internet to prevent further problems.[90]

US pharmacies and healthcare payments disrupted by ransomware attack on service provider
US pharmacies were disrupted by a ransomware attack on Change Healthcare, causing problems in processing prescriptions for patients. As a result, patients could not collect medication from their pharmacy.[91] Change Healthcare processes not only medicine prescriptions but also claims for pharmacists and health insurers, resulting in healthcare providers not being paid and uncertainty about whether treatments would be covered.[92] It took weeks to restore all systems.[93] The hackers allegedly obtained personal data, including that categorised as special personal data, of a large portion of the American population.[94] Just weeks after the attack and payment of the ransom, the company was blackmailed again.

April 2024

Backdoor discovered in widely used Linux software
A severe vulnerability (CVE-2024-3094), in the form of a backdoor, was discovered in XZ Utils's software library liblzma. This is an open-source data compression application present in many Linux distributions. An attacker can gain remote access to systems through the backdoor. Given the complexity of the attack, it appears to be a deliberately created backdoor, potentially the result of years of effort. Open sources suggest that a state actor may be responsible.[95]

June 2024

British hospitals cancel operations due to ransomware attack on laboratory
Synnovis laboratory systems were encrypted, reducing the company's ability to process requests. This significantly affected the work of several hospitals.[96] British hospitals were forced to halt operations as a result of a ransomware attack on a service provider.[97]

IT system TeamViewer compromised by Russian hackers
By using an employee's login credentials, hackers managed to infiltrate the internal IT systems of the German company TeamViewer. The attack, which the company attributes to Russian state hackers, reportedly had no consequences for customers. According to TeamViewer, the attacked internal IT system is completely separate from the production environment and customer data. The hackers allegedly copied the directory data of employees, gaining access to names, business contact information and encrypted passwords.[98]

Sensitive personal information from identity and age verification service accessible online
AU10TIX, a company that provides identity and age verification for TikTok, Uber and X, among others, leaked sensitive user data. Login credentials for an AU10TIX logging platform were available online for more than a year, allowing unauthorised individuals access to sensitive personal information and copies of users' identity documents. The leaked data included names, birth dates, nationalities, identification numbers and images of passports, driving licences and identity cards. Results of verification processes were also visible.[99]

International actions against malicious actors and their infrastructure

International operations by law enforcement and investigative agencies disrupt criminal infrastructure

This reporting period saw various international operations in which investigative agencies disrupted criminal infrastructure. For example, in 2023, one of the world's largest botnets, Qakbot, was neutralised during an international police and justice action. A total of 22 servers were seized in the Netherlands, and servers in France and Germany were also taken offline.[100] In 2024, Europol and several police services disrupted the activities of hacker group LockBit with 'Operation Cronos'. The Dutch police played an important role in this operation, taking thirteen key servers offline.[101] Later that year, a coordinated, international operation by law enforcement authorities dismantled multiple botnets that played a key role in global cybercrime. During this operation, called Operation Endgame, more than 100 computer servers worldwide were taken offline and over 2,000 domain names were taken over. The police seized dozens of servers in Dutch data centres.[102] Europol coordinated 'Operation Morpheus', which successfully tackled the criminal use of the legitimate Cobalt Strike tool and led to the takedown of nearly 600 IP addresses. Various police services cooperated with private companies during this operation.[103]

Cybercriminals arrested and/or placed on sanctions list

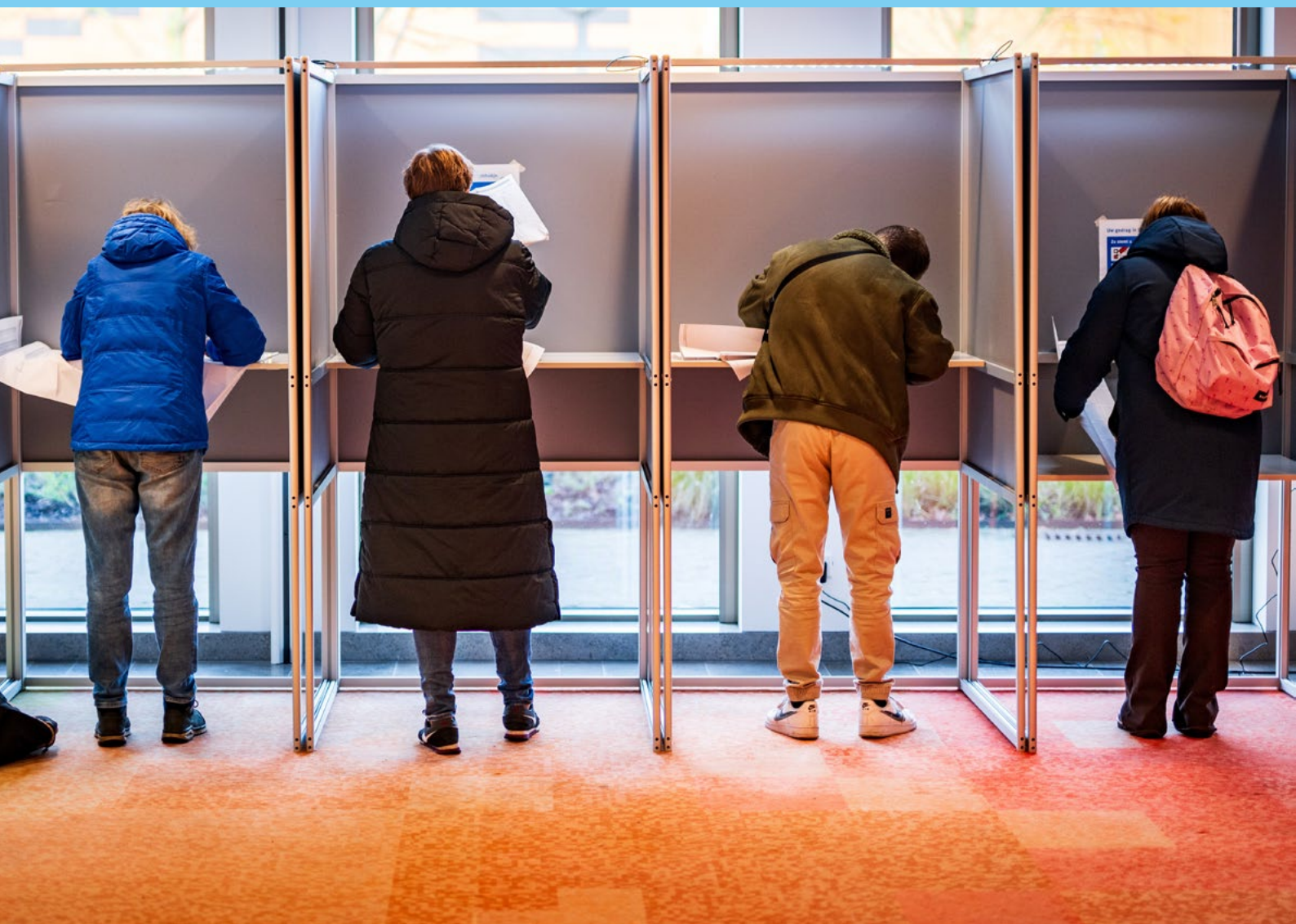
This reporting period was marked not only by disruptions to criminal infrastructure but also by arrests of cybercriminals, sometimes as part of these disruptions. In October 2023, a malware developer allegedly involved in Ragnar Locker ransomware was arrested in Paris; he was from the Czech Republic. Other suspects were questioned, and a house search took place in Ukraine.[104] An operation targeting the LockBit ransomware group disrupted criminal infrastructure and led to the arrest of two individuals in Poland and Ukraine. [105] The US and French authorities also charged five individuals. A man was arrested in connection with 'Operation Endgame' for allegedly working with the Conti and LockBit ransomware groups.[106]

For the first time – and at the initiative of the Netherlands – cybercriminals have been placed on the EU sanctions list. This includes six hackers, two of whom are considered cybercrime kingpins responsible for operations that have caused significant damage in both the EU and Ukraine. As a result of these sanctions, their European assets are frozen, and they are barred from entering the EU. European citizens and organisations are also prohibited from sending money or conducting business with these people or groups. According to the Public Prosecution Service, National Police and Ministry of Foreign Affairs, this means that parties offering digital infrastructure can no longer provide services to these cybercriminals and these companies also have a duty to investigate. This aims to prevent further misuse of digital infrastructure within the EU.[107]The United States and United Kingdom have previously placed cybercriminals on sanctions lists;[108] in 2024, for example, the United States sanctioned alleged members of the LockBit ransomware group.[109]

Russian actors misuse Dutch infrastructure; intelligence services and police intervene

The Dutch intelligence services and National Police, in cooperation with the US, disrupted an online influence campaign. Together with US and Canadian authorities, the AIVD and MIVD published the results of their joint investigation. The campaign aimed to influence US public debate; there is no indication that it was used to influence public debate in the Netherlands or Europe. Dutch digital infrastructure was misused for the campaign, with one of the servers used being located in the Netherlands. The AIVD and MIVD consider it highly likely that the Russian government was involved in developing the software used in this campaign.[110]

Digital voting is a well-known example that demonstrates that trust in digital security is necessary to want to use digital processes. In the Netherlands, we still cast our votes with a red pencil and on paper. The voting computers were abolished in 2009 because they were to vulnerable to hacking.



3 New challenges for digital security

Following developments over the past year, several new digital security challenges have been identified. State actors are intensifying their activities and broadening their capabilities, using various tools from a broader toolkit. Both state and criminal actors are seeking new ways to carry out attacks and to evade detection for as long as possible. Non-digital factors are also influencing digital security. For instance, the large-scale concentration at the three major cloud providers poses a risk to digital security. Additionally, scarce cyber capacity may jeopardise digital resilience. The development of a powerful quantum computer already poses a risk to national security. The global online data trade provides extensive access to sensitive personal data and poses a risk to national security. Trust in digital processes is crucial for users who want to use them. When that trust disappears, significant problems can arise.

State actors intensify activities and broaden capabilities

State cyberattacks are not isolated but part of a broader toolkit

As stated in CSAN 2022, cyberattacks by state actors seem to have become the new normal.[111] These cyberattacks do not stand alone; they are part of a broader toolkit that states use to pursue their interests. Cyberattacks can be carried out in combination with other means. Additionally, various cyberattacks can be carried out in conjunction with one another.

Looking solely at individual cyberattacks that directly impact Dutch interests overlooks the broader threat arising from state actors' use of a broader toolkit. It can be tempting to view different physical or digital incidents individually and conclude that the effects are relatively minor. But such a narrow focus ignores the fact that many actions are interconnected and, when combined, do indeed have an impact. Focusing narrowly solely on the consequences of an individual cyberattack is also too limited; it is beneficial to view these in conjunction when considering their effects. This also involves the relationship between a cyberattack and other deployed resources.

State actors intensify activities and broaden capabilities

Multiple state actors are intensifying their cyber activities. This is certainly true for Russia and China.[112] In 2023, compared to the first year of the war in Ukraine, there was an increase in cyber operations by Russian state actors against European and NATO alliance activities. It is likely that some of these cyber operations were carried out with the aim of gaining a foothold within critical infrastructure, to potentially sabotage it at a later date. Additionally, hackers are attempting to breach systems of the

Dutch government and other EU and NATO countries, to obtain information, including about support for Ukraine.[113]

For China, the pace of cyber operations on Western targets remains high, and Chinese intelligence services are continually ramping up activities to attack Western targets. Although Chinese state hacker groups have been conducting large-scale and persistent cyber espionage campaigns against Dutch and allied interests for some time, 2023 saw an increase in the intensity, scope and technical level of these cyber campaigns.[114] The campaign by the digital attack group 'Volt Typhoon' against US military and civilian infrastructure illustrates this further (see Annual Review). Until now, the Chinese cyber threat mainly consisted of potential espionage, but what is striking about the Volt Typhoon campaign is that Chinese hackers may have also been preparing for sabotage, not only espionage. So far, there are no known activities from this programme targeting Europe. However, Chinese capacity in this area is growing rapidly and could potentially be deployed worldwide within a relatively short time. This makes the Chinese cyber sabotage programme a potential threat to the Netherlands, among other countries, in the coming years.[115]

North Korea is also notable, particularly due to the increasing amounts of money the country is generating through cyberattacks. Although not new, North Korean cyberattacks aimed at earning money for the regime made the news. The results of recent UN research underscore that the North Korean cyber programme poses a global threat, particularly to the crypto sector. The Netherlands also has a vibrant crypto market, and North Korean cyberattacks on it cannot be ruled out. The total of 3 billion US dollars that North Korea is reported to have earned is significant, but what is particularly noteworthy is that the lion's share was obtained in 2022 and 2023, (1 billion and 600 million US dollars respectively).[116] These amounts could help finance the regime or, for example, its nuclear, cyber or other weapons programmes.

New cyber powers are also investing in cyber programmes, allowing them to intensify their activities. Some receive help from allies.[117] New or emerging state actors often belong to countries with growing power aspirations or those tangentially involved in regional or other conflicts. The AIVD and MIVD did not identify any attacks from such countries targeting the Netherlands in 2023.[118] There are also countries that purchase cyber tools on the open market. Commercial providers of advanced cyber tools are on the rise and the capabilities of their spyware are now highly sophisticated.[119] This enables countries without their own cyber programme to also start or intensify their activities.

These new or emerging state actors partly focus on countries in the region or on digital espionage and monitoring of opponents or activists.[120] The intention to target Dutch interests currently seems low. Future developments could lead to Dutch interests becoming a target. Additionally, it is important to consider the threat that new or emerging states pose to dissidents/opponents or activists residing in the Netherlands. According to a cybersecurity company, a state actor, for example, penetrated websites belonging to an ethnic minority speaking out against the current regime.[121] Although this affected Dutch digital infrastructure, it was not the primary target.

In addition to intensifying cyber activities, some countries are also broadening their capabilities: they are adding new methods to their existing arsenal or using different means. Besides using other means from the broader toolkit, the deployment or involvement of non-state actors is also part of this expansion. In 2023, 'hacktivist' collectives' carried out more of Russia's digital espionage, sabotage and influence activities. In some cases, 'traditional' Russian cyber actors use these hacktivist covers. In other cases, these are actually hacktivist groups acting as an extension of the Russian state. In relation to China, it is striking how much the Chinese offensive cyber programme is based on cooperation between businesses, universities and Chinese intelligence services. The dividing lines between organisations are unclear: individuals sometimes fulfil both a scientific role and a role in the Chinese security apparatus, while working with Chinese state or other companies.[122]

Actors seek new ways to carry out cyberattacks.

Malicious actors often choose the path of least resistance

Malicious actors still frequently opt for attack routes that offer relatively easy and quick access. Actors continue to make extensive use of phishing, particularly in its more targeted form known as spear phishing. This involves sending emails that appear trustworthy and relevant but contain an infected link or attachment. Russian hackers carried out a large-scale phishing campaign called 'DiplomaticOrbiter' in 2022, which targeted diplomats and think tanks around the world.[123] Additionally, actors can also make use of previous data breaches that may contain usernames and passwords.[124] Actors also proactively scan internet-connected systems to see if organisations are using software known to have a vulnerability (see Chapter 4). If vulnerabilities are not patched in time, this can provide access for malicious actors.

Living-off-the-Land and targeting edge devices are characteristic modus operandi in 2023

State and criminal actors are also actively seeking new ways to carry out cyberattacks and are trying to evade detection in increasingly sophisticated ways. This includes the use of Living-off-the-Land (LOTL) attacks.[125] Because LOTL attacks use legitimate tooling and applications that the victim is using, they are often not automatically blocked by antivirus programmes and other security measures. This makes it more difficult to detect attacks, which is desirable for both state and criminal actors. Moreover, LOTL

techniques leave fewer 'digital fingerprints', making it harder to prove the involvement of specific groups or countries.[126]

Various government organisations are also seeing a trend of malicious actors increasingly attacking edge devices.[127] These are systems located at the edge of a network and consist of security and other products such as firewalls, VPN servers and routers. Edge devices have long been an attractive target for malicious actors, partly because monitoring and detection on them is very complex. The MIVD describes that Chinese actors are increasingly focusing on edge devices (specifically VPN systems).[128] The NCSC states that Russian actors and criminal ransomware groups have also misused VPN systems.[129]

Compromising edge devices can have far-reaching consequences. For instance, a malicious actor can build in a backdoor to maintain access. Edge devices are often used as an entry point for the underlying network. In this way, malicious actors can gain access to sensitive or confidential information. Edge devices also often process sensitive data, including user login details. Malicious actors can use these login details to try to stay under the radar after initial compromise.

Non-digital developments influence digital security

Large-scale concentration at major cloud providers poses a risk

Increasingly more organisations are using cloud services, and this market has grown rapidly.[130] Organisations are purchasing these services on a large scale primarily from three major cloud providers: Amazon, Microsoft and Google. Even when using European or Dutch providers, there is still a chance that they too use services from these cloud providers.[131] Along with benefits, there are also risks associated with large-scale concentration of cloud services among the largest cloud providers.

Explanation of cloud services

Cloud services are IT services offered via the internet. The user does not purchase hardware and software but pays for the actual use of one or more services running on a cloud provider's infrastructure. Cloud services are often divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The boundaries between them are not always clear-cut. The largest cloud providers are active in all three layers mentioned and are thus vertically integrated.[132]

There are several reasons why organisations primarily use the three largest cloud providers. These include the wide availability of functionalities, integration possibilities of services and scalability.[133] Another reason is the knowledge among IT experts about using the services of these specific providers. In addition to these more substantive reasons, regulations and procurement procedures are also cited.[134] For instance, the largest cloud providers often make more favourable offers in tenders compared to smaller parties.[135] Once a large cloud provider has been chosen, it is also easier to purchase additional services within the existing contract than to start a new procurement procedure.[136]

Another argument mentioned for using the services of the largest cloud providers is that there are supposedly few or no European or Dutch alternatives. The largest cloud providers have a huge range of services and these can also be purchased by customers as one package. An alternative is to combine cloud services from different cloud providers. This does place additional demands on the expertise and internal management of the cloud user. In this regard, one expert compares the large cloud providers to IKEA, where you can buy many products from the same store.[137] However, if you are only looking for a houseplant, for example, there are many other shops.

There are also risks associated with large-scale concentration among those largest cloud providers. A first risk is that strategic dependencies are increased. This has implications for our digital open strategic autonomy. The Netherlands is already largely dependent for cloud services mainly on the three U.S. companies, and the dynamics in the cloud services market reinforce this (see below). One consequence is that legislation in the U.S. also applies to Dutch organizations to a greater or lesser extent.[V] Furthermore, under changed geopolitical circumstances, a strategic dependency can have major consequences. Moreover, for the Netherlands, there are limitations to the oversight that can be exercised over these companies. For example, the headquarters of these companies in the EU are in other countries and supervision of those companies takes place in those countries. A Dutch supervisor must then liaise with the supervisor in the other country to be able to supervise these parties.[138]

A second risk is that this creates a single point of failure. An outage or cyberattack can have global repercussions. The three largest providers form a very attractive target for cyber actors due to the concentration of cloud services and underlying data. An attack on a cloud service provider has therefore been assessed as likely in the Government-wide Risk Analysis and, moreover, as serious.[139] The US Cyber Safety Review Board has raised questions about the security of at least one of these providers. It found that this provider has a corporate culture in which sound risk management and investments in security are systematically not prioritised.[140] For years, there have been numerous examples of misconfiguration of cloud

V This is far from limited to the so-called "US cloud act" that allows the government to demand access to information - under legal safeguards. The US government can also, for example in the event of a large-scale outage or attack, demand priority for restoration of services in the US. Sanctions legislation can also have knock-on effects.

services resulting in cyber incidents.[141] Much of the security is left to customers who often do not have the necessary knowledge or are unaware of the options. Security options must be continuously enabled and maintained, alternatively are available only as a separate service. The technical complexity of configuring and securing cloud services exceeds the capacity of most organisations, even mature ones.[142]

A third risk is the dominant position of the large cloud providers, which is reinforced from both the supply and demand sides in the cloud market. On the supply side, the three largest cloud providers seem to be focusing on building their own ecosystem, which organisations find difficult to leave after the initial choice. In the cloud market, competition is mainly about attracting new customers. After that initial moment of choice, there are limitations to switching to another provider. Those switching restrictions are technical, organizational/procedural and financial in nature. Moreover, due to the dominant position, those companies potentially lack the incentives to keep innovating and to ask real prices from customers.[143] Because organizations on the demand side tend to choose the three largest providers, this also increases their dominant position. As a result, alternative providers have less and less opportunity to survive.[144]

Large-scale effects due to digital monocultures

The worldwide computer outage caused by cybersecurity company CrowdStrike in July 2024 (see Annual Review) served as a wake-up call for the potential consequences of a digital monoculture. It affected at least 8.5 million computers, corresponding to 1% of the global Windows users.[145] The EFF states that incidents like the CrowdStrike outage have become inevitable due to these monocultures.[146] Other markets for digital services, hardware and software are also dominated by only a few companies. These monocultures create single points of failure, as previously argued for the three largest cloud providers.

Resilience at risk due to scarce cybersecurity capacity

The shortage of cybersecurity experts may undermine the digital resilience of the Netherlands. According to the Employee Insurance Agency (UWV), no other professional field has such a severe shortage as the ICT sector, with demand for software developers and security specialists, in particular, having increased over the past five years.[147] The shortage of digital professionals is moreover a cross-sector problem; they are needed in all sectors to enable the digital transition.[148]

Additionally, the demand for cybersecurity professionals is expected to increase as a result of future laws and regulations. The continued development and use of AI will also create new challenges and require new competencies, resulting in an increasing demand for cybersecurity professionals.[149]

It is not only the increased demand that has led to scarcity; the supply is also not keeping pace. Research shows that much of the demand for cybersecurity professionals is for mid-level and senior positions. This often requires upskilling or retraining, which means organisations need to retain their existing cybersecurity professionals and attract new ones. However, these efforts are currently falling short.[150]

The combination of advancing digitalisation, increasing demand and future laws and regulations that must be complied with and monitored makes it likely that shortages will continue to increase in the coming years. Partly due to competition in the labour market, it is also complex for the government to attract and retain skilled workers with expertise. This may ultimately impact the digital resilience of the Netherlands, especially as government organisations play a crucial role in areas such as digital resilience and combating cybercrime. Additionally, it may become interesting for malicious actors to investigate which organisations have the largest shortages – and potentially the weakest defence.[151]

Future powerful quantum computer already poses a risk to national security

The development of a powerful quantum computer presents opportunities but also leads to risks for national security. A quantum computer with sufficient computing power can weaken or break commonly used encryption methods. Cryptography plays a key role in ensuring the availability, integrity and confidentiality of digital processes and data. Examples include controlling traffic lights and bridges, communication in the form of email or app messages, and protecting identity data.[152] Additionally, cryptography is used to encrypt confidential, trade secret and state secret information.

Cryptography forms an essential part of large portions of the Dutch cyberspace. The use of cryptography protects the continuity of critical infrastructure, economic security and social security. As such, cryptography is essential for safeguarding the national security of the Netherlands, both now and in the future.

The development of a powerful quantum computer has accelerated in recent years.[153] Although it is unlikely that existing quantum computers can effectively break current cryptography, the potential risks resulting from the arrival of a powerful quantum computer must already be taken into account. Encrypted data that is intercepted and stored now can be decrypted at a later time.[154] This is also known as ‘store now, decrypt later’, and according to the AIVD and NCSC, it currently poses the most urgent threat to organisations in relation to the arrival of a powerful quantum computer. Organisations must take this threat

into account if they have data that needs to remain confidential for an extended period. [155]

Future resilience dependent on current preparation

The migration to quantum-safe cryptography faces complex challenges that will require much time, planning and preparation. Organisations that start preparations too late to migrate to quantum-safe cryptography risk not being resilient in time against the threat of the quantum computer.

Large-scale trade in sensitive personal data poses a threat to national security

Data companies trade globally in sensitive personal data

Various data companies trade globally in sensitive personal data of citizens and employees of organisations ('data trade'). Much of this trade is linked to the business model behind many websites and apps, namely earning or recovering money by offering advertisements. However, users of paid digital devices, software or digital services also exchange personal data with providers. Some providers do this, in turn, with sometimes dozens or hundreds of partners who may also do it with partners.[156]

Data companies use advanced advertising technology, also known as real-time bidding (RTB). A key aspect of RTB is that websites and apps provide automated advertising space. Advertisers can, in turn, purchase advertisements for very specific user profiles. Various platforms and parties are involved in matching the supply and demand for advertising space and they exchange sensitive personal data for this purpose. This includes current location data, biometric, financial and/or psychological and medical data. Some companies process the obtained data with other data, create user profiles and sell them.[157] That data can also be used for training generative AI models: it is unclear what happens to that data and whether it can show up somewhere in any way. State actors can also be part of data trade through front companies and collect and process personal data in this way.[158]

Data trade also uses techniques other than the aforementioned RTB. A well-known example is how Facebook collects data about the online activities of internet users. A study by a US consumer organisation showed that, on average, 2,230 companies sent data about the study participants to Facebook.[159] Another example is data collection by Google. According to the Dutch Foundation for Large-Scale Damage & Consumers (Stichting Massaschade & Consument), Google collects all kinds of user data via Android, violating Dutch and European rules. The Foundation contends that an enormous amount of information about smartphone use is channelled to Google servers, even if the most privacy-friendly settings are enabled. A study would not only show that Google collects much more data than is allowed, but that it also links this data to individual users.[160] Smart devices and modern cars also collect a lot of personal data and share it with manufacturers, who in turn can share it with other parties. In a parliamentary letter of January 2024, the previous Minister of Infrastructure and Water Management stated that vehicle data should be under the control of motorists and only shared with third parties after obtaining the motorist's consent.[VI] The letter also pointed out the risks of espionage by manufacturers from countries with an offensive cyber strategy against the Netherlands.[161]

Large scale and precision of data trade can harm security interests

The large scale and precision of data trade and the way online advertising markets function can harm national security in various ways. The first is the large-scale breach of confidentiality of sensitive personal data. For years, 'unauthorised access to information (and/or its publication)' has been identified as a risk to national security for good reason. Although there is a legal distinction, there is effectively no difference between illegal breach of confidentiality as a result of a cyberattack or a breach through the aforementioned forms of data trade.[VII] A second way in which national security could be affected is misuse of the aggregated datasets and/or detailed personal profiles. These are not only valuable for data traders themselves, but also for numerous malicious actors, including state actors, criminals or extremists, and activists. The precision of these profiles exposes groups or individuals to an increased risk of digital espionage or online or physical intimidation, which can harm national security. This can include politicians or other people in sensitive government or non-government positions, but also threatened individuals or members of diaspora communities from authoritarian regimes.[162] In a letter to the House of Representatives, the Rutte IV government stated that it was 'fully aware' of the risks that the online advertising industry poses to the public's privacy and national security.[163] A US presidential decree from February 2024 also shows awareness of the risks of online data trade.[164] It primarily focuses on protecting American government personnel (in sensitive positions) and processes. In doing so, it attempts to prevent this data from inadvertently falling into the hands of state actors such as Russia, Iran and North Korea.[165]

VI As from September 2025, the Data Act no longer allows the data holder to share (or trade in) data from smart devices with third parties unless this is part of the agreement with the user.

VII It is beyond the scope of this CSAN to judge the degree of illegality or legality of this exchange and trade. The cited claim for large-scale damage illustrates that certain practices may be against the law. Experts in various articles also argue that certain practices do not comply with the law.

Criminals also collect, enrich and sell data

Criminals also gather personal data and then enrich and sell it to other criminals. By combining various details such as residential addresses, telephone numbers, bank accounts, passport information, and number plates, valuable victim profiles are compiled, ready for use in various forms of crime.[166] Criminals can use these data and/or profiles to expose police officers, threatened individuals and others in sensitive positions to online and/or physical intimidation.

Notifying victim and targets is complex due to legal barriers

The police increasingly encounter ever-growing datasets with victim information in criminal investigations. By notifying victims, they are enabled to take mitigating actions, such as installing updates or patches. As a result, victims are no longer part of a botnet used to carry out attacks on targets in the Netherlands, for example. Because many of the victims in a dataset are regularly located outside Europe, these victims cannot be notified due to legal barriers. These legal impossibilities stem in part from the importance of protecting privacy.

Until now, it has only been possible to effectively notify victims and targets on an ad hoc basis. However, notifying actual or potential victims generally involves practical and legal problems. Yet large-scale victim and target notification is essential to permanently take down criminal digital infrastructure (on a much larger scale than has been possible so far) and to prevent ongoing victimisation. Sharing data internationally to notify victims could directly help reduce the digital threat to the national security of the Netherlands and other countries.[167]

Digital security is a prerequisite for trust in digital processes

The fact that digital security is essential in our highly digitalised society has often been mentioned in the various editions of the CSAN in recent years. The focus was mainly on the necessity of digital security to be able to use digital processes. This is to prevent social disruption and to recover as quickly as possible if it occurs. Much less emphasis was placed on digital security as a prerequisite for trust in digital processes.[VIII]

Trust is necessary to want to use digital processes

Trust is necessary to want to use digital processes It is only with trust that organisations or individuals ('users')[IX] can deal with the many uncertainties and complexities associated with their use. Without trust, they would be overwhelmed by the thought of everything that could possibly go wrong.[168]

Trust requires more than just digital security. A web shop can be as secure as possible, but if criminals run it and do not deliver the product that has been paid for, it obviously undermines trust in the web shop. Digital security is therefore not the only prerequisite for trust, but a necessary one. Digital voting is a well-known example that shows that trust in digital security is necessary. In the Netherlands, we still cast our vote with the red pencil and on paper. Voting computers were abolished in 2009 because they were too vulnerable to hacking.[169]

Despite cyber incidents, digital processes are still widely used

Cyber incidents demonstrate that guarantees for digital security do not exist. Nevertheless, users make extensive use of digital processes. One possible reason for this is that it is based on the functionalities and ease of use of processes. Users focus much less on harmful effects. Another reason is that use occurs within a social context: if everyone uses these processes, then it must be fine. Users also expect that legislation, regulations and supervision form a safety net.[170] A reason might also be that there are hardly any analogue alternatives left or there is no freedom of choice. The barriers to not using certain processes are therefore too high.

Possible concerns and suspicion

The fact that users make extensive use of digital processes does not necessarily mean that they have complete trust in their security. They might have concerns and suspicion about the safety of specific processes or even digital processes in general.

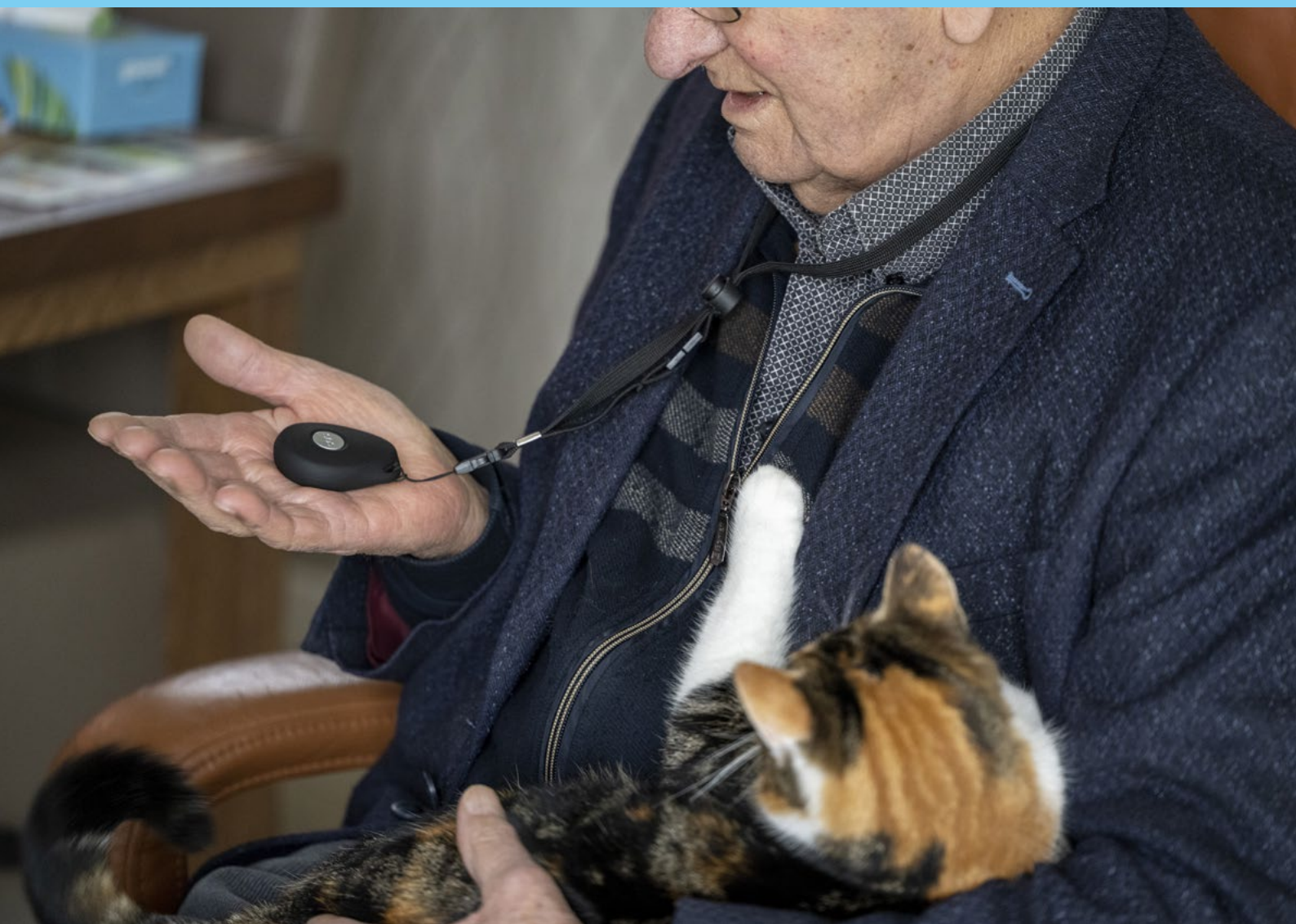
As argued above, the disappearance of trust can lead to users no longer wanting to use digital processes. Imagine if one million citizens no longer wanted to file their tax returns digitally because they no longer trust the security of the Tax Administration's processes. If that many citizens wanted to file analogue returns by post again, it would have major consequences for tax collection.

VIII Preference is given to relying on digital processes rather than their providers. First, unless explicitly stated otherwise, these are digital processes in general and not the specific processes of a specific provider. Many 'providers' are moreover involved in practice. Consider online banking, where many 'providers' play a direct or indirect role, including our own bank, the 'other party's' bank, providers, web hosts, cloud suppliers and organisations such as iDeal or Google Pay or Apple Pay.

IX Several perspectives can be chosen for *trust* in digital security, including that of buyer or provider. Unless stated otherwise, the user's perspective has been chosen, partly because both customers and providers make use of various digital processes, and providers in turn are also customers of many processes.

It is difficult to pinpoint exactly what trust is based on and what is needed to maintain it. What is clear, however, is that trust in digital security is one of the building blocks for wanting to use, and continue to use, digital processes. Maintaining and/or strengthening trust is therefore important to harness the opportunities of digitalisation.

Elderly people living at home use a portable alarm button to alert care workers in case of emergency. In November 2023, more than 3,000 alarm buttons did not work due tot a ransomware attack on the service provided. The criminals also had access to data.



4 Structural challenges for digital security

Various factors have long posed a challenge to digital security. State and criminal actors have been responsible for the lion's share of attacks for years. These attacks can affect national security. Additionally, developments that at first glance seem unrelated to cybersecurity can still have a lasting influence on the threat and resilience. This certainly applies to geopolitical and technological developments. As any organisation can be affected by a cyber incident, digital risks therefore require a more comprehensive approach to risk management. Although the security of digital processes is essential in our digitalised society, the importance of that security sometimes competes with other interests. However, the importance of digital security is becoming increasingly anchored in laws and regulations.

Geopolitical and technological developments influence threats

The digital threat is complex and influenced by many non-digital developments. Consider geopolitical tensions, which can lead to state actors deploying cyber capabilities to promote their interests. Geopolitical tensions, conflicts and socially controversial topics can also give rise to hacktivism. This has been visible, for example, since the start of the war against Ukraine. Technological developments, such as generative AI, can also influence digital security (see box).

Generative AI influences digital security

The use and possibilities of generative AI are still developing fully, and the impact on society remains unclear in many aspects. There are at least four relevant perspectives. Developments within and use of generative AI have so far fallen under:

1. The algorithms and the data with which the algorithms are fed can be deliberately manipulated. This can be done, for example, through cyberattacks.
2. Users can, often unintentionally and unknowingly, provide access to search queries and/or sensitive information through the questions they ask, the information they enter or the information with which they feed the applications.
3. Generative AI can be used for cyberattacks. For instance, AI can be used to create more recipient-tailored phishing emails. Malicious actors can also use generative AI to quickly and automatically detect interesting targets and gather information about them. Malware can also be developed with a lower threshold.
4. Generative AI can be used to defend against cyberattacks, for example, by detecting irregularities in data.

State and criminal actors account for the lion's share of cyberattacks

For a long time, state and criminal actors have been responsible for the majority of cyberattacks. It is important to note that there may be a certain amount of mixing between them. State actors can hire, permit or pressure cybercriminals to carry out cyberattacks on desired targets. Additionally, state actors can pose as criminal organisations. As a result, the dividing line between financially motivated cybercriminals and state actors is vague and difficult to distinguish.

Besides state and criminal actors, hacktivists, insiders, script kiddies and, to a lesser extent, terrorists, can carry out cyberattacks.

State actors have offensive cyber programmes against the Netherlands

State actors use the cyberspace to achieve their political, military and/or economic goals. The digital threat posed by state actors to Dutch society is varied.

The Netherlands is the target of offensive cyber programmes from countries such as China, Russia, North Korea and Iran, which carry out cyberattacks against a wide range of potential targets. Offensive cyber programmes therefore threaten Dutch national security.

Cyberattacks are relatively inexpensive, scalable and difficult to attribute, with a high, often long-lasting yield. A successful breach can sometimes continue to provide information invisibly, covertly and with impunity for years. This can be information for espionage purposes, but it can also be information about systems and networks, for example. That information can then be used to carry out sabotage or preparatory acts for sabotage.

During the reporting period, various cyber operations by state actors against the Netherlands came to light (see Annual Review). Chapter 3 provides more detail and new insights into the threat posed by state actors.

Cybercriminals can affect national security

Cybercriminals remain capable of causing extensive damage to digital processes. They act from financial motives and do not intend to disrupt society. Nevertheless, their attacks can cause so much impact that they affect national security interests. The capacity of some cybercriminal groups is equally as high as that of state actors.

The use of ransomware poses a risk to national security when it comes to the continuity of vital processes, the leaking and/or publishing of confidential or sensitive information and impairing the integrity of the cyberspace. National security is at risk when the target of such an attack is part of the critical infrastructure (including the national government and all designated vital processes) and the attack disrupts the continuity of vital processes. Additionally, as vital organisations exist in an ecosystem with non-vital organisations, an attack on a non-vital organisation can be a stepping stone to or affect vital organisations.

In the past, some criminal groups stated that they did not target critical infrastructure. Indeed, this would be unwise as it would put them in the spotlight of intelligence and investigative agencies. On the other hand, there could be a tendency in vital sectors to pay ransoms quicker due to the importance of business continuity, making it an attractive target for criminals after all. Experts consulted by the NCTV state that criminals are opportunistic. While this means that deliberately attacking critical infrastructure is not a regular occurrence, it also means that criminals do not have an ethical standard regarding not attacking critical infrastructure.

For cybercriminals, extortion remains an attractive business model. Criminals do this, among other things, by encrypting files or systems and demanding ransom in exchange for decryption. Criminals can also threaten to publish stolen information (see Annual Review). Stolen information is sometimes enriched with other data and sold – even when victims have paid the criminals to prevent publication.

Cybercriminals are part of and depend on a broader digital ecosystem that includes both malicious and legitimate elements. This ecosystem forms an opportunity structure for them. Due to specialisation among cybercriminals, they depend on each other's online and other services in the context of Cybercrime-as-a-Service. Other actors, for example state actors, sometimes use this as well. This dependence also applies to the purchase of legal services, such as web hosting and communication services like VPN or domain registrations. Reseller arrangements reinforce the hosting problem, with resellers renting out hosting packages. This can lead to uncertainty about the identity of the person responsible for hosting – particularly illegal – data and the person who can or must comply with a judicial order.

Depending on legal services, however, also offers opportunities for increasing digital resilience. When it comes to internet services in the broad sense, principles such as acceptable use, know your customer, the duty of care principle and anti-abuse provisions are often still voluntary. As a result, these principles cannot be legally enforced, which creates room for non-compliance. This offers cybercriminals many opportunities to work anonymously and at scale. Opportunities they do not let pass by.

The risks for criminals of being caught or convicted are relatively low. Geopolitics also plays a role in this. When relations with other countries deteriorate, or worsen further, investigation and prosecution become increasingly complex. For example, criminals can move freely in certain countries or are not extradited. Investigation is also hampered by legal bottlenecks in sharing data between the various relevant parties. Even so, various coordinated actions by enforcement and investigative agencies show that it is in fact possible to disrupt criminal groups and their attacks (see Annual Review).

Any organisation can be a target for malicious actors

All digital processes are potentially vulnerable

All digital processes, organisations, and sectors are potentially vulnerable to cyberattacks and can be affected in various ways. First, an organisation can be a deliberately chosen and direct target for malicious actors, for example, because it processes a lot of personal data. Second, an organisation within the ecosystem can be attacked as a stepping stone to other, more interesting targets. Third, organisations can become victims 'by chance'. For instance, malicious actors actively search for systems that contain vulnerabilities that can be exploited. If an organisation uses such a system, it can be attacked without malicious actors concerning themselves with the question of what kind of organisation it is.

Whether it concerns countries, sectors or organisations, few can function independently of a broader ecosystem. Digital processes, systems and networks are strongly intertwined within the ecosystem. The result is a large and growing attack surface for malicious actors and a greater chance of outages. Attack surface refers to the ways in which a malicious actor can attack digital processes. In digital processes, vulnerabilities – organisational or human – are repeatedly found that can be exploited. The probability of large-scale outages also increases due to complexity and interconnectedness. Outdated (legacy) systems also increase the risk of outages. Legacy systems are often in use within OT, for example.

There are nodes within the ecosystem where much information or digital processes are concentrated. Although this may be explicable and justified from a business perspective, these choices are accompanied by security risks. After all, concentrated information or processes are attractive targets for malicious actors. State actors collect personal data on a large scale, with the collection primarily aimed at monitoring and identifying relevant individuals and population groups. Personal data is also very attractive to cybercriminals. They can use this, for example, for (spear) phishing attacks or to enrich and trade information. Databases or sectors that process large amounts of personal data are therefore particularly attractive. Examples include cloud service providers (see Chapter 3), or the travel and aviation sector where large amounts of personal data are processed. The healthcare and telecom sectors are also interesting targets for malicious actors because of the information processed there.

Attackers seek the weakest link within supply chains

Supply chains within the ecosystem are an attractive target. Attackers look for less resilient organisations within chains. They can then affect the rest of the chain, or a specific organisation within the chain, through that organisation. After all, a chain is only as strong as its weakest link. An attack on the supply chain causes problems not only for the compromised company but also for other organisations in the chain. This also occurred in the past reporting period. For instance, 3CX software was infected with malware, potentially compromising the networks of thousands of companies (see Annual Review).

Operational Technology of great importance, and in the sights of malicious actors

Operational Technology (OT) plays a central role in controlling, monitoring and managing physical processes within vital and other organisations. Examples include access systems or building

automation systems. OT functions as the engine of vital processes. Due to the important role of OT, large-scale outages and cyberattacks against OT systems can have major consequences for society. In addition to reputational or financial damage, this can also cause damage to industrial equipment and the immediate environment. In extreme cases, casualties may occur. The digital security of OT is therefore crucial.

OT is becoming increasingly intertwined with information technology (IT). While this has many advantages, it also means that the attack surface is enlarged, meaning OT systems could become compromised. It has been shown that cyber actors are interested in compromising OT. For example, there are types of malware that can be used to sabotage OT systems. Criminal actors are increasingly targeting industrial environments as a business model. Since the end of 2023, Microsoft has observed an increase in the number of reports of attacks aimed at poorly secured OT devices exposed to the internet (see Annual Review). Further and possibly more targeted disruption of OT systems cannot be ruled out in this context.

The Netherlands is an attractive target for attackers

With its high-quality knowledge economy and as a frontrunner in certain technologies, the Netherlands is an attractive target for malicious actors and they may steal, or attempt to steal, knowledge about it. In addition, the Netherlands hosts various international organisations that process information that could be of interest to malicious actors. For example, in October 2023, the International Criminal Court (ICC) in The Hague fell victim to a cyberattack (see Annual Review).

Due to the internet infrastructure in the Netherlands, it can also be attractive for malicious actors to carry out cyberattacks from the Netherlands against citizens, organisations or governments in other countries. The infrastructure is fast, cheap and reliable, making it attractive for misuse.

Security of digital processes is and remains essential in a highly digitalised society

The security of digital processes is and remains essential in our highly digitalised society and is thus inextricably linked to national security. Hardly any processes are left without a digital component.

When digital processes do not function properly, the operation of organisations is affected. Chain effects can impact sectors or even the entire society, as illustrated by the faulty software update from CrowdStrike and the software error on a Defence network. Cyber incidents can also have physical consequences. For instance, power outages can occur, education can come to a standstill or patient care can be hindered.

Digital risks require a comprehensive approach to risk management

Digital risks have several special characteristics. They relate to an extremely complex system, namely the cyberspace. As there is no comprehensive overview of what the impact could be of a large-scale, multi-day disruption of digital processes in the Netherlands, this also makes it complex to identify and assess potential risks. This is partly due to the broader digital ecosystem in which organisations operate. While information about cyber incidents is partly available, it is certainly not complete and not always accessible to relevant parties. For the management of aircraft accidents or floods, for example, much more information is available and over a longer period. Simulating incidents or building models to map the course of incidents and consequences is helpful for risk management. For digital risks, this is extremely complex.

These special characteristics of digital risks require a comprehensive approach to risk management. One way, for example, is not only to look at incidents that have already occurred, and not merely to comply with legal requirements. It also still holds true that basic measures help and that a portion of cyber incidents can be prevented with them. Lastly, it is useful to assume that there is already a malicious actor in your network (assume breach) when setting up and managing a network.

Five basic principles for digital resilience provide guidance

Many digital incidents are caused by not having basic security measures in place. Examples include weak passwords or failing to install patches. This is unfortunate, because often the organisation can be made much more digitally resilient with relatively simple steps. But organisations also differ, which means there is no one-size-fits-all set of measures. A self-employed person has different information needs than an organisation in the vital sector. With the five basic principles for digital resilience, the NCSC and DTC provide guidelines for getting the basics in order (see Appendix 3 of this CSAN for this purpose).

Importance of digital security competes with other interests

As digital security is not the only interest that needs to be protected, it competes with other interests. While such conflicts of interest can occur within one organisation, the interests of organisations compete with interests at the national level. An example of this is the large-scale concentration at the three largest global cloud providers. Decisions affecting digital security are not based solely on security considerations; they also involve political, economic, legal and other factors.

Legislation consolidates, implementation underway

Upcoming additional digital security requirements are poised to enhance digital resilience in the coming years. These stem from new EU laws and regulations, the Dutch Cybersecurity Strategy 2022–2028 and its associated action plan. Through this development, the importance of digital security continues to be anchored in legislation. These laws and regulations are in various stages of implementation. Several laws, including their current stage, are described in the box below. A selection has been made here, focusing on legislation that is cross-sectoral. Laws and regulations focusing on specific sectors are therefore not included.

Implementation takes time

The implementation of various laws and regulations is underway. Some legislation, such as the DMA, has already been implemented and supervision has been arranged. This is not yet the case for other legislation, such as the DSA and Cbw/NIS2.

Fleshing out and raising awareness of legislation inevitably takes time. Legislation does not lead to immediate changes in digital resilience or impact digital risks. This not only relates to the design of legislation but also to awareness and preparation among companies, implementation organisations and supervisory authorities.

New digital security legislation at various stages[171]

- **Digital Services Act (DSA):** regulates the responsibility and liability of internet providers, hosting companies, online platforms, search engines and marketplaces. As a result of the DSA, services must better protect users' rights, tackle online deception and illegal information, and improve transparency. The legislation has applied to the 19 largest platforms since August 2023. From February 2024, it will also apply to other digital services. EU Member States are responsible for supervising other digital services. In the Netherlands, the supervisory authorities have not yet been legally established, limiting their ability to take action under the DSA.[172]
- **Digital Markets Act (DMA):** provides additional market and merger supervision and competition rules for the world's largest online platforms. These platforms have had to comply with the DMA since March 2024. The Netherlands Authority for Consumers & Markets is the national supervisory authority for the DMA. It can collect possible violations in the Netherlands and investigate them with the European Commission.[173]
- **Cyber Resilience Act (CRA):** aims to create a safer European digital internal market and a society where unsafe products can be barred and removed from the market. It is expected that digital products – including software, hardware and components – will have to comply with extensive cybersecurity requirements and standards as from 2027.[174]
- **Network and Information Security Directive (NIS2):** regulates which entities must comply with which mandatory security requirements. As a result of the NIS2 directive, many more organisations in the Netherlands will face legal obligations, supervision and support for their digital resilience. This applies to governments, vital organisations and other organisations operating in sectors of social and/or economic importance.[175] A principle in NIS2 is that it explicitly holds the directors of these organisations responsible for cyber policy. Sanctions may follow if this policy is not in order. The intended implementation in October 2024 has been postponed in the Netherlands and is expected in 2025. The Cybersecurity Act (Cbw) is the legislative bill to transpose NIS2 into national law.
- **The Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union** (EUIBAs) was adopted in 2023 and entered into force on 7 January 2024. This regulation is related to the NIS2. While NIS2 is a directive that Member States must transposed into their national law, the regulation aims to ensure the level of cybersecurity at EU institutions, bodies, and agencies.[176]
- **Cyber Solidarity Act (CSOA):** aims to strengthen capabilities in the EU to detect, prepare for and respond to significant and large-scale cybersecurity threats and attacks. The intended entry into force is at the end of 2024.[177]

Strategic themes still apply, with some additional challenges for risk management

The CSAN 2022 introduced six strategic themes (see box below) that formed a building block for the Dutch Cybersecurity Strategy 2022–2028. These strategic themes are still applicable and each complicate risk management individually and in combination.

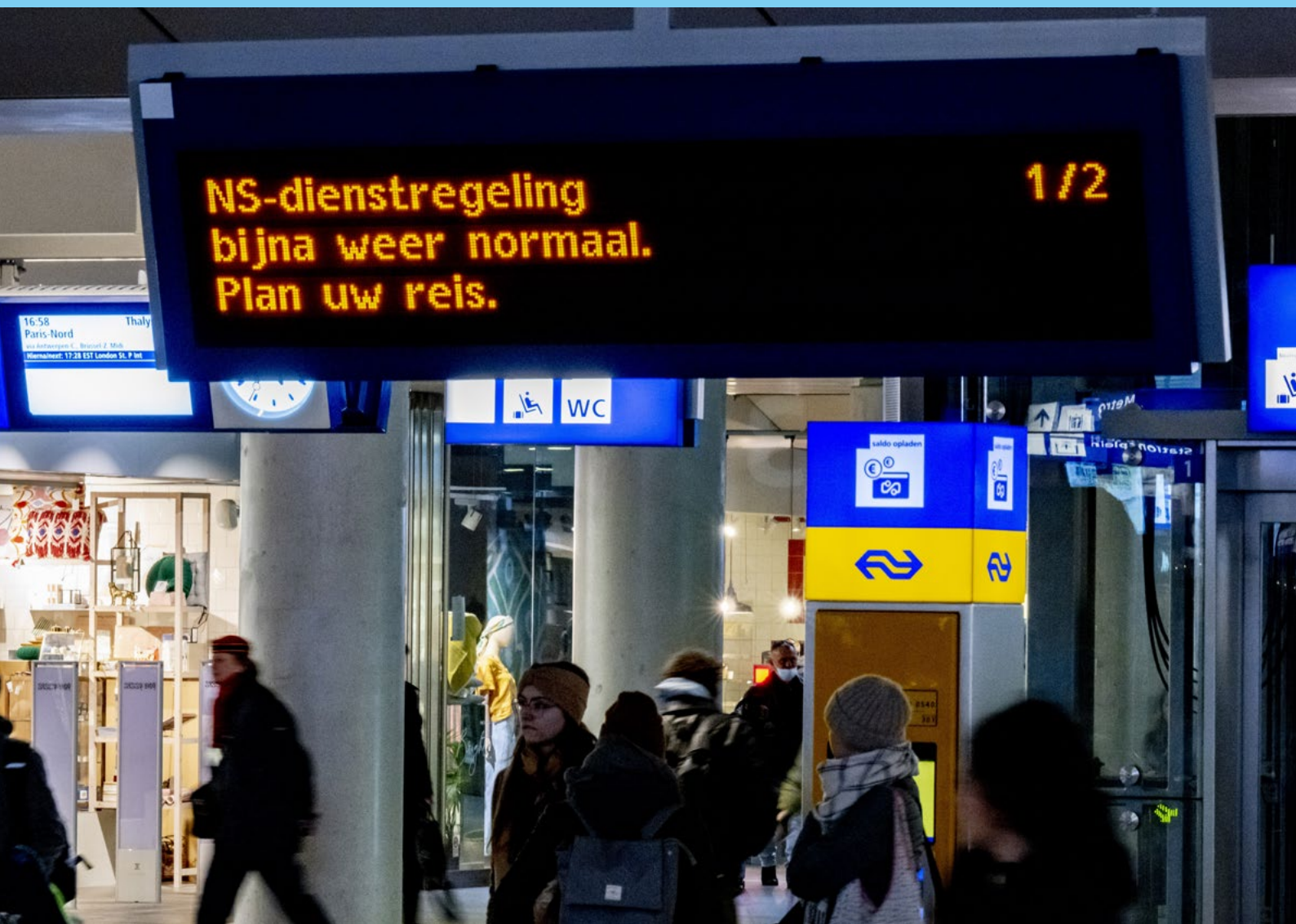
Strategic themes mentioned in the CSAN 2022 and addressed in the Dutch Cybersecurity Strategy 2022–2028

- Risks form the downside of digitized society.
- Cyberspace is a playing field for regional and global dominance.
- Cybercrime is scaleable, while resilience – for now – is not.
- Market dynamics complicate controlling digital risks.
- Coordinated and integrated risk management is still in its infancy.
- Restrictions in digital autonomy also restrict digital resilience

Many of the findings in this CSAN align with one or more of the mentioned themes and add depth to them. This applies in particular to:

1. The observation that states are intensifying their activities and broadening their capabilities, and that state cyberattacks are not isolated but part of a wider toolbox;
2. Actors seek new ways to carry out cyberattacks;
3. The large-scale concentration at the the three largest cloud providers;
4. The global online data trade;
5. The need for users' trust in digital processes for them to want to use, and continue using, digital processes.

The digitisation of the railway makes public transport more efficient and safe, but also more vulnerable to cyber attacks or outages.



Appendix

1 Explanatory notes

Explanation of the preparation method

The National Coordinator for Security and Counterterrorism (NCTV) prepares the Cybersecurity Assessment Netherlands (CSAN), cooperating with the National Cybersecurity Centre (NCSC) for this purpose. The NCTV adopts the CSAN each year. The information, insights and expertise of government services, organisations in vital processes, academia and other parties are gratefully used for this purpose.

The CSAN is prepared in three phases:

1 Analysis
The NCTV collects and analyses relevant information about incidents, trends and shifts in the triangle of interest, threat and resilience. The following questions underlie the CSAN:

1. Which relevant incidents occurred in the Netherlands or in comparable countries from March 2023 to June 2024, and what new insights do they provide?
2. Which broader political, economic, social and technological developments and factors are expected to influence digital security in the coming years? Which developments could be game changers?
3. Which changes can be identified in digital threats that affect national security? Consider the nature and extent of the threat, targets, actors, vulnerabilities, forms of outage and actor methods.
4. Which changes can be identified that affect interests that could be compromised when cyber incidents occur? And what could be the impact?
5. Which changes can be identified in the extent to which the Netherlands is resilient against these digital threats?
6. To what extent are changes occurring in the greatest risks to the national security of the Netherlands?
7. What events, developments or insights influence the strategic themes as identified in CSAN 2022 and what influence do they exert?

NCTV analysts made an initial inventory of the 'ingredients' for the CSAN based on these questions. These were then discussed in three sessions with experts from public organisations. Two interviews were held with professors, specifically on the topic of trust.

2 Writing and peer review
After completing the analysis phase, individual authors wrote draft chapters. Colleagues from the NCTV, NCSC, AIVD and MIVD have since reviewed the Annual Review.

3 Validation
The CSAN undergoes an extensive validation process, in which the draft text is submitted for comment to external partners. After processing all the comments, the NCTV prepares and adopts the final text. After the CSAN is published, there is a primary internal evaluation. The collected feedback is then incorporated into the CSAN process for the following year.

2 Methodological explanation of ransomware attack figures

Generating an overall picture of ransomware attacks is complex

Ransomware attacks remain a pervasive and persistent phenomenon both globally and in the Netherlands, causing significant financial damage due to necessary recovery work and business interruption. These attacks often also compromise the confidentiality of personal and/or company-sensitive information, leading to additional damage. Despite the impact and numerous reports on these attacks, an overall picture of the number of ransomware attacks is lacking.

As research commissioned by the Research and Documentation Centre (WODC) indicates, generating an overall picture is far from straightforward. According to the researchers, existing data sources fail to offer a clear picture of ransomware attacks on Dutch companies and institutions for the years studied: 2020, 2021 and 2022. Many data sources are too generic, making it impossible to extract specific information for the Netherlands, or they do not cover the entire period. Additionally, commercial interests play a role for some parties, or the information they make publicly available is very limited. The researchers moreover conclude that no studied data source is free from limitations.

- A first limitation is the availability of relevant data.
- A second limitation, applicable to most data sources, is that they do not specifically focus on Dutch companies and institutions. The focus of many data sources is on North America or is global. The only data sources specifically focusing on the Netherlands are police reports, data breach notifications to the Dutch DPA and the results of the CBS Cybersecurity Monitor.
- A third limitation is that no single data source is complete.
- Finally, the quality of the data in some cases is insufficient for identifying and analysing ransomware attacks on Dutch companies and institutions.[178]

Generating an overall picture of cyber incidents is even more complex

The reasons outlined for the complexity of obtaining an overall picture of ransomware attacks apply equally to an overall picture of cyber incidents. It is actually far more complex to get an overall picture of cyber incidents. One reason is the issue of definition. While it is already challenging to choose a definition for ransomware attacks, this applies even more so to cyber incidents. Is receiving a phishing email considered a cyber incident, or must it have led, for example, to malware being placed on the recipient's device? Does marketplace fraud using identity data from a hack qualify as a cyber incident? Is sending a sensitive email, for instance from a psychiatric institution, with all addressees in the 'To' field (instead of the BCC field) a cyber incident? Another reason, which also applies to ransomware attacks, is that the Netherlands cannot be unambiguously delineated in the cyberspace. Consider Dutch branches abroad, foreign branches in the Netherlands with or without headquarters in another European country, Dutch companies processing data from around the world, foreign companies using Dutch infrastructure, companies in other countries processing data of Dutch citizens or organizations, and so on.

Explanation of figures in Annual Review from Melissa partnership project

The Annual Review compiles information on ransomware incidents at larger organisations (from about 100 FTEs). It is based on incident information from Computest, DataExpert, Deloitte, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, the NCSC and police report figures. In relation to companies, these are firms that conduct incident response for ransomware attacks. Incidents are assessed by security experts who apply a strict definition of ransomware. As a result, this annual review may differ from others where surveys were conducted among the general

public and/or smaller organisations. Because the data is anonymised, perfect deduplication is not possible. Reference is therefore made to an estimate of unique incidents.[179] It should be noted that because the initial ransomware attack is taken as the basis, an attack on a service provider with dozens of customers who also fall victim to the same attack thus counts as one attack.[180]

According to the Annual Review, 81 of the 147 ransomware attacks were only known to the police, 40 only to the affected companies and 26 to both the affected companies and the police. This shows that 40 attacks were not reported to the police. Although this is not mandatory, it is advisable.[181]

Explanation of figures from the Dutch Data Protection Authority (DPA)

The figures are based on an analysis of reported data breaches to the DPA in 2023.[182] The DPA defines ransomware as '...a form of malware (malicious software) that holds a computer or files hostage. Usually, payment is then demanded.' Only exfiltration, without encryption or demand for payment of ransom, falls under other forms of malware. Similar to the Melissa project system, the DPA's figures are only based on the first attack; thus if one ransomware attack leads to ten reports to the DPA, this is counted as one in the figures. The reports themselves come from the data controllers. This can be the company where the attack took place and/or another company if their processor (e.g. an IT supplier) was affected by ransomware that also affected the company's data. A ransomware attack where personal data is affected must be reported unless there is no risk to individuals. This can mean that even if no data has been exfiltrated, there is still a reporting obligation. After all, the hackers had access to personal data for the purpose of encryption.

The actual number may be higher than 178 because:

- Despite the legal obligation, no report was made;
- No access was gained to personal data: this seems unlikely as personal data is almost always stored;
- The ransomware attack was prevented early;
- This concerns a foreign branch of an organisation with its headquarters in another country. The data breach report would then be filed with a foreign supervisory authority.

Difference between the Melissa project figures and those of the DPA

The number of reported ransomware attacks to the DPA is greater than what Melissa reported. An explanation for this could be the lower limit that Melissa uses for the size of the company, namely 100 FTEs. This lower limit does not apply to reports made to the DPA. Another explanation is that organisations that do not report to the police and do not seek help from cybersecurity companies cooperating in the Melissa project are excluded from Melissa's figures. However, they or their customers must report to the DPA.

In principle, it can be assumed that there exists a legal obligation to report almost all attacks to the DPA. After all, it is very likely that the attackers had access to sensitive personal data. The extent to which ransomware attacks reported by Melissa have been communicated to the DPA is unknown.

3 Basic principles for digital resilience

Many digital incidents occur because organisations have not implemented basic security measures. Examples include weak passwords or failing to install patches. This is unfortunate, because often the organisation can be made much more digitally resilient with relatively simple steps. But organisations also differ, which means there is no generic set of measures. A self-employed person has different information needs than an organisation in the vital sector. With the five basic principles of digital resilience, the NCSC and DTC provide guidelines for getting the basics in order.

Five basic principles for digital resilience

1. **Identify and assess risks**
   The first step is to identify what needs to be protected. By identifying dependencies (including suppliers), interests, threats and current resilience, organisations gain insight into their risks and interests to be protected. This provides insight into which security measures are needed to protect those interests.
2. **Promote safe behaviour**
   Many cyber incidents arise as a result of interactions between humans and technology. Employees can unintentionally (but sometimes intentionally) cause great damage to an organisation. In this sense, humans are the 'first line of defence'. Safe behaviour can be promoted by making people aware of and training them how to address risks. Above all, this is achieved by working towards a culture where they can safely report something if it does go wrong. Several technical tools, such as password managers, can also help in making safe choices.
3. **Protect systems, applications and devices**
   Systems, applications and devices keep organisations running. However, vulnerabilities in software and hardware can damage them or cause them to malfunction. As a result, your organisation's important or critical processes may be disrupted. It is therefore important to protect systems, applications and devices by choosing secure settings (hardening, segmentation) and detecting threats in due time (detection and monitoring). This reduces the attack surface and allows incidents to be addressed in time.
4. **Manage access**
   If access to data and systems is not consistently managed, it can lead to data breaches or unauthorised access. It is thus necessary to define which systems and data should be accessible for each user for the work that needs to be done. As a rule of thumb, do not grant more rights than necessary for the work (least privilege). Access rights must be altered when someone gets a new position or leaves the organisation.
5. **Prepare for incidents**
   Not all incidents can be prevented. In fact, to be resilient, it is good to assume that there is already a malicious actor in your network (assume breach) when setting up and managing a network. It is important to know how to respond to cyber incidents and, if things do go wrong, how to recover from them.

   If you want to read more about the basics and what measures you can take to improve your digital resilience, visit https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes and www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen for more information.

4 Sources and references

1 A revised conceptual framework has been used since CSAN 2021. The authors have gratefully used the following document for its creation: J. van den Berg, 'A basic set of mental models for understanding and dealing with the cybersecurity challenges of today', Journal of Information Warfare 19:1 (2020), https://repository.tudelft.nl/islandora/object/uuid%3A41a590a2-e11b-4ad3-b5aa-f3e51b2b7313.

2 Description taken from 'DDoS', NCSC, https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ddos (accessed 2024-08-14).

3 Description taken from 'Factsheet Help! Mijn website is beklad', NCSC, 2015-03-04, https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2019/juni/01/factsheet-help-mijn-website-is-beklad/20150304_FS-Help-Mijn-website-is-beklad-archief.pdf.

4 'Hacktivists Stoke Pandemonium Amid Russia's War in Ukraine', WIRED, 03-05-2022, https://www.wired.com/story/hacktivists-pandemonium-russia-war-ukraine/.

5 'Multiple Ukrainian Government Websites Hacked and Defaced', BleepingComputer, 14-01-2022, https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/.

6 Description taken from 'Dreigingsbeeld Statelijke Actoren 2021', AIVD, MIVD & NCTV, 03-02-2021, https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren.

7 Description taken from 'Cybersecuritybeeld Nederland 2020', NCTV, 2020-06-29, https://www.nctv.nl/documenten/publicaties/2018/06/13/cybersecuritybeeld-nederland-2018.

8 Figures that the Dutch DPA obtained from bilateral contacts.

9 Figures that the Dutch DPA obtained from bilateral contacts.

10 'Jaarbeeld Ransomware 2023', NCSC, 22-2-2024, https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023/Jaarbeeld_Ransomeware_2023_jan_dec.pdf, 20 June 2024; [interview report NCTV/AAN – Dutch DPA, dated March 2024, unpublished].

11 'Trends on Zero-Days Exploited In-the-Wild in 2023', Google, 27-03-2024, https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends.

12 'Cybersecurity Dreigingsbeeld voor de zorg 2023', Z-Cert, 27-02-2024, https://z-cert.nl/cybersecurity-dreigingsbeeld-voor-de-zorg-2023/.

13 'Exposed and vulnerable: Recent attacks highlight critical need to protect internet-exposed OT devices', Microsoft, 30-05-2024, https://www.microsoft.com/en-us/security/blog/2024/05/30/exposed-and-vulnerable-recent-attacks-highlight-critical-need-to-protect-internet-exposed-ot-devices/.

14 'het Samenhangend Inspectiebeeld cybersecurity vitale processen', Rijksoverheid.nl, 17-06-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/06/17/tk-samenhangend-inspectiebeeld-cybersecurity-vitale-processen.

15 'Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland', RTL Nieuws, 07-03-2023, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5370082/attent-zorg-behandeling-hack-ransomware-paspoorten-datalek.

16 'Datalek bij waternet: gegevens bezoekers Waterleidingduinen in handen van hackers', AT5, 15-03-2023, https://www.at5.nl/artikelen/219522/datalek-bij-waternet-gegevens-bezoekers-waterleidingduinen-in-handen-van-hackers.

17 'Gevaar op zee na hack bij maritieme dienstverlener', Digital Trust Center, https://www.digitaltrustcenter.nl/gevaar-op-zee-na-hack-bij-maritieme-dienstverlener.

18 'Maritiem dienstverlener Royal Dirkzwager getroffen door ransomware', Security.nl, 20-03-2023, https://www.security.nl/posting/789992/Maritiem+dienstverlener+Royal+Dirkzwager+getroffen+door+ransomware.

19 'Rapportage Datalekken 2023', Dutch Data Protection Authority, April 2024, https://www.autoriteitpersoonsgegevens.nl/uploads/2024-04/Rapportage%20datalekken%202023.pdf.

20 'Uitspraken. ECLI:NL:RBROT:2023:2931', https://uitspraken.rechtspraak.nl/, 06-04-2023, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2023:2931.

21 'Ransomwaregroep publiceert gegevens cliënten Brabantse zorginstelling', 20-04-2023, Security.nl,https://www.security.nl/posting/793808/Ransomwaregroep+publiceert+gestolen+cli%C3%ABntgegevens+Brabantse+zorginstelling.

22 'Zuid-Hollandse provider kon door ransomware geen internet leveren aan klanten', Tweakers, 24-04-2023,https://tweakers.net/nieuws/209058/zuid-hollandse-provider-kon-door-ransomware-geen-internet-leveren-aan-klanten.html.

23 'Website Rechtspraak.nl door ddos-aanval slecht of niet bereikbaar', Security.nl, 05-05-2023,https://www.security.nl/posting/795318/Website+Rechtspraak_nl+door+ddos-aanval+slecht+of+niet+bereikbaar.

24 'Website Staten-Generaal plat door 'overbelasting', Agconnect.nl, 04-05-2023, https://www.agconnect.nl/business/security/website-staten-generaal-plat-door-overbelasting.

25 'Klantenportaal HVC Energie is tijdelijk ontoegankelijk na cyberaanval', Tweakers, 26-05-2023, https://tweakers.net/nieuws/210142/klantenportaal-hvc-energie-is-tijdelijk-ontoegankelijk-na-cyberaanval.html.

26 'HVC wijst IT-leverancier na hackaanval de deur. Afvalverwerkings- en energiebedrijf heeft klantsysteem na cyberincident op eigen servers ondergebracht', Noordhollands Dagblad, 26-06-2024, https://www.noordhollandsdagblad.nl/regio/alkmaar/hvc-wijst-it-leverancier-na-hackaanval-de-deur.-afvalverwerkings-en-energiebedrijf-heeft-klantsysteem-na-cyberincident-op-eigen-servers-ondergebracht/14465686.html.

27 'Progress Software facing dozens of class action lawsuits, SEC investigation following MOVEit incident', The Record, 12-10-2023, https://therecord.media/progress-facing-lawsuits-sec-action.

28 'Landal GreenParks waarschuwt 12.000 gasten voor mogelijk datalek', Security.nl, 08-07-2023, https://www.security.nl/posting/798904/Landal+GreenParks+waarschuwt+12_000+gasten+voor+mogelijk+datalek 'Clop begins naming alleged MOVEit victims', Computerweekly, 15-07-2023, https://www.computerweekly.com/news/366541817/Clop-begins-naming-alleged-MOVEit-victims.

29 'Unpacking the MOVEit Breach: Statistics and Analysis', Emsisoft, 13-12-2023, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

30 'Pro-Russische groep legt websites Nederlandse havens plat', RTL Nieuws, 14-06-2023, https://www.rtlnieuws.nl/economie/artikel/5390268/pro-russische-cybercriminelen-ddos-aanval-havenbedrijf-rotterdam-amsterdam.

31 'IT-storing legde treinverkeer in en rond Amsterdam plat – update', Tweakers, 05-06-2023, https://tweakers.net/nieuws/210430/it-storing-legde-treinverkeer-in-en-rond-amsterdam-plat.html.

32 'Apeldoorn lekt gegevens inwoners na software-update van burgerportaal', Security.nl, 02-07-2023, https://www.security.nl/posting/801788/Apeldoorn+lekt+gegevens+inwoners+na+software-update+van+burgerportaal.

33 'Nederlandse organisaties doelwit van DDoS-aanvallen', NCSC, 08-08-2023, https://www.ncsc.nl/actueel/nieuws/2023/augustus/8/nederlandse-organisaties-doelwit-van-ddos-aanvallen.

34 'Site luchthaven Groningen plat, pro-Russische hackersgroep claimt ddos-aanval', Algemeen Dagblad, 27-08-2023, https://www.ad.nl/groningen/site-luchthaven-groningen-plat-pro-russische-hackers-groep-claimt-ddos-aanval~af075e19/

35 'Russische hackers weer actief', Rotterdams Dagblad, 22-08-2023.

36 'Cyberattack on British telecom Lyca prevented customers from making calls, topping up', The Record, 04-10-2023, https://therecord.media/cyberattack-on-lyca-stops-calls.

37 'International Criminal Court systems breached for cyber espionage', BleepingComputer, 21-10-2023, https://www.bleepingcomputer.com/news/security/international-criminal-court-systems-breached-for-cyber-espionage/.

38 'Computersystemen van Internationaal Strafhof aangevallen', NOS, 19-09-2023, https://nos.nl/artikel/2491054-computersystemen-van-internationaal-strafhof-aangevallen.

39 'Het CIDI is al wekenlang mikpunt van aanhoudende cyberaanvallen', EW Magazine, 20-11-2023, https://www.ewmagazine.nl/nederland/achtergrond/2023/11/het-cidi-is-al-wekenlang-mikpunt-van-aanhoudende-cyberaanvallen-1377466/.

40 'Landelijke storing alarmknoppensysteem voor ouderen door cyberaanval', NOS, 13-11-2023, https://nos.nl/artikel/2497671-landelijke-storing-alarmknoppensysteem-voor-ouderen-door-cyberaanval.

41 'Akira Ransomware Strikes Again: Compass Group Italia and Aqualectra Utility Hit by Data Breach', The Cyber Express, 08-12-2023, https://thecyberexpress.com/akira-ransomware-attack.

42 'Aqualectra herstelt na cyberaanval', Curacao.nu, 07-12-2023, https://curacao.nu/aqualectra-herstelt-na-cyberaanval/

43 'Turkish espionage campaigns in the Netherlands', Hunt and Hackett, 05-01-2024, https://www.huntandhackett.com/blog/turkish-espionage-campaigns.

44 'Cutting Edge, Part 4: Ivanti Connect Secure VPN Post-Exploitation Lateral Movement Case Studies', Mandiant, 04-04-2024, https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement.

45 'MIVD onthult werkwijze Chinese spionage in Nederland', Defence, 06-02-2024, https://www.defensie.nl/actueel/nieuws/2024/02/06/mivd-onthult-werkwijze-chinese-spionage-in-nederland.

46 'Nijmeegse chipmaker gehackt, criminelen dreigen kroonjuwelen te lekken', RTL, 12-04-2024, https://www.rtl.nl/tech/artikel/5444863/nexperia-gehackt-ransomware-cybercriminelen-dark-web?redirect=rtlnieuws.

47 'Russische propaganda te zien op kinderzender in Nederland na verstoring door hackers', NOS, 06-04-2024, https://nos.nl/artikel/2515707-russische-propaganda-te-zien-op-kinderzender-in-nederland-na-verstoring-door-hackers.

48 'BabyTV wéér overgenomen: kinderen zien gewelddadige Russische propaganda', Nu.nl, 17-04-2024, https://www.nu.nl/tech/6309428/babytv-weer-overgenomen-kinderen-zien-gewelddadige-russische-propaganda.html.

49 'Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout', BNR, 11-04-2024, https://www.bnr.nl/nieuws/tech-innovatie/10544662/geheime-afmeldcodes-van-duizenden-alarmsystemen-opvraagbaar-door-softwarefout.

50 'NCSC meldt actief misbruik van kritiek Palo Alto firewall-lek in Nederland', Security.nl, 19-04-2024,https://www.security.nl/posting/838602/NCSC+meldt+actief+misbruik+van+kritiek+Palo+Alto+firewall-lek+in+Nederland.

51 'AddComm geraakt door ransomware', AddComm, 22-05-2024, https://www.addcomm.nl/addcomm-geraakt-door-ransomware/.

52 'AddComm maakt afspraak met criminelen om gestolen klantdata te verwijderen', Security.nl, 28-05-2024, https://www.security.nl/posting/843180/AddComm+maakt+afspraak+met+criminelen+om+gestolen+klantdata+te+verwijderen.

53 'APT Activity Report' ESET, 14-05-2024, https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf.

54 'Grootste landelijke pinstoring in jaren kost supermarkten miljoenen', FD, 18-05-2024, https://fd.nl/bedrijfsleven/1517007/grootste-landelijke-pinstoring-in-jaren-kost-supermarkten-miljoenen.

55 'Hackers leggen websites politieke partijen plat op dag van Europese verkiezingen', Nu.nl, 06-06-2024, https://www.nu.nl/tech/6315777/hackers-leggen-websites-politieke-partijen-plat-op-dag-van-europese-verkiezingen.html.

56 'Meerdere kwetsbaarheden in Cisco Webex', NCSC, 07-06-2024, https://www.ncsc.nl/actueel/nieuws/2024/juni/07/meerdere-kwetsbaarheden-in-cisco-webex.

57 'SNS Bank, ASN Bank en RegioBank hebben opnieuw last van een storing', Tweakers, 24-06-2024, https://tweakers.net/nieuws/223570/sns-bank-asn-bank-en-regiobank-hebben-opnieuw-last-van-een-storing.html.

58 'ING erkent technische storing na problemen met overboekingen', Tweakers, 19-06-2024, https://tweakers.net/nieuws/223410/ing-erkent-technische-storing-na-problemen-met-overboekingen.html.

59 'Gegevens 60.000 terugbetalers op straat na fout bij DUO', BNR, 24-06-2024, https://www.bnr.nl/nieuws/nieuws-politiek/10550815/gegevens-60-000-terugbetalers-op-straat-na-fout-bij-duo.

60 'Storing in online dienstverlening', RDW, 13-06-2024, https://www.rdw.nl/particulier/nieuws/2024/storing-in-online-dienstverlening.

61 'Urenlange storing bij Odido opgelost', NOS, 30-06-2024, https://nos.nl/artikel/2526752-urenlange-storing-bij-odido-opgelost.

62 'Helping our customers through the CrowdStrike outage', Microsoft, 20-07-2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

63 'CrowdStrike: logicafout zorgde voor blue screen of death bij computers', Security.nl, 20-07-2024, https://www.security.nl/posting/850698/CrowdStrike%3A+logicafout+zorgde+voor+blue+screen+of+death+bij+-computers.

64 'Hoe een softwarefoutje luchthavens, media en ziekenhuizen kon platleggen', NOS, 19-07-2024, https://nos.nl/artikel/2529551-hoe-een-softwarefoutje-luchthavens-media-en-ziekenhuizen-kon-platleggen.

65 'Systemen bij overheidsdiensten plat door storing bij ministerie van Defensie', NOS, 28-08-2024, https://nos.nl/artikel/2534851-systemen-bij-overheidsdiensten-plat-door-storing-bij-ministerie-van-defensie.

66 'Kamerbrief over IT storing bij Defensie en andere overheidsdiensten', Dutch Central Government, 28-08-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/08/29/kamerbrief-it-storing-bij-defensie-en-andere-overheidsdiensten-tk.

67 'Spoedafdeling Brusselse ziekenhuis Sint-Pieter heropend na cyberaanval', VRT, 11-03-2023, https://www.vrt.be/vrtnws/nl/2023/03/11/spoedafdeling-brussels-ziekenhuis-sint-pieter-heropend-na-cybera/.

68 'Explosie aan datalekken door zerodaylek in Fortra GoAnywhere', Security.nl, 29-03-2023,https://www.security.nl/posting/791073/Explosie+aan+datalekken+door+zerodaylek+in+Fortra+GoAnywhere.

69 'Securitybedrijven slaan alarm over malware in desktopapplicatie 3CX', Security.nl, 30-03-2023, https://www.security.nl/posting/791292/Securitybedrijven+slaan+alarm+over+malware+in+desktopapplicatie+3CX+-+update.

70 'Symantec: aanval achter 3CX-hack raakte ook cruciale, Europese infrastructuur', Tweakers, 23-04-2023, https://tweakers.net/nieuws/209026/symantec-aanval-achter-3cx-hack-raakte-ook-cruciale-europese-infrastructuur.html.

71 '3CX: 'Supply Chain Attack Affects Thousands of Users Worldwide', Symantec, 30-03-2023, https://symantec-enterprise-blogs.security.com/threat-intelligence/3cx-supply-chain-attack.

72 'Hackers leggen websites van overheid plat in meer dan helft van Duitse deelstaten', VRT, 05-04-2023, https://www.vrt.be/vrtnws/nl/2023/04/05/hackers-leggen-websites-van-overheid-plat-in-meer-dan-helft-van/#:~:text=In%20meer%20dan%20de%20helft,verschillende%20delen%20van%20het%20land.

73 'Gemeente Herselt slachtoffer van cyberaanval: gemeentehuis, bibliotheek en OCMW al dagenlang dicht', VRT, 06-04-2023,https://www.vrt.be/vrtnws/nl/2023/04/06/cyberaanval/.

74 'Pro-Russische hackers vallen Europese luchtverkeersleiding aan', FD.nl, 20-04-2023, https://fd.nl/politiek/1474188/pro-russische-hackers-vallen-europese-luchtverkeersleiding-aan.

75 'Volt Typhoon targets US critical infrastructure with living-off-the-land techniques', Microsoft, 24-05-2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

76 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', CISA, 07-02-2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

77 'US confronts China over Volt Typhoon cyber espionage', Reuters, 08-05-2024, https://www.reuters.com/world/us/us-confronts-china-over-volt-typhoon-cyber-espionage-2024-05-08/.

78 'Noorse overheid erkent gehackt te zijn via zeroday in Ivanti', Tweakers, 26-07-2023, https://tweakers.net/nieuws/212098/noorse-overheid-erkent-gehackt-te-zijn-via-zeroday-in-ivanti.html.

79 'Poland investigates cyber-attack on rail network', BBC, 26-08-2023, https://www.bbc.com/news/world-europe-66630260.

80 'NATO says it is addressing an apparent cyberattack after strategy documents posted online', CNN, 03-10-2023, https://edition.cnn.com/2023/10/03/politics/nato-cyber-attack-strategy/index.html.

81 'Hackers steal user database from European telecommunications standards body', The Record, 02-10-2023, https://therecord.media/etsi-telecommunications-standards-body-hack-database-stolen.

82 'Die Energieversorgung Dänemarks war im Visier von Hackerangriffen. Eine Spur führt nach Russland', Neue Zürcher Zeitung (Internationale Ausgabe), 14-11-2023, https://www.nzz.ch/technologie/mehrere-hackerangriffen-nahmen-die-energieversorgung-daenemarks-ins-visier-eine-spur-fuehrt-nach-russland-ld.1765449.

83 'DP World hack: port operator gradually restarting operations around Australia after cyber-attack', The Guardian, 13-11-2023, https://www.theguardian.com/australia-news/2023/nov/13/australian-port-operator-hit-by-cyber-attack-says-cargo-may-be-stranded-for-days.

84 'DP World confirms data stolen in cyberattack, no ransomware used', Bleeping Computer, 28-11-2023, https://www.bleepingcomputer.com/news/security/dp-world-confirms-data-stolen-in-cyber attack-no-ransomware-used/.

85 'Two-day water outage in remote Irish region caused by pro-Iran hackers', The Record, 11-12-2023, https://therecord.media/water-outage-in-ireland-county-mayo.

86 'Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group ', CBS News, 26-11-2023, https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/.

87 'Federal investigators confirm multiple US water utilities hit by hackers', CNN, 01-12-2023, https://edition.cnn.com/2023/12/01/politics/us-water-utilities-hack/index.html.

88 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities', CISA, 01-12-2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

89 'Albanian parliament, telecom company hit by cyber attacks', The Record, 27-12-2023, https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks.

90 'Hospitals offline across Romania following ransomware attack on IT platform', The Record, 13-02-2024, https://therecord.media/romanian-hospitals-offline-after-ransomware-attack.

91 'Prescriptions nationwide impacted by cyber incident at Change Healthcare ', The Record, 22-02-2024, https://therecord.media/prescriptions-nationwide-impacted-by-change-healthcare-incident.

92 'Change Healthcare incident drags on as report pins it on ransomware group', The Record, 27-02-2024, https://therecord.media/change-healthcare-blackcat-alphv-incident-drags-on.

93 'Change Healthcare brings some systems back online after cyberattack', The Record, 08-03-2024, https://therecord.media/change-healthcare-brings-some-systems-online.

94 'UnitedHealth says Change hackers stole health data on 'substantial proportion of people in America'', 23-04-2024, https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/.

95 'The XZ Backdoor: Everything You Need to Know', WIRED, 02-04-2024, https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/.

96 'NHS London statement on Synnovis ransomware cyber attack – Tuesday 4 June 2024', NHS England, 04-06-2024, https://www.england.nhs.uk/london/2024/06/04/nhs-london-statement-on-synnovis-ransomware-cyber-attack/.

97 'Hospitals cyber attack impacts 800 operations', BBC, 14-06-2024, https://www.bbc.com/news/articles/cd11v377eywo.

98 'TeamViewer: Hackers copied employee directory and encrypted passwords', The Record, 01-07-2024, https://therecord.media/teamviewer-cyberattack-employee-directory-encrypted-passwords.

99 'Identiteitsverificatiebedrijf TikTok, Uber en X lekte kopieën van id-documenten', Security.nl, 27-06-2024.

100 'Cybercrimebeeld Nederland', Public Prosecution Service and Police, 28-06-2024, https://fts.politie.nl/cybercrimebeeld/.

101 'Servers neergehaald van 's werelds grootste ransomware groepering', Police, 20-02-2024, https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html.

102 'Meerdere botnets ontmanteld in grootste internationale operatie tegen ransomware ooit, Police, 30-05-2024, https://www.politie.nl/nieuws/2024/mei/30/11-meerdere-botnets-ontmanteld-in-grootste-internationale-operatie-tegen-ransomware-ooit.html.

103 'Europol coordinates global action against criminal abuse of Cobalt Strike', Europol, 03-07-2024, https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-global-action-against-criminal-abuse-of-cobalt-strike.

104 'Ragnar Locker ransomware developer arrested in France', Bleepingcomputer, 20-10-2023, https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-developer-arrested-in-france/

105 'Ransomware group LockBit is disrupted by a global police operation that includes 2 arrests', AP, 20-02-2024, https://apnews.com/article/lockbit-ransomware-website-police-disrupt-0297653ddfc245fcdf7d-9308c6c1e6fe.

106 'Police arrest Conti and LockBit ransomware crypter specialist', Bleepingcomputer, 12-06-2024, https://www.bleepingcomputer.com/news/security/police-arrest-conti-and-lockbit-ransomware-crypter-specialist/.

107 'Russian hackers sanctioned by European Council for attacks on EU and Ukraine', The Record, 24-06-2024, https://therecord.media/six-russian-hackers-sanctioned-european-council-eu-ukraine; 'EU-sancties tegen zes Russische hackers', NOS.nl, 24-06-2024, https://nos.nl/artikel/2525962-eu-sancties-tegen-zes-russische-hackers.

108 'VS en VK zetten nog eens elf verdachten achter Trickbot-malware op sanctielijst', Security.nl, 07-09-2023, https://www.security.nl/posting/809408/VS+en+VK+zetten+nog+eens+elf+verdachten+achter+Trickbot-malware+op+sanctielijst.

109 'VS legt sancties op aan vermeende leden LockBit-ransomwaregroep', Security.nl, 20-02-2024, https://www.security.nl/posting/830419/VS+legt+sancties+op+aan+vermeende+leden+LockBit-ransomwaregroep.

110 'Nederland en VS verstoren Russische digitale beïnvloedingsoperatie', AIVD, 09-07-2024, https://www.aivd.nl/actueel/nieuws/2024/07/09/nederland-en-vs-verstoren-russische-digitale-beinvloedingsoperatie.

111 'Cybersecurity Assessment Netherlands. CSAN 2022', NCTV, July 2022.

112 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf; 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministry of Defence, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf; Microsoft Digital Defense Report 2023, Microsoft, October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023; 'M-Trends 2024 Special Report', Google, 13-5-2024, https://services.google.com/fh/files/misc/m-trends-2024.pdf.

113 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

114 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministry of Defence, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

115 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministry of Defence, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

116 'Exclusive: UN experts investigate 58 cyber attacks worth $3 bln by North Korea', Reuters, 8-2-2024, https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyber attacks-worth-3-bln-by-north-korea-2024-02-08/; 'Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)', United Nations Security Council, 7 March 2024, https://undocs.org/en/S/2024/215; 'Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises', Chainanalysis, 24-1-2024, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/.

117 'Microsoft Digital Defense Report 2023', Microsoft, October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023; 'Microsoft shifts to a new threat actor naming taxonomy', Microsoft, 18-4-2023, https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/; 'AIVD Jaarverslag 2023', 'Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+-Jaarverslag+2023.pdf.

118 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf

119 'The most notorious instances of commercial spyware', Kaspersky, 21-3-2024, https://www.kaspersky.com/blog/commercial-spyware/50813/.

120 Marczak, Scott-Railton, McKune, Abdul Razzak, Deibert, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', 18-9-2018, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf.

121 'Turkish espionage campaigns in the Netherlands', Hunt and Hackett, 5-1-2024, https://www.huntandhackett.com/blog/turkish-espionage-campaigns.

122 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministry of Defence, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

123 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

124 'Cybercrimebeeld Nederland 2024', Public Prosecution Service & Police, 11-6-2024, https://www.om.nl/onderwerpen/cybercrime/cybercrime-beeld-cybercrimebeeld-ccbn.

125 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

126 'AIVD Jaarverslag 2023', Ministry of the Interior and Kingdom Relations, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

127 'Factsheet omgaan met edge devices', NCSC, 10-6-2024, https://www.ncsc.nl/documenten/factsheets/2024/juni/10/kennisproduct-omgaan-met-edge-devices.

128 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministry of Defence, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

129 'Factsheet omgaan met edge devices', NCSC, 10-6-2024, https://www.ncsc.nl/documenten/factsheets/2024/juni/10/kennisproduct-omgaan-met-edge-devices.

130 'Marktstudie Clouddiensten', Netherlands Authority for Consumers & Markets, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

131 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

132 'Marktstudie Clouddiensten', Netherlands Authority for Consumers & Markets, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

133 Based on the following, among other sources: 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; 'Baas in eigen cloud – het kan, maar Europa doet het niet', de Correspondent, 7-5-2024, https://decorrespondent.nl/15295/baas-in-eigen-cloud-het-kan-maar-europa-doet-het-niet/a6fda854-11c2-0676-355c-129f8a76bf4d.

134 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; feedback on draft text of a large government unit.

135 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

136 Feedback on draft text from a large government entity.

137 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; 'Baas in eigen cloud – het kan, maar Europa doet het niet', de Correspondent, 7-5-2024, https://decorrespondent.nl/15295/baas-in-eigen-cloud-het-kan-maar-europa-doet-het-niet/a6fda854-11c2-0676-355c-129f8a76bf4d.

138 Genoemd door partner tijdens expertmeeting in het kader van CSBN voorbereidingen.

139 'Rijksbrede Risicoanalyse Nationale Veiligheid', National Security Analysts Network, 31-07-2022, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2022/07/31/rijksbrede-risicoanalyse-nationale-veiligheid-2022/Rijksbrede+Risicoanalyse+Nationale+Veiligheid+2022.pdf.

140 'Review of the Summer 2023 Microsoft Exchange Online Intrusion', Cyber Safety Review Board, 20-03-2024, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

141 'NSA Releases Top Ten Cloud Security Mitigation Strategies', NSA, 7-03-2024, https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/.

142 'Manifesto: Actioning Baseline Cloud Security by Default', CyberSecurity Coalition, 25-6-2024, https://blog.cybersecuritycoalition.be/manifesto-actioning-baseline-cloud-security-by-default/.

143 'Marktstudie Clouddiensten', Autoriteit Consument & Markt, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

144 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

145 'Helping our customers through the CrowdStrike outage', Microsoft, 2027-07-20, Helping our customers through the CrowdStrike outage - The Official Microsoft Blog.

146 'CrowdStrike, Antitrust, and the Digital Monoculture', Electronic Frontier Foundation, 2024-08-01, https://www.eff.org/deeplinks/2024/07/crowdstrike-antitrust-and-digital-monoculture.

147 'ICT in beeld', UWV, 10-8-2023, https://www.werk.nl/arbeidsmarktinformatie/sector/ict/personeelstekort-in-ict-blijft-ondanks-toename-aantal-ict-ers.

148 'Lijst van vragen en antwoorden over de Jaarverslagen van de ministeries van Justitie en Veiligheid 2023 (Kamerstuk 36560-VI-1), Binnenlandse Zaken en Koninkrijksrelaties 2023 (Kamerstuk 36560-VII-1 en Economische Zaken en Klimaat 2023 (Kamerstuk 36560-XIII)', House of Representatives, 4-6-2024, https://www.tweedekamer.nl/kamerstukken/detail?id=2024Z09679&did=2024D22834.

149 'Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity', Talent for Technology and Dialogic Platform, April 2024, https://www.cybersecurityraad.nl/documenten/brieven/2024/07/04/csr-signaal-brief-cybersecurity-arbeidsmarkt.

150 'Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity', Talent for Technology and Dialogic Platform, April 2024, https://www.cybersecurityraad.nl/documenten/brieven/2024/07/04/csr-signaal-brief-cybersecurity-arbeidsmarkt.

151 'Foresight 2030 Threats', ENISA, Ma 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024.

152 'Antwoorden op aanvullende kennisvragen inzake Kwantumtechnologie en de gevolgen voor encryptie', Ministry of the Interior and Kingdom Relations, 7-11-2023, https://open.overheid.nl/documenten/7cc21d78-75bb-4778-9615-cccb2b79b613/file.

153 'Maak je organisatie quantumveilig', NCSC & AIVD, 18-09-2023, https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig.

154 'Bereid je voor op de dreiging van quantumcomputers', AIVD, 23-09-2021, https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.

155 'The PQC Migration Handbook', TNO, 4-4-2023, https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/ V 'Quantumveilige cryptografie', Digital Government, 7-11-2023 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/.

156 For substantiation, see the following paragraphs.

157 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023, https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Hoe datahandelaren adressen van jou én van bedreigde personen te koop aanbieden', RTL, 5-1-2024, https://www.rtl.nl/boulevard/crime/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te; 'Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico', BNR, 10-01-2024, https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico.

158 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023, https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Biden order will limit how much data can be sold to Russia and China', The Record, 28-02-2024, https://therecord.media/biden-executive-order-data-sales-adversaries-russia-china.

159 'Each Facebook User Is Monitored by Thousands of Companies', Consumer Reports, 17-01-2024, https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/.

160 'Stichting start massaclaim tegen Google wegens dataverzamelen Android', Security.nl, 8-04-2024, https://www.security.nl/posting/837020/Stichting+start+massaclaim+tegen+Google+wegens+dataverzamelen+Android.

161 'Minister: automobilist moet zeggenschap over voertuigdata hebben', Security.nl, 18-01-2024, https://www.security.nl/posting/825979/Minister%3A+automobilist+moet+zeggenschap+over+voertuigdata+hebben.

162 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023, https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Hoe datahandelaren adressen van jou én van bedreigde personen te koop aanbieden', RTL, 5-1-2024, https://www.rtl.nl/boulevard/crime/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te; 'Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'', BNR, 10-01-2024, https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico; 'Kabinet wil bewustzijn burgers over dataverzameling apps en sites vergroten', Security.nl, 26-06-2024, https://www.security.nl/posting/847721/Kabinet+wil+bewustzijn+burgers+over+dataverzamelin-g+apps+en+sites+vergroten.

163 'Kabinet wil bewustzijn burgers over dataverzameling apps en sites vergroten', Security.nl, 26-06-2024, https://www.security.nl/posting/847721/Kabinet+wil+bewustzijn+burgers+over+dataverzamelin-g+apps+en+sites+vergroten.

164 'FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data', The White House, 28-02-2024, https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

165 'Biden order will limit how much data can be sold to Russia and China', The Record, 28-02-2024, https://therecord.media/biden-executive-order-data-sales-adversaries-russia-china.

166 'Cybercrimebeeld Nederland 2024', Public Prosecution Service & Police, 11-6-2024, https://www.om.nl/onderwerpen/cybercrime/cybercrime-beeld-cybercrimebeeld-ccbn

167 Internal information, from the Public Prosecution Service.

168 Free to various articles of and a presentation by Keymolen, including 'Trust and trustworthiness in a data-driven context', E. Keymolen, 27-03-2020, https://www.youtube.com/watch?v=oqr39l7sjyU; 'Regulating security on the Internet: control versus trust', Bibi van den Berg & Esther Keymolen, International Review of Law, Computers & Technology, 31:2.; 'Can we trust trust-based data governance models?', Bart van der Sloot, Esther Keymolen, in Data & Policy (2022); 'Trustworthy tech companies: talking the talk or walking the walk?', Esther Keymolen, AI Ethics (2023). Keymolen addresses the concept of trust in a broader context than digital security. The link to digital security is the authors' own interpretation.

169 'Digitalisering van het verkiezingsproces? Bij twijfel niet doen', 16-3-2023, https://www.nederlandrechtsstaat.nl/digitalisering-van-het-verkiezingsproces-bij-twijfel-niet-doen/.

170 'Trust and trustworthiness in a data-driven context', E. Keymolen, 27-03-2020, https://www.youtube.com/watch?v=oqr39l7sjyU.

171 In het CSBN2023 werden zowel de DMA als DSA beschreven. Vanwege deze reden zijn deze ook dit jaar opgenomen, om zo de voortgang te kunnen weergeven.

172 'Eerste bedrijven onder Digital Services Act', Digital Government, 8-5-2023, https://www.digitaleoverheid.nl/nieuws/europese-dsa-verscherpt-online-toezicht/; 'DSA voor alle digitale diensten van kracht', Digital Government, 19-2-2024, https://www.digitaleoverheid.nl/nieuws/dsa-voor-alle-digitale-diensten-van-kracht/.

173 'Overzicht wetten en regels voor online platforms', Netherlands Authority for Consumers & Markets, n.d., https://www.acm.nl/nl/online-platforms/overzicht-wetten-en-regels-voor-online-platforms.

174 'Europees akkoord: veiligheidseisen en standaarden voor alle digitale producten', Dutch Central Government, 1-12-2023, https://www.rijksoverheid.nl/actueel/nieuws/2023/12/01/europees-akkoord-veiligheidseisen-en-standaarden-voor-alle-digitale-producten.

175 'Voortgangsrapportage Nederlandse Cybersecuritystrategie', Dutch Central Government, 9-10-2023, https://www.rijksoverheid.nl/documenten/rapporten/2023/10/09/tk-bijlage-1-voortgangsrapportage-nederlandse-cybersecuritystrategie-2023.

176 'REGULATION (EU, Euratom) 2023/2841 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL', Official Journal of the European Union, 18-12-2023, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302841

177 'The EU Cyber Solidarity Act', European Commission, n.d., https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

178 'Ransomware-aanvallen op instellingen en bedrijven in Nederland', Dialogic Innovation and Interaction, 12-09-2023, https://repository.wodc.nl/handle/20.500.12832/3292.

179 'Jaarbeeld Ransomware 2023', Project Melissa, 22-02-2024, https://cyberveilignederland.nl/upload/userfiles/files/Jaarbeeld_Ransomeware_2023_jan_dec.pdf.

180 Explanation given by a Melissa project employee during an interview.

181 'Jaarbeeld Ransomware 2023', Project Melissa, 22-02-2024, https://cyberveilignederland.nl/upload/userfiles/files/Jaarbeeld_Ransomeware_2023_jan_dec.pdf.

182 Gegevens Autoriteit Persoonsgegevens verkregen uit bilaterale contacten.

Publication details

The Cybersecurity Assessment Netherlands, 2024 (CSAN 2024) provides insight into the digital threat, the interests that may be affected by this, digital resilience and, lastly, the digital risks. It also aims to provide an insight into possible changes in the strategic themes detailed in the CSAN 2022. These themes formed a substantive basis for the Netherlands Cybersecurity Strategy 2022–2028. CSAN 2024 built on these themes and describes developments within them. The CSAN provides a substantive basis for evaluating the action plan derived from it. The focus is on national security.

The National Coordinator for Security and Counterterrorism (NCTV) prepares the CSAN, cooperating with the National Cybersecurity Centre (NCSC) for this purpose. The NCTV gratefully makes use of the information, insights and expertise of government services, providers of critical processes, scientists and other parties. The NCTV adopts the CSAN each year.

Together with partners from the security domain, the NCTV helps make the Netherlands secure and stable by recognising threats and strengthening the resilience and protection of national security interests. The purpose is to prevent and minimise social disruption. Since the establishment of the NCTV, a single government organisation has been responsible for counterterrorism, cybersecurity, national security and crisis management.

The NCSC contributes to making the Netherlands digitally resilient and, in doing so, creating a favourable digital climate for organisations and society. The NCSC does this through cooperation with other public and private partners at home and abroad to improve the digital resilience of organisations. The NCSC also helps prevent disruptive cyber incidents and crises and to mitigate their impact.

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
info@nctv.minjenv.nl
@nctv_nl

Oktober 2024