National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

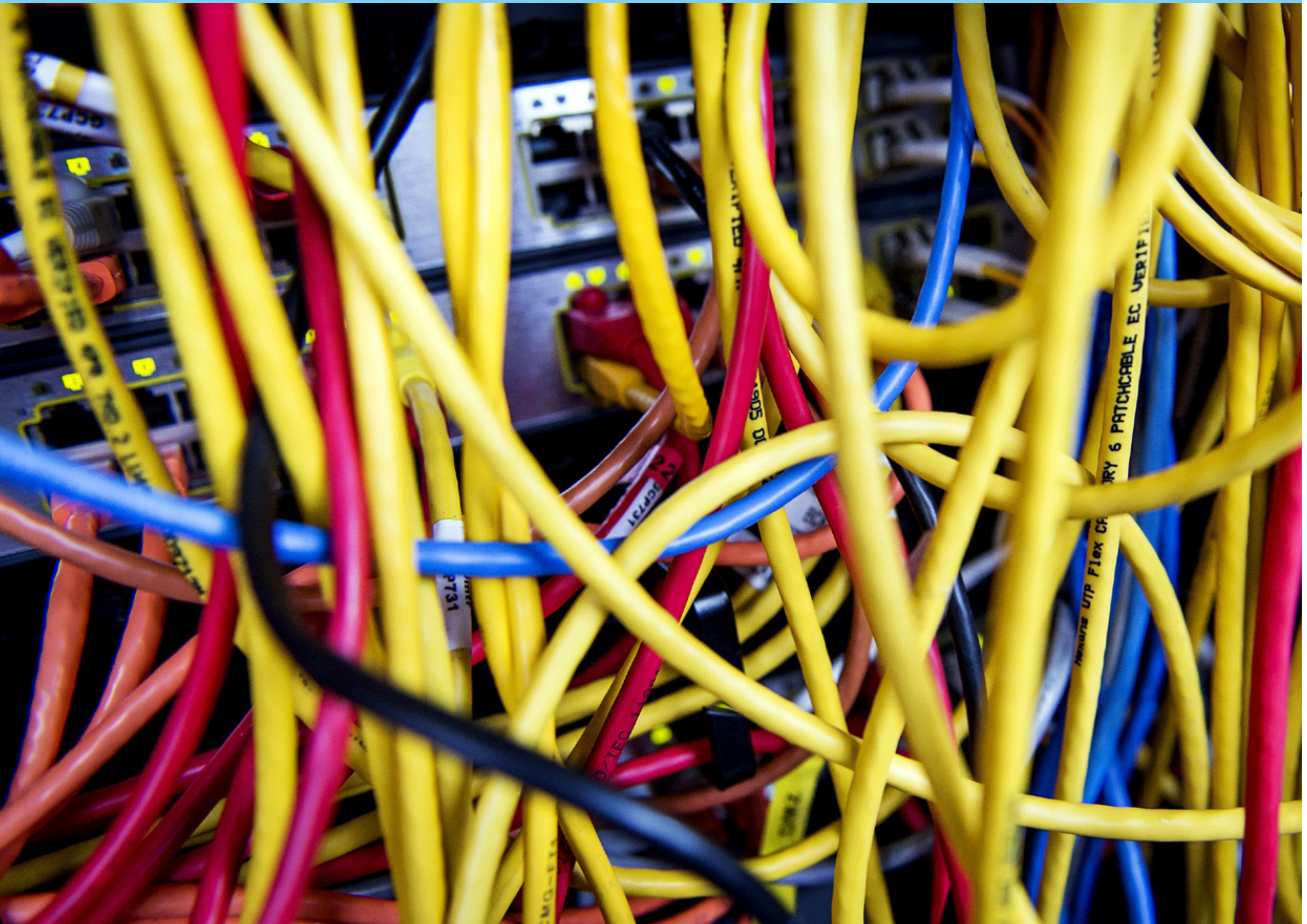
Cybersecurity Assessment Netherlands 2025

Risky mix in an unpredictable world

Cover image: Europe, and therefore the Netherlands, is dependent on providers from other, mostly non-European countries for many different digital processes and services. Digital dependencies that were not previously considered risky may become so later, for example due to geopolitical developments.

Table of contents

There is a wide variety of attacks, cyber capabilities are increasing, and there is a mixture and proliferation of actors. Geopolitical unpredictability is translating into the digital domain. As a result, the digital threat landscape is becoming increasingly complex.



Risky mix in an unpredictable world

The digital threat landscape is becoming increasingly diverse and unpredictable. State actors, cybercriminals and other malicious actors are carrying out a wide range of attacks. Moreover, geopolitical unpredictability is spilling over into the digital domain. State actors are developing or expanding cyber programmes by using non-state actors or private organisations. Furthermore, shifting geopolitical relations can make digital dependencies risky even if they previously were not. Malicious actors can also use generative AI, which makes attacks easier and more scalable.

All these developments are unfolding at the same time and influence one another, which makes the threat landscape increasingly complex. Building and maintaining digital resilience is certainly not getting any easier, but it does not need to be overly complex either. Basic digital principles provide an effective barrier against a large proportion of cyberattacks. Digital security has long ceased to be just a matter for technical experts. Especially for non-digital factors such as geopolitics, it is – or should be – a matter for the boardroom.

Wide variety of incidents illustrates a diverse and unpredictable threat landscape

The digital threat landscape is becoming increasingly diverse, unpredictable and complex. Among other things, this is clear from the wide variety of incidents that occurred during this reporting period. These involved a variety of attackers, methods, targets and motives.For instance, the Chinese state actor Salt Typhoon targeted several Dutch and foreign organisations, the Russian actor Laundry Bear carried out a cyberattack on the National Police, North Korean hackers stole digital currencies from, among others, Dutch organisations, and the Netherlands became victim of cyber sabotage for the first time by a Russian state-backed group. And, for the first time, a Russian state-backed group carried out cyber sabotage in the Netherlands. Cybercriminals also carried out attacks continuously. for example by stealing sensitive personal and patient data of nearly one million people from a laboratory. Pro-Russian hacktivists – often backed by the state – also carried out several DDoS campaigns against Dutch websites, including during the NATO summit in June 2025.

It once again became clear that cyber incidents can spill over into the physical domain. For example, hackers gained access to the Public Prosecution Service's (OM's) Citrix Netscaler systems through a vulnerability. After discovering the hack, the OM decided to disconnect its systems from the internet, causing disruption in the criminal justice chain and in daily operations. The incident at the OM also illustrates that malicious actors remain highly interested in edge devices.[I] Both state actors and cybercriminals frequently and increasingly attack these systems, aiming to penetrate connected networks.

Although incidents in the Netherlands during this reporting period did not cause societal disruption or have a significant impact on national security, several incidents did have the potential to do so. More so than in previous years, it became clear in the Netherlands that the impact of cyber incidents extends beyond the digital domain. They affect digital processes, daily work and personal lives. This illustrates how dependent our country is on digital systems and how that dependence makes us vulnerable.

Geopolitical unpredictability poses risks to digital security

International relations are becoming more unpredictable, and that affects digital security. Deteriorating relations can make cyberattacks more appealing to state actors because they are cheap, scalable and because involvement is deniable. As a result, a growing number of countries are setting up or expanding cyber programmes and countries are using non-state actors or private organisations to carry out (parts of) those attacks. Research by the AIVD and MIVD, for instance, show that every pro-Russian hacktivist group they investigated receives some degree of support from the Russian government. In China, intelligence and security services, knowledge institutions and companies are closely connected. Chinese companies provide attack infrastructure or malware, for example, while knowledge institutions research vulnerabilities in edge devices. As a result, Chinese actors are systematically successful in hacking Western governments and companies.

The same geopolitical unpredictability can also make digital dependencies risky when they previously were not. Like other countries, the Netherlands depends on foreign providers – including those in the United States – for many digital processes and services. Laws and regulations from such countries can have extraterritorial effects, and their choices can thus affect the Netherlands even when not directly aimed at it. As this creates uncertainty, it is important to assess dependencies continuously for potential risks and, where possible, to establish digital and non-digital fallback options.

Geopolitical developments – and their current unpredictability in particular – make the threat landscape opaque and unpredictable. It should also be taken into consideration that this is happening at a time when technology is advancing rapidly. Generative artificial intelligence (AI) is developing at great speed, and malicious actors can use it to carry out attacks more easily and on a larger scale – even when they are less advanced.

Telecom sector illustrative of the convergence of threats, risks and considerations

The telecom sector is a clear example of where many risks, threats and considerations converge. A successful attack on the telecom sector can have major consequences, not least because many other sectors depend on the functioning of telecommunications. Because of that dependency, an incident in the telecom sector can quickly have far-reaching consequences for other sectors, including critical ones. Although all critical sectors are attractive targets for malicious actors, the telecom sector continues to draw their attention. The sector can be attractive for espionage purposes; according to the AIVD, hacks on telecommunications providers are among the most valuable intelligence positions for state actors. Sabotage can also be an objective, which may be directed against (specific) customers who use the network. In addition, the sector is of interest to cybercriminals, mainly because of the large volumes of personal data that are processed within it.

The telecom sector constantly performs a balancing act between security and accessibility of the services it provides. To offer users communication services, it must grant access to the network. As a result, millions of users are connected to the network, which requires a certain degree of openness that can conflict with digital security.

The reality of the threat facing the telecom sector, and the potential impact of a successful attack, became clear through the global attack campaign by the cyber actor Salt Typhoon. The hackers penetrated deeply into the infrastructure of US telecom networks and, according to media reports, gained access to private communications of the US President and Vice-President, among others. Salt Typhoon also targeted several smaller internet service and hosting providers in the Netherlands.

Although the various threats, risks and considerations that converge in the telecom sector are not unique to it, they illustrate the complexity of the current threat landscape and the need for continuous risk assessment.

Basic principles increase resilience against a complex threat landscape

The conclusion that threats are becoming more unpredictable and complex does not necessarily mean that defending against them is so as well. Many digital incidents arise from a lack of proper 'digital hygiene'. The digital basic principles, as set out by the National Cyber Security Centre (NCSC) and the Digital Trust Centre (DTC), still form an effective defence against a large proportion of cyberattacks. For an average organisation, the message is therefore clear: do not fixate on the complex threat landscape, but first defend against it by applying the basic principles. A key component of those principles is being prepared for incidents, thereby focusing on resilience and the ability to recover once an incident has occurred.

Several incidents involving Dutch victims show that cybersecurity measures within many central government organisations have been inadequate for some time. Despite various projects and improvement programmes on cybersecurity within the central government, these organisations are often unable to detect and mitigate attacks independently. Many government organisations do not comply with the information security guidelines prescribed by the central government itself. This lack of cybersecurity also creates a false sense of security; it is simply impossible to conclude that government organisations are not currently compromised. Resilience levels differ from one organisation and sector to another, but it is clear that the central government still has work to do in this area. This particularly includes properly arranging fallback options in the event of failure or disruption of digital processes. It also appears that the dependence on external digital service providers and the potential risks arising from it are not being adequately considered. The current geopolitical unpredictability may (further) increase those risks.

The preceding sections show that not all factors influencing digital security are digital in nature. Geopolitical developments, for instance, have no digital component, yet they do affect digital security. This means that digital security has long ceased to be solely a task for technical experts. It is also, or perhaps even more so, a matter for those in management, to ensure that non-digital factors form part of an ongoing and continuous risk assessment.

[I] Edge devices are located at the edge of a network and consist of security and other products such as firewalls, VPN servers and routers.

Clinical Diagnostics (Eurofins) announced in August that sensitive patient data had been stolen from healthcare providers who had had tests carried out at the laboratory. This is believed to have happened during a ransomware attack in July. The centre for population screening (Bevolkingsonderzoek Nederland) informed 941,000 people that their data had (possibly) been stolen during the attack.

bevolkingsonderzoek nederland

Voor vroege opsporing van kanker

Utrecht, 11 september 2025

Betreft: Datalek persoonsgegevens deelnemers bevol

Ons kenmerk: 3_1114518

1 Annual Review

Although nuances are changing, there have been no major shifts in the overall threat assessment. There is a wide variety of incident types, causes, attackers and levels of impact. Both state actors and cybercriminals carry out cyberattacks against Dutch targets and/or affect Dutch interests. Edge devices remain of constant interest to malicious actors, as illustrated by the incident at the Public Prosecution Service. Disruptions caused by DDoS attacks also continue. For example, websites and applications – such as DigiD – were unavailable or only partially accessible on several occasions. Furthermore, cybersecurity incidents at suppliers and service providers also regularly lead to data breaches among their customers. One example is the ransomware attack on a laboratory, in which sensitive data belonging to various healthcare providers and their patients was stolen. The NATO summit also took place in the Netherlands in 2025. Although geopolitical events are an attractive target for malicious actors, no cyber incidents occurred during the NATO summit that disrupted the summit or causes societal disruption.

In addition to cyberattacks, there were again many examples of disruptions resulting from unintentional actions. Software errors were often the cause of these disruptions.

Variety of incidents illustrates a diffuse threat assessment

Disruption of services caused by DDoS attacks

During the past reporting period, several DDoS attacks caused (temporary) service disruptions. Between January and March 2025, for example, four attacks made DigiD unavailable for an hour or longer. As a result, related services were also partly inaccessible, and users were temporarily unable to log in. A DDoS attack is easy to launch, and organisations can make themselves relatively resilient to this type of attack. In general, the impact of DDoS attacks is therefore limited, usually affecting only the availability of digital processes for a short time. In the case of the DigiD attacks early this year, Logius – the administrator of DigiD – stated that these attacks were of a different calibre. According to Logius, the attacks adapted more quickly to defensive measures.[1] Logius also noted that it could not confirm whether the number of DDoS attacks on DigiD had increased compared with previous years. The type of attack may have been more visible to users because it affected an essential process. DDoS attacks on DigiD also caused disruptions later in the year. Other attacks that disrupted services included those on Adyen, SURF and Dutch government websites. The attack on Adyen caused payment problems in shops, online retailers and the hospitality sector. It is not known who was responsible for the attacks on DigiD and Adyen. DDoS attacks on SURF caused internet and other disruptions at educational institutions and hospitals; the perpetrators are also unknown.

Finally, Dutch government websites were temporarily offline due to DDoS attacks carried out by pro-Russian hackers.

At least 121 unique Dutch ransomware incidents in 2024

In 2024, the National Cyber Security Centre (NCSC), the Police, the Public Prosecution Service (OM), Cyberveilig Nederland and cybersecurity companies exchanged information on ransomware incidents each month as part of Project Melissa (see Appendix 2). The data show that there were at least 121 unique ransomware incidents in the Netherlands in 2024. Of these, 76 were identified through police reports and 20 through incident response companies. In addition, 25 incidents overlapped – cases that appeared both in the monthly data collection and in police reports. In 2023, Project Melissa identified at least 147 unique ransomware attacks. It should be noted that this figure is based on the initial ransomware attack: an attack on a single provider with dozens of customers who are also affected by the same incident counts as one attack. An analysis of ransomware attacks in 2024 shows that cybercriminals are not using new techniques to deploy ransomware. Criminals most often still gain access through software vulnerabilities and by taking over accounts.[2] In 2024, the Dutch Data Protection Authority received 1,430 unique data breach notifications related to cyberattacks, of which it investigated 853. Of the investigated attacks, 112 (13 percent) involved ransomware. Data were stolen in at least 53 percent of those ransomware attacks.[3]

Espionage, sabotage and (preparation for) sabotage by state actors, including in the Netherlands

The AIVD and MIVD state that Russia, China, Iran and North Korea have offensive cyber programmes targeting Dutch interests. Through these programmes, they conduct espionage, influence operations and acts of sabotage. Sabotage potentially has the greatest impact on Dutch society.[4] Other countries besides those mentioned are also investing in cyber programmes. Although the offensive cyber programmes of these countries may not currently be directed specifically at the Netherlands, that could change in the future. As a result, Dutch interests may be affected, or the Dutch digital infrastructure could be misused or exploited to carry out attacks against other targets.[5]

During this reporting period, major international cybersecurity companies published several reports on global cyber campaigns by state actors, in which Dutch victims were also identified. Media reports indicated, for example, that Delft University of Technology was (unsuccessfully) targeted by Salt Typhoon. It has been confirmed that the university was scanned, but there was no actual attack. CrowdStrike also reported during this period that North Korean hackers also carried out cyberattacks against Dutch organisations.

Furthermore, in September 2024, the police fell victim to a cyberattack. Through this attack, malicious actors stole work-related contact information from police employees. The AIVD, MIVD and police were not able to determine that other data was stolen. In May 2025, the Dutch intelligence services attributed this attack to a previously unknown, most likely Russian state-sponsored cyber actor. Besides the National Police, this group, called Laundry Bear, reportedly also attacked other Dutch organisations as part of a global campaign. In addition, the MIVD warned in May 2025 about an espionage campaign by APT28[II], which reportedly conducted operations against Ukraine and NATO member states. The Dutch armed forces, ministries and business sector were direct and indirect targets of these cyber espionage attempts. The MIVD also reported that the Netherlands became a victim of deliberate cyber sabotage by a Russian state-sponsored group for the first time in 2024. This cyber sabotage attack targeted the digital control system of a public facility.[6]

Incidents at suppliers lead to data breaches, illustrating the vulnerability of the supply chain

A cyber incident at a supplier or service provider can have far-reaching consequences for organisations within the same supply chain, including the company's customers. This reporting period provided an example in the form of a cyberattack on a supplier serving several municipalities. This caused data breaches at municipalities including Dinkelland, Tubbergen and Amersfoort. A ransomware attack on a Dutch laboratory also led to the leak of highly sensitive data belonging to hundreds of thousands of patients. The data originated from various healthcare providers that had commissioned work from the laboratory.

Processes disrupted by software errors and outdated hardware

In July 2024, CrowdStrike rolled out a software update that caused Windows systems to go offline and display a 'blue screen of death'. As a result, entire systems shut down and (critical) organisations around the world faced problems. A month later, a software error in a standard network component of the Defence network NAFIN led to a large-scale outage in the Netherlands, disrupting processes at various government bodies and at Eindhoven Airport. The NAFIN and CrowdStrike outages were visible because of their major impact, but also on a smaller scale processes were disrupted by outages during this reporting period. The Rijnstate Hospital in Arnhem was forced to cancel planned care after a software update prevented staff from processing data in patient records. In March, the Public Prosecution Service (OM) even temporarily took its ICT systems offline because of a 'persistent outage'. Although the exact cause was not disclosed, the OM indicated that it was increasingly experiencing outages, (partly) due to outdated infrastructure.

NATO Summit in the Netherlands: incidents within expectations, no significant impact

On 24 and 25 June 2025, the NATO Summit took place in The Hague. The summit attracted dozens of world leaders, ministers and thousands of delegates, and received global attention. Such geopolitical events are an attractive target for malicious actors. Although a few disruptions occurred in the transport and telecom sectors during the summit, these had no cybersecurity component according to those involved. The media reported a DDoS campaign by pro-Russian hackers targeting Dutch organisations, but its actual impact was very limited.

The NCSC developed scenarios in advance with its partners. These made it possible to prepare effectively for foreseeable incidents and to assess and gauge the likelihood of any incidents during the NATO Summit against those scenarios. All incidents fell within the predefined scenarios. However, the attention surrounding such an event shows that even the smallest and more common disruptions are immediately thrust into the spotlight. This can heighten the perceived level of threat and distort the overall picture.

To ensure good preparedness, efforts were made before, during and around the NATO Summit to strengthen various aspects of digital resilience. Considerable attention was also given to non-technical measures, such as public–private cooperation. All these efforts aimed not only to keep the NATO Summit secure, but also to reap the benefits afterward.

Cyberattacks affect all levels of society – major incidents expose vulnerabilities

Edge devices remain attractive to malicious actors

The CSAN 2024 stated that malicious actors are increasingly targeting edge devices. This reporting period shows that such devices remain consistently attractive targets for malicious actors. A Dutch incident illustrating this was the exploitation of vulnerabilities in Citrix, for which the NCSC (again) warned about in July. This was linked to the incident at the Public Prosecution Service (OM) in July 2025. Due to these vulnerabilities, the OM decided to disconnect all systems from the internet and switch to emergency procedures. This affected the criminal justice chain, with lawyers reporting that they were unable to carry out their work effectively. In some cases, the disconnection caused immediate delays. In August 2025, the OM confirmed that unauthorised parties had gained access to its systems through a vulnerability. It is not known whether data were stolen or manipulated. The NCSC stated that several other Dutch organisations had also been successfully attacked and that one of the vulnerabilities had been exploited long before it was publicly disclosed.

Cyberattacks on the telecom sector illustrate malicious interest in critical infrastructure

Cyberattacks by both state actors and cybercriminals affect all levels of society, including critical infrastructure. The CSAN 2024 already described a range of cyberattacks that affected organisations in critical sectors in Western countries. During this reporting period, cybersecurity companies and government bodies again observed attacks demonstrating the continuing interest of malicious actors in critical infrastructure. Worldwide, several attacks on the telecom sector were observed in the past period. Some of these attacks were long-lasting and showed that malicious actors had already been present in the systems for an extended time. A notable example is the series of attacks by the Chinese hacker group Salt Typhoon on (primarily) telecom companies, in which large providers in the United States were compromised for a prolonged period (see Chapter 3 for further detail). In the Netherlands, the group compromised routers belonging to smaller internet service and hosting providers. As far as is known, the hackers did not penetrate the internal networks. The telecom sector is an attractive target for state actors, partly because of the volume of sensitive and other data involved (see Chapter 3). Cybercriminals also carry out attacks on the sector. A new ransomware group, for example, claimed responsibility for an attack on the US telecom company WideOpenWest. The criminals reportedly gained control of critical systems and stole data. There were also examples of cyber incidents at telecom companies in Europe. Both Orange and Bouygues (in France), for instance, reported that they had fallen victim to cyberattacks. As further details about these attacks are unknown, the party responsible and their motives remain unclear.

Largest cryptocurrency theft ever, reportedly by North Korean state hackers

North Korea is a state actor whose offensive cyber programme focuses on both espionage and financial gain. Incidents frequently occur in which North Korean actors carry out financially motivated attacks. The profits from these operations help North Korea to evade international sanctions and sustain its regime. Dutch victims are also among those affected. Cryptocurrency exchanges and companies in that sector are favoured targets – attacked obviously not only by state hackers but also by cybercriminals. A striking example this period was the cyberattack on ByBit, in which allegedly North Korean (state) hackers stole nearly 1.5 billion US

[II] The abbreviation APT stands for Advanced Persistent Threat: an ongoing threat from a sophisticated adversary, such as state actors or cybercriminals. An APT differs from other digital threat actors in terms of its capabilities, the length of time invested, its motive, persistence and sometimes the methods chosen by the attacker. Unique APTs are often given specific names within the cybersecurity community. These may consist of APT followed by a number, or code names such as Fancy Bear or Forest Blizzard.

dollars in digital currency. This is, at the time of writing, the largest cryptocurrency theft ever recorded.

International actions against malicious actors and their infrastructure

International operations disrupt cyber-criminal infrastructure

During this reporting period, several large-scale international operations took place in which investigative authorities around the world disrupted criminal infrastructure. In 2025, Operation Endgame was carried out once again.[7] During this coordinated international operation, investigative authorities dismantled several botnets[III] used for large-scale cyber crime. More than 300 servers were taken offline worldwide, including 60 in the Netherlands. In addition, Operation Magnus, led by the Dutch Police and the Public Prosecution Service (OM), focused on dismantling infostealers –[8] malware that steals sensitive information, such as login credentials, from victims. Operation PowerOFF, coordinated in part by the Dutch Police and the OM, targeted providers and users of DDoS-for-hire services.[9] The proxy service Anyproxy was also taken offline under Operation Moonlander.[10] Cybercriminals used this platform for phishing, ransomware attacks, data theft and the like. Part of the Anyproxy infrastructure was hosted in the Netherlands. Finally, in an international operation coordinated by the Dutch Police and the OM with the United States and Finland, what is known as a Counter Antivirus (CAV) service was taken offline.[11] Such a CAV service allows malware developers to test whether their malware is detected by various antivirus programmes. The service taken down was AVCheck, one of the largest CAV platforms used internationally by cybercriminals.

The Netherlands plays an important role in international cooperation and focuses on information sharing and offender prevention

The Netherlands contributes actively to international cooperation against cyber threats. In 2025, the Dutch Fiscal Intelligence and Investigation Service (FIOD), the German Federal Criminal Police Office (BKA), Europol and the cybersecurity firm zeroShadow dismantled a server network in Germany that was being used to launder cryptocurrency stolen by North Korea. The operation led to the seizure of €34 million in cryptocurrency.[12]

The Dutch government works with public and private organisations, both nationally and internationally, to promote information sharing. The Melissa partnership focuses on combating ransomware attacks by pooling, sharing and jointly applying technical, legal and operational expertise and resources. The partners in this collaboration contributed to Operation Endgame and the investigation into a CAV service.

The Dutch Police are investing in offender prevention together with public and private partners[IV]. Foreign police organisations are also being encouraged to engage in offender prevention. The Dutch Police launched the International Cybercrime Offender Prevention network (InterCOP), a collaborative initiative that now includes 37 countries. [13] As part of the investigation into the CAV service, the Dutch Police carried out broad interventions. For example, a fake login page was placed online to reach, warn and deter AVCheck users. In the previously mentioned Operations Endgame and PowerOFF, alternative interventions were also deployed with the aim of disrupting and/or deterring offenders.

Individuals and groups arrested, convicted and/or placed on sanctions lists

During this reporting period, several individuals and groups were sanctioned, convicted and/or arrested. As part of Operation Endgame, twenty cybercriminals were added to Europe's Most Wanted Fugitives list.[14] Under Operation Magnus, the United States indicted an administrator of an infostealer, and the Belgian Police arrested two individuals.[15] An international operation coordinated by Europol and Eurojust targeted both the perpetrators and the underlying infrastructure of the pro-Russian hacker group NoName057(16). Over the past few years, NoName057(16) has carried out numerous digital attacks against countries that support Ukraine, including the Netherlands. Two people have been arrested, arrest warrants have been issued for eight others, and more than a thousand supporters of the group have been notified that they are under investigation. More than one hundred servers used by the group to conduct DDoS attacks have been taken offline.[16] Despite these actions, NoName057(16) remains active. The group has formed new alliances with other pro-Russian hackers and continues its attacks, targeting political parties, government bodies, transport companies and police forces across several European countries.[17]

For the first time in the Netherlands, this reporting period saw the conviction of a hosting provider found guilty of facilitating a botnet.[18] [19] The servers involved were seized and destroyed.

The Police and the Public Prosecution Service (OM) have also strengthened cooperation with the Netherlands Authority for Consumers & Markets (ACM). The ACM has been designated as the supervisory authority for compliance with the obligations arising from the Digital Services Act (DSA). These obligations for hosting providers under the DSA include responding promptly and adequately to orders and Notice and Takedown requests. Such obligations apply to all hosting providers within the European Union (EU). The Police, the OM and the ACM will work closely together to tackle bad hosting. The same applies to the Authority for the Prevention of Online Terrorist Content and Child Sexual Abuse Material (ATKM), with which there will also be cooperation to tackle bad hosting.

As stated in the CSAN 2024, two cybercriminals were placed on the European sanctions list for the first time in late June 2024 at the initiative of the Netherlands. The EU recently extended these sanctions for another three years.[20] In December 2024, the EU added the Russian state hacker unit GRU 29155[V] to the sanctions list. In September 2024, the MIVD had already warned about the activities of this unit, which were reportedly aimed at identifying and disrupting Western support for Ukraine.[21] On 27 January 2025, a further three Russian individuals belonging to GRU 29155 were added to the EU sanctions list for their involvement in cyberattacks on Estonia.[22] [23]

In 2025, the EU imposed sanctions on the web hosting provider Stark Industries and the two individuals who run the company for enabling 'destabilising activities' against the EU. As a result, PQ Hosting was also indirectly sanctioned.[24] These sanctions mean that the individuals concerned are banned from entering the EU, their assets are frozen, and EU citizens and companies are prohibited from doing business with the sanctioned entities and individuals. This marks an important step towards a safer cyber domain.

[III] The term botnet (derived from 'robot network') is used for a collection of computers on which malware is installed without the owners being aware of it. These infected computers (bots) form a network and are centrally controlled through a server. For example, a botnet can be used to forward unwanted email (spam) or to carry out DDoS attacks.

[IV] Offender prevention looks at (1) deterring potential offenders and (2) trying to redirect them towards positive and legal choices.

[V] The GRU, also abbreviated as GROe, is Russia's military intelligence service. 29155 refers to a specific unit within that organisation.

2024

July 2024

Inland

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

Abroad

- Russian state hackers carry out cyberattacks on the Olympic Games

August 2024

Inland

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

September 2024

Inland

- Data of police employees stolen in cyberattack by a very likely Russian state-sponsored actor
- Company data stolen at Fortinet after cyberattack

October 2024

Inland

- Dutch government websites temporarily offline after DDoS attacks by pro-Russian hackers
- Appointments cancelled after outage affecting several municipalities in Gelderland following software update
- Critical vulnerability in FortiManager exploited worldwide
- Data stolen in phishing attack on the municipality of Velsen
- Thousands of email addresses leaked after hack of employee at Combinatie Jeugdzorg

Abroad

- Websites of critical infrastructure and the Cypriot government temporarily disrupted by coordinated cyberattacks from pro-Palestinian groups
- European healthcare institutions targeted with ransomware
- European governments and military organisations targeted by Russian phishing attacks

November 2024

Inland

- Data stolen after large-scale exploitation of critical vulnerability in Cleo file transfer software
- Data stolen at Ahold Delhaize after ransomware attack

Abroad

- German pharmaceutical wholesaler's processes disrupted by ransomware attack

December 2024

Inland

- Municipal data leaked after cyberattack on software supplier

Abroad

- 680 gigabytes of data stolen from Blue Yonder by ransomware group
- Chinese hackers compromise US telecom infrastructure
- Customers of Danish water treatment company left without water after cyber sabotage by pro-Russian hackers

2025

January 2025

Inland

- Communication problems at emergency services due to hours-long nationwide C2000 system outage
- No classes and exams postponed after cyberattack on Eindhoven University of Technology
- DigiD unavailable due to outage caused by DDoS attack
- Three consecutive days of (internet) disruptions at educational institutions and hospitals caused by DDoS attacks
- Patient appointments cancelled and surgeries postponed due to computer outage at Rijnstate Hospital
- Personal data of 2,200 users leaked after attack on Almere council website
- Embassies in European countries, including the Netherlands, targeted by suspected Russian hackers

Abroad

- Location data of potentially millions of people leaked after hack at data broker
- Data stolen in ransomware attack on Italian hospital, but systems not encrypted

February 2025

Inland

- Paragon spyware used against European WhatsApp users, including Dutch numbers
- Police number 0900-8844 temporarily unavailable due to outage

Abroad

- Systems of Canadian telecom companies compromised

March 2025

Inland

- DigiD intermittently unavailable due to recurring DDoS attacks
- Criminal court hearings disrupted during recovery work after Public Prosecution Service outage
- Dutch companies targeted by North Korean hackers

Abroad

- 1.5 billion US dollars in cryptocurrency stolen by North Korean hackers

April 2025

Inland

- DigiD partly unavailable due to DDoS attacks
- Data breach at ministries due to incorrect uploading of documents, impact unclear
- Payment disruptions caused by DDoS attacks on Adyen
- Over fifty Dutch websites briefly inaccessible due to DDoS attacks

Abroad

- Walloon government disconnects from the internet after targeted cyberattack
- APT29 conducts phishing attacks on diplomatic entities in Europe
- Pro-Russian hackers manipulate water flow at Norwegian dam

May 2025

Inland

- The Netherlands (in)directly targeted in cyber-espionage operations by Russian state hackers

Abroad

- Empty supermarket shelves in the United Kingdom after cyberattack

June 2025

Inland

- Dutch organisations targeted by DDoS attacks, limited impact
- International Criminal Court targeted by cyberattack

July 2025

Inland

- Criminal justice chain disrupted after Public Prosecution Service took network offline due to Citrix vulnerability
- Organisations worldwide compromised through SharePoint vulnerability, Dutch organisations also affected

Abroad

- Disruption of services for French Orange customers after cyberattack
- Nationwide 4G and 5G outage in Luxembourg after cyberattack
- Data stolen from Orange Belgium after cyberattack

August 2025

Inland

- Sensitive citizen data leaked after ransomware attack on laboratory
- Operations of institutions in the Caribbean disrupted by cyber incidents
- KLM data stolen after attackers gained access through external platform
- Routers of internet service and hosting providers compromised by Salt Typhoon

Abroad

- Data 6.4 million French Bouygues Telecom customers stolen in cyberattack
- Data stolen from major companies after attacks on CRM systems
- Data stolen and business operations disrupted after cyberattack on telecom company Colt
- Large-scale data theft from Salesforce environments after breach at Salesloft Drift
- Jaguar Land Rover production and services disrupted for weeks following cyberattack

Notable incidents in the Netherlands

July 2024

Air traffic, healthcare and others disrupted by global computer failure due to faulty update
On 19 July, CrowdStrike introduced a software update that rendered approximately 8.5 million Windows systems unusable worldwide.[25] The error caused 'Blue Screens of Death' on Windows systems.[26] 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).[27][28] 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 failure. The problems were caused by how access was being provided to the Netherlands Armed Forces Integrated Network (NAFIN). 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. The IT failure also affected DigiD.[29] NAFIN is a heavily secured network that connects Defence locations, among others, and is also used at data centres of various ministries and police stations. An error in the software caused a time synchronisation issue on the network.[30] The evaluation of the outage shows that insufficient attention was paid to cyber risks and to the wider social impact.[31]

September 2024

Data of police employees stolen in cyberattack by a very likely Russian state-sponsored actor
At the end of September, the Police fell victim to a hack in which the contact details of police employees were stolen. Hackers obtained data from all police employees through the global address list. Private information was also stolen in some cases.[32] The attackers used what is known as a pass-the-cookie attack.[VI] In May 2025, the intelligence services announced that a very likely Russian state-sponsored cyber actor, known as Laundry Bear, was responsible for the attack. In addition to the attack on the National Police, the group also targeted other organizations worldwide, including in the Netherlands. [33]

Company data stolen at Fortinet after cyberattack
Fortinet confirmed that it had been the victim of a cyberattack in which the hacker claimed to have stolen both customer and company data. According to the attacker, 440 GB of data were stolen from a Microsoft Azure SharePoint server. The criminal reportedly demanded a ransom from Fortinet, but the company did not pay it. Fortinet stated that the incident affected less than 0.3 per cent of its customer base and did not result in malicious activity targeting customers.[34] Research by the NCSC found that the impact on the Netherlands was limited.[35]

[VI] In a pass-the-cookie attack, hackers steal session cookies to take over accounts.

October 2024

Dutch government websites temporarily offline after DDoS attacks by pro-Russian hackers
Several Dutch government websites were temporarily unavailable due to a DDoS attack. A pro-Russian hacktivist group claimed responsibility for the attack.[36]

Appointments cancelled after outage affecting several municipalities in Gelderland following software update
A major technical outage prevented residents of Nijmegen, Beuningen, Berg en Dal, Wijchen, Druten and Heumen from accessing their municipalities. All appointments were cancelled. An update of authentication software caused the outage. The municipalities ruled out a hack.[37]

Critical vulnerability in FortiManager exploited worldwide
A critical vulnerability in Fortinet's FortiManager management tool was exploited worldwide. In many cases, configuration files were stolen that included hashed user passwords.[38] The exploitation had been taking place since June 2024, before a patch became available. Research by the NCSC showed that vulnerable systems in the Netherlands were also accessible from the internet. The NCSC and sectoral partners informed the affected organisations.

Data stolen in phishing attack on the municipality of Velsen
The municipality of Velsen fell victim to a phishing attack. The phishing email in question was sent from a well-known and trusted organisation, causing a municipal employee to open it. As a result, email addresses of 327 residents of Velsen were stolen, along with several internal addresses and telephone numbers.[39]

Thousands of email addresses leaked after hack of employee at Combinatie Jeugdzorg
A hacker stole thousands of email addresses from care institutions and other companies working with the Eindhoven-based organisation Combinatie Jeugdzorg. Client email addresses were also leaked. According to Combinatie Jeugdzorg, only email addresses were involved, and as far as is known, no other personal information was taken. The perpetrator of the hack remains unknown.[40]

November 2024

Data stolen after large-scale exploitation of critical vulnerability in Cleo file transfer software
Malicious actors exploited vulnerabilities in the Cleo file transfer software. The cyber-criminal group Clop is believed to have been responsible for the attacks, stealing data from dozens of organisations.[41] The criminals also stole data from the Dutch company Centric. According to the company, they gained access to a test server containing privacy-sensitive data from one client –[42] specifically, data relating to 24 current or former residents of the municipality of Amersfoort.[43]

Data stolen at Ahold Delhaize after ransomware attack
A hacker collective claimed to have carried out a ransomware attack on Ahold Delhaize, reportedly stealing 6 terabytes of data in the process.[44] Although initial reports suggested that the stolen data concerned American records, later findings showed that data from existing and former Dutch employees were also taken.[45] Subsequent reports indicated that the personal data of approximately 2.2 million people were affected.[46]

December 2024

Municipal data leaked after cyberattack on software supplier
Several municipalities reported that personal data of their residents had been leaked following an attack on an external supplier. The incident involved a ransomware attack. The municipality of Amersfoort reported that data of 100,000 current and former residents had been leaked.[47] The municipality of Arnhem reported data breaches affecting dozens of residents. [48] The municipalities of Tubbergen and Dinkelland also reported data breaches, although the number of affected individuals remains unknown.[49]

January 2025

Communication problems at emergency services due to hours-long nationwide C2000 system outage
The C2000 system was unavailable for several hours on New Year's Eve. The outage affected the EOCS, which allows control room operators to speak with emergency responders in the field. Thanks to the availability of the backup system, operators were still able to communicate with responders. However, officers said the backup system was practically unusable and communication was very difficult.[50] In addition to the C2000 failure, the emergency button on police radios also malfunctioned.[51]

No classes and exams postponed after cyberattack on Eindhoven University of Technology
In early January, Eindhoven University of Technology (TU/e) suffered a cyberattack. The university took its systems offline for a week, halting all teaching activities. Exams were therefore postponed.[52] TU/e later published the findings of its investigation, which showed that attackers had been active on the network for five days. They had exploited leaked account credentials to log in via the VPN connection.[53]

DigiD unavailable due to outage caused by DDoS attack
This month, DigiD was temporarily unavailable for several days as a result of DDoS attacks.[54] No further details about the attacks have been released.

Three consecutive days of (internet) disruptions at educational institutions and hospitals caused by DDoS attacks
For three days in a row, educational institutions and hospitals experienced (internet) disruptions caused by DDoS attacks on SURF. As a result, educational institutions across the Netherlands faced slow or unavailable connections.[55] Several hospitals were also affected by the DDoS attacks.[56]

Patient appointments cancelled and surgeries postponed due to computer outage at Rijnstate Hospital
On 14 January, a computer outage forced Rijnstate Hospital to cancel all appointments, scheduled surgeries and examinations at three branches. Staff were unable to save new data in the electronic patient records, prompting the hospital to suspend all non-urgent care. The problem is believed to have occurred after running software updates.[57]

Personal data of 2,200 users leaked after attack on Almere council website
Personal data belonging to 2,200 users of the website raadvanalmere.nl were leaked following a cyberattack. The website was taken offline afterwards. The leaked data reportedly included names, email addresses, and in some cases phone numbers and information about the users' residential areas.[58]

Embassies in European countries, including the Netherlands, targeted by suspected Russian hackers
Researchers at Bitdefender observed a digital espionage campaign believed to have been carried out by Russian hackers. Embassies in several European countries, including the Netherlands, Germany and Romania, were targeted.[59]

February 2025

Paragon spyware used against European WhatsApp users, including Dutch numbers
Italian authorities reported that seven WhatsApp users with Italian phone numbers were targeted with the Paragon spyware. Users from more than a dozen other European countries were also targeted by the commercial spyware, including Dutch, German and Belgian numbers. This suggests that the users are based in those countries, although their identities have not been disclosed. It is not known how many Dutch numbers were targeted or whether the spyware attacks were successful.[60] WhatsApp stated that around 90 users were targeted in total, including journalists.[61]

Police number 0900-8844 temporarily unavailable due to outage
On 25 February, the national police number 0900-8844 was temporarily unavailable due to a technical outage. An alternative number was made available for non-urgent matters. The emergency number remained accessible. The cause of the outage has not been disclosed.[62]

March 2025

DigiD intermittently unavailable due to recurring DDoS attacks
Throughout the month, DigiD experienced repeated disruptions caused by DDoS attacks.[63] As a result, DigiD, DigiD Machtigen, BSN, Digipoort and MijnOverheid were only partly accessible.[64] Logius attributed the disruptions to more sophisticated DDoS attacks.[65]

Criminal court hearings disrupted during recovery work after Public Prosecution Service outage
At the end of March, the Public Prosecution Service (OM) temporarily disconnected its entire IT environment from the internet. The cause was initially unclear but was later found to be a 'persistent outage'. During recovery work, employees were unable to log in, and court hearings were disrupted. Some hearings could not go ahead or had to be rescheduled.[66]

Dutch companies targeted by North Korean hackers
According to a report by CrowdStrike, the North Korean hacker group Famous Chollima also targeted Dutch companies.[67] The names of the affected companies were not disclosed, but CrowdStrike stated that most of the attacks were directed at the tech sector. The company observed more than 300 incidents by this group in 2024, 40 per cent of which involved insider threats. It is unclear how many of these incidents occurred in the Netherlands; the majority of attacks were aimed at the United States.

April 2025

DigiD partly unavailable due to DDoS attacks
DigiD services were again partly unavailable this month as a result of DDoS attacks. It is not known who was responsible for the attacks.[68]

Data breach at ministries due to incorrect uploading of documents, impact unclear
Several ministries in The Hague suffered a data breach. The problem arose in internal processes when metadata were not properly removed during the conversion of documents to a publication format. As a result, personal data of civil servants could be traced.[69]

Payment disruptions caused by DDoS attacks on Adyen
Payment company Adyen was hit by multiple DDoS attacks, causing payment problems for customers in shops, online retailers and the hospitality sector.[70]

Over fifty Dutch websites briefly inaccessible due to DDoS attacks
At the end of April, at least 57 Dutch websites experienced problems following DDoS attacks. Among those affected were the websites of the municipalities of Apeldoorn, Nijmegen, Breda and Tilburg, which were temporarily offline. Pro-Russian hacktivists claimed responsibility for the attacks, who mainly targeted government websites. Other affected sites included those of GVB, Arriva and NRC.[71]

May 2025

The Netherlands (in)directly targeted in cyber-espionage operations by Russian state hackers
Investigations by several organisations, including the MIVD, showed that Russian state hackers – known as APT28 – carried out cyberattacks against Ukraine and NATO member states. The Dutch armed forces, ministries and business sector were both direct and indirect targets of these espionage operations. The aim of the attacks included mapping and disrupting Western (military) support for Ukraine.[72]

June 2025

Dutch organisations targeted by DDoS attacks, limited impact
In the run-up to the NATO Summit, around ten organisations in the Netherlands were targeted by DDoS attacks. [73] The affected organisations were mainly public bodies that had a role in the summit. Among them were the NATO headquarters in the Netherlands and Notubiz, which provides the Council Information System used by municipalities and provinces to publish official documents. As a result, pages containing council and provincial documents on various municipal and provincial websites were less accessible than usual.[74] The pro-Russian hacker group NoName057(16) claimed responsibility for some of the attacks.

International Criminal Court targeted by cyberattack
At the end of June, the International Criminal Court (ICC) was the target of a 'sophisticated and targeted' cyberattack. The ICC did not disclose whether sensitive information was stolen or who was behind the attack but stated that the attack had been stopped in time.[75]

July 2025

Criminal justice chain disrupted after Public Prosecution Service took network offline due to Citrix vulnerability
On Thursday 17 July, the Public Prosecution Service (OM) disconnected its systems from the internet following a warning about vulnerabilities in Citrix NetScaler.[76] As a result, the OM had to switch to emergency procedures to continue its operations. This caused disruption within the criminal justice chain, with some cases facing immediate delays.[77] In early August, the OM gradually reconnected its systems to the internet. The investigation showed that unauthorised parties had gained access to the OM's Citrix NetScaler systems. So far, there is no evidence that data were stolen or altered.[78] The NCSC stated that several critical Dutch organisations had been successfully attacked through one of the Citrix vulnerabilities, and that one of the flaws had been exploited long before it was publicly disclosed.[79] The Custodial Institutions Agency also launched an investigation after indications that the same vulnerabilities had been exploited.[80]

Organisations worldwide compromised through SharePoint vulnerability, Dutch organisations also affected
Critical vulnerabilities in Microsoft SharePoint were exploited both by state actors and for ransomware attacks.[81] Vulnerable systems were found at several Dutch and foreign organisations. The presence of a vulnerability in a system does not necessarily mean it was exploited.[82] Media reports indicated that hundreds of servers were compromised by attackers, with four per cent of the infections observed in the Netherlands.[83]

August 2025

Sensitive citizen data leaked after ransomware attack on laboratory
After Bevolkingsonderzoek Nederland reported a data breach, Clinical Diagnostics (Eurofins) confirmed in August that sensitive patient data had been stolen from healthcare providers that had commissioned tests from the laboratory. The incident occurred during a ransomware attack in July. Bevolkingsonderzoek Nederland notified 941,000 individuals that their data may have been stolen in the attack. However, the breach extends beyond that organisation. Patient data from tests commissioned by other healthcare institutions, such as hospitals and GP practices, were also affected.[84] Cybercriminals claimed to have stolen 300 GB of data, part of which appeared online. RTL's analysis showed that the leaked information included patients' names, home addresses, dates of birth, citizen service numbers, and medical test results and findings. Advice issued as a result of the tests was also among the stolen data. The stolen data further contained information about politicians, prisoners, people detained under hospital orders and women living in domestic abuse shelters.[85] The hacker group demanded ransom, threatening to publish the stolen data. They later issued another ransom demand and threatened to publish the stolen data, claiming that previous agreements had not been honoured, before retracting the threat.[86] Clinical Diagnostics reportedly paid a ransom initially to prevent further data leaks by the criminals, but the amount paid has not been disclosed.[87] At the time of writing, investigations into the attack's modus operandi and underlying causes are ongoing.

Operations of institutions in the Caribbean disrupted by cyber incidents
Several organisations in the Caribbean part of the Kingdom of the Netherlands experienced operational disruptions due to cyber incidents. Among others, the Curaçao Tax and Customs Administration was affected by a ransomware attack. One of its systems was taken offline when the hack was discovered. The Joint Court of Justice, which operates on all six islands, also discovered malicious software within its IT systems and subsequently took them offline.[88]

KLM data stolen after attackers gained access through external platform
Attackers stole KLM data, possibly including customer names and contact details, after gaining access to an unspecified 'external platform' used by the airline for customer service. The platform is believed to have been Salesforce. The number of affected customers has not been disclosed.[89]

Routers of internet service and hosting providers compromised by Salt Typhoon
Investigations by the AIVD and MIVD found that Chinese hackers had gained access to routers belonging to smaller Dutch internet service and hosting providers. As far as is known, the hackers did not penetrate internal networks. The attacks were attributed to the group known as Salt Typhoon and formed part of a large-scale global campaign. Major telecom providers in the Netherlands were not affected.[90]

Notable incidents abroad

July 2024

Russian state hackers carry out cyberattacks on the Olympic Games
According to the French Ministry of Foreign Affairs, the Russian military intelligence service was behind a series of cyberattacks in France, including an attack on a sports organisation involved in organising the 2024 Olympic and Paralympic Games. The group APT28 was held responsible for these attacks. Several ministries, companies in the defence industry and organisations in the financial sector were also reportedly targeted by the Russian hackers.[91]

October 2024

Websites of critical infrastructure and the Cypriot government temporarily disrupted by coordinated cyberattacks from pro-Palestinian groups
Critical infrastructure and government websites in Cyprus were targeted by a series of coordinated cyberattacks claimed by several pro-Palestinian hacker groups, including LulzSec Black.[92] According to the authorities, most of the attacks were unsuccessful. The targeted organisations including banks, airports and government websites were only temporarily disrupted. Various attack techniques were observed, including DDoS attacks. The operation was reportedly carried out in response to Cyprus's support for Israel.

European healthcare institutions targeted with ransomware
According to Orange Cyberdefense, European healthcare institutions were targeted with ransomware between June and October 2024 through a vulnerability in CheckPoint security gateways.[93] Orange Cyberdefense did not disclose how many healthcare institutions were affected or what the impact of the attacks was.

European governments and military organisations targeted by Russian phishing attacks
European governments and military organisations were targeted in a phishing campaign that Google attributed to a Russian-linked actor tracked as UNC5837. The campaign used signed .rdp file attachments to establish Remote Desktop Protocol (RDP) connections from the victims' computers. [94]

November 2024

German pharmaceutical wholesaler's processes disrupted by ransomware attack
The German pharmaceutical wholesaler AEP was hit by a ransomware attack that encrypted part of its IT systems.[95] Once the attack was detected, all external connections were cut and the affected systems were shut down. As a result, customers were unable to place orders and pharmacies were only partially supplied. AEP, which serves more than 6,000 pharmacies, was unreachable by phone and only very limitedly by email following the attack.

December 2024

680 gigabytes of data stolen from Blue Yonder by ransomware group
The ransomware group Termite claimed responsibility for an attack on the software company Blue Yonder.[96] The Software-as-a-Service (SaaS) provider serves more than 3,000 clients, including Microsoft, Renault, Lenovo, Procter & Gamble and Carlsberg. The company also has Dutch customers, including Jumbo and Hema.[97] Customers in several countries experienced the effects of the incident, though it did not cause major disruptions. Businesses mainly faced problems with their payment and planning systems. Customers and employees of the Jumbo and Hema were not inconvenienced. Blue Yonder did not specify how many customers were affected by the attack. Termite claimed to have stolen around 680 gigabytes of data, including documents, mailing lists, database dumps and insurance files.

December 2024

Chinese hackers compromise US telecom infrastructure
Chinese hackers from the group Salt Typhoon had access to the networks of several US telecom providers for at least a year.[98] According to US authorities, the affected companies included T-Mobile, Verizon, AT&T and Lumen Technologies. [99] The hackers reportedly obtained call data of prominent politicians.[100] CISA and the FBI confirmed that the hackers accessed the private communications of a 'limited number' of people. Media reports, citing anonymous sources, stated that the attackers also accessed the US government's wiretapping platform and stole law enforcement request records and customer call data.[101] The campaign is believed to have been ongoing for one to two years, and it is uncertain whether the hackers have been fully removed from the systems.

Customers of Danish water treatment company left without water after cyber sabotage by pro-Russian hackers
According to Danish authorities, pro-Russian hackers attacked a Danish water treatment company in late December 2024, leaving customers without water for several hours. One of the pipelines burst due to increased water pressure.[102]

January 2025

Location data of potentially millions of people leaked after hack at data broker
Following a hack at Gravy Analytics, a commercial data broker, location data of potentially millions of people were leaked.[103] Gravy Analytics discovered that an attacker had gained access to its cloud environment using a stolen key. Online, someone claimed responsibility for the intrusion, stating they had stolen a dataset containing 17 terabytes (TB) of information. The dataset allegedly included location data of users from hundreds of popular apps – such as Candy Crush, FlightRadar, Grindr and Tinder. The hacker threatened to release the data publicly if the company refused to pay the demanded ransom.

Data stolen in ransomware attack on Italian hospital, but systems not encrypted
An Italian hospital was targeted in a ransomware attack that exploited a firewall vulnerability, resulting in the theft of personal data belonging to patients and staff.[104] Through the compromised firewall, the attackers obtained domain credentials, which gave them access to the file server. The server contained health data, although it was intended only for administrative use. The incident was limited to data theft, as the ransomware itself was never activated.

February 2025

Systems of Canadian telecom companies compromised
In February, the Canadian Centre for Cyber Security reported malicious activity affecting several Canadian telecommunications companies. The activity was attributed specifically to the Chinese cyber actor Salt Typhoon. According to the Canadian government, the systems were compromised through a known Cisco vulnerability. The authorities did not specify which telecom companies were affected.[105]

March 2025

1.5 billion US dollars in cryptocurrency stolen by North Korean hackers
Nearly 1.5 billion US dollars in digital currency were stolen in a hack on the cryptocurrency exchange Bybit, making it the largest cryptocurrency theft ever recorded. Several investigators and US authorities have attributed the attack to North Korean hackers.[106] Experts from several firms quickly reported that the Lazarus Group had already laundered at least 300 million US dollars of the stolen funds.[107]

April 2025

Walloon government disconnects from the internet after targeted cyberattack

The Walloon government disconnected its systems from the internet after detecting a large-scale, ‘sophisticated and targeted intrusion’ in its IT environment.[108] The attacker, whose identity remains unknown, is believed to have exploited a vulnerability in the government’s systems. To prevent (further) impact from the attack, the authorities decided to take the systems offline, which resulted in several administrative services being unavailable.

APT29 conducts phishing attacks on diplomatic entities in Europe

According to the cybersecurity company Check Point, the Russian hacker group APT29 conducted a months-long phishing campaign targeting European diplomatic entities. The attackers sent fake invitations to wine tastings and dinners, purportedly from a European ministry of foreign affairs.[109] The campaign appears to have focused on European diplomatic missions, including embassies of non-European countries located in Europe.

Pro-Russian hackers manipulate water flow at Norwegian dam

Norwegian authorities believe pro-Russian hackers were behind suspected sabotage at a dam in Bremanger, Norway. During the incident, the hackers interfered with the dam’s water flow by gaining access to a digital system that remotely controls one of its valves. They opened the valve to increase the flow of water, which remained open for around four hours and released millions of litres of water. The incident did not pose a danger to the surrounding area.[110]

May 2025

Empty supermarket shelves in the United Kingdom after cyberattack

Parts of the IT systems of the British supermarket chain Co-op were taken offline after a ransomware attack was detected. The company reported that the incident disrupted its operations, causing empty shelves in some stores.[111] Before encrypting Co-op’s systems with ransomware, the attackers had stolen data belonging to 6.5 million customers.[112] The attack on Co-op was part of a broader campaign targeting the UK retail sector, with Marks & Spencer and Harrods also falling victim to cyberattacks. According to the UK Cyber Security Monitoring Centre, the financially motivated cyber actor Scattered Spider[VII] was behind the campaign.[113] The group is known for using telephone-based phishing (vishing) tactics, in which they impersonate IT staff.[114]

July 2025

Disruption of services for French Orange customers after cyberattack

Orange, one of the largest mobile service providers in both Europe and Africa, announced that it had detected a cyberattack affecting one of its internal systems. The company immediately took measures, including isolating affected systems. This led to service disruptions for certain business clients and some consumer services, mainly in France.[115] The criminals behind the WarLock ransomware are also believed to have stolen data in the attack.[116]

Nationwide 4G and 5G outage in Luxembourg after cyberattack

On 23 July, Luxembourg’s 4G and 5G mobile networks were unavailable for more than three hours. Large swathes of the population were unable to contact emergency services because the 2G backup network became overloaded. Internet access and online banking were also unavailable. According to statements by the government to the national parliament, the outage was caused by a cyberattack. The attack was described as deliberately disruptive rather than an attempt to compromise the telecom infrastructure.[117]

Data stolen from Orange Belgium after cyberattack

Telecom provider Orange Belgium suffered a cyberattack at the end of July. According to the company, unauthorised individuals gained access to ‘one of the IT systems’. The hackers reportedly accessed 850,000 customer accounts, leaking names, phone numbers, SIM card numbers and PUK codes, among other data.[118]

[VII] Media reports have emerged about the campaigns of financially motivated groups Scattered Spider and ShinyHunters. Some media have suggested that there is at least some overlap between the groups.

August 2025

Data 6.4 million French Bouygues Telecom customers stolen in cyberattack

French telecom provider Bouygues announced that it had detected a cyberattack on 4 August. The attack resulted in the theft of data belonging to 6.4 million customers, including contact details, business data and IBAN numbers.[119]

Data stolen from major companies after attacks on CRM systems

In July and August, several companies reported data breaches after attackers gained access to their Customer Relationship Management (CRM) systems. In several cases, the breaches involved Salesforce environments. Google confirmed that its Salesforce environment had been compromised following a telephone-based phishing (vishing) attack, resulting in the theft of data from potential Google Ads customers.[120] Cisco also disclosed that attackers had stolen personal data from users of cisco.com, one of which had gained access to a third-party CRM system through vishing.[121] These attacks on Salesforce CRM systems have been linked to the financially motivated group ShinyHunters[VIII].[122]

Data stolen and business operations disrupted after cyberattack on telecom company Colt

British telecommunications firm Colt Technology Services suffered a cyberattack in early August, leading to a multi-day outage affecting several business operations. The criminals behind the WarLock ransomware claimed responsibility for the attack and offered the stolen data for sale.[123]

Large-scale data theft from Salesforce environments after breach at Salesloft Drift

Investigators discovered a large-scale campaign in which hackers, tracked by Google as UNC6395, systematically exported vast amounts of data from corporate Salesforce environments. The attackers did not exploit a vulnerability in Salesforce itself but infiltrated its systems through Salesloft Drift, a third-party integration platform. By compromising Drift, the attackers stole Open Authorization and refresh tokens used for Salesforce integrations, which they then used to access Salesforce customer data.[124] According to Obsidian, more than 700 companies were affected.[125] It has been confirmed that the attackers stole data from, among others, the cybersecurity firms Zscaler, Palo Alto and Cloudflare.[126] [127]

Jaguar Land Rover production and services disrupted for weeks following cyberattack

British car manufacturer Jaguar Land Rover (JLR) announced that it had proactively shut down its systems after detecting a cyber incident.[128] The disruption halted production for several weeks, and employees were instructed to stay at home. On 10 September, JLR reported that some data had likely been affected but did not provide further details.[129] According to the BBC, responsibility for the attack was claimed in a Telegram channel named Scattered Lasus$ Hunters, and the hackers allegedly demanded ransom.[130]

[VIII] Media reports have emerged about the campaigns of financially motivated groups Scattered Spider and ShinyHunters. Some media have suggested that there is at least some overlap between the groups.

In early January, Eindhoven University of Technology (TU/e) was the victim of a cyberattack. As a result, systems were taken offline for a week, making it impossible to conduct any educational activities. Research by TU/e shows that attackers used leaked account details to log in via the VPN connection.

mf lecture rooms 1-9
shops & services
toilets
library · mf lecture room 10
commonroom • honors academy
mathematics & computer science
mf lecture rooms 11-15
health food wall
Did you know...
At this moment the TU/e has been hit by a cyber attack and all the systems, including the network connections, are shut down.
For more information and updates on the situation, please check the website. https://www.tue.nl
...Market Hall can be used as a Living Lab by TU/e students, researchers, and teachers?
Scan to learn more about Market Hall Living Lab and our other Living Labs >>>>>>
tue.nl/livinglabs

2 Increasingly complex threat assessment due to increasing cyber capabilities worldwide

Countries are increasingly willing to use power to advance their geopolitical interests. These developments are driving the further global expansion of cyber capabilities. States are deploying state-supported groups such as 'hacktivist' collectives and are also involving private companies and organisations to assist in state-led cyberattacks. In addition, more countries are developing offensive cyber programmes. This mixture and proliferation of actors are making threat assessment increasingly complex and unpredictable.

State cyber capabilities expanding and merging with non-state organisations

State actors use cyberattacks to achieve political, military or economic objectives. By developing offensive cyber programmes, they can pursue their interests (covertly) without crossing the legal threshold[IX] of armed conflict. Increasingly more countries are joining a race for knowledge, technology, weapons, control of raw materials and economic advantage – all factors that influence the global balance of power.[131] The world is increasingly in open conflict, and we are living in a turbulent period in which international relations are growing ever more unpredictable.[132] [133] As power dynamics shift, countries are more willing to use power to defend their own interests.[134] These geopolitical developments can contribute to the further growth and deployment of cyber capabilities worldwide.

Some state actors not only conduct cyberattacks themselves but also make sophisticated use of existing or newly formed collectives or organisations. In some cases, these are 'state-backed groups'. Such groups are not primarily part of state structures – they may include hacktivists or cybercriminals – but they may be tolerated, supported or directed by state actors. States rely on state-backed groups for several reasons. A key motive is plausible deniability: even when evidence suggests that a state was responsible for a cyberattack, it can shift the blame to another group that is officially outside state structures. This blending of actors means that a strict distinction between, for example, techniques or targets cannot

---

[IX] That is to say: below the threshold of what generally qualifies in international law as an 'armed conflict'.

always be made by actor type. The use of state-backed groups introduces several risks (see box below).

Risks of state-backed groups in the threat assessment

- State-backed groups may gain access to more resources from a state actor, thus increasing their capabilities.
- If it is not known that a group is state-backed, the threat it poses may be systematically underestimated because its true capabilities and intent are unclear.
- State-backed groups are generally less aware of potential risks, which may lead to unintended consequences, large-scale damage or escalation.

Pro-Russian hacktivists are an extension of the Russian state

Russia is a clear example of a state that frequently uses state-backed groups. The Russian threat manifests through a diffuse, opportunistic and unpredictable interplay between Russian government entities – including intelligence and security services – and a diverse network of Russian or pro-Russian individuals, organisations and groups active both in Russia and in the West. These actors are deployed, or volunteer themselves, to carry out often lucrative activities.[135] According to the MIVD and AIVD, the number of hacker collectives linked to the Russian regime has increased over the past two years, and the groups have become more diverse.

Some state-backed groups act in line with Russian state interests but appear to operate independently. This is particularly true for pro-Russian hacktivists. For a long time, the intelligence services assessed the threat posed by such hacktivists as low. In the first year of Russia's war against Ukraine, these groups carried out low-level cyber campaigns that, according to the MIVD and AIVD, were very unlikely to pose a threat to Dutch national security. In the second year of the war, however, several groups developed or acquired more advanced technical capabilities and showed a willingness to conduct impactful cyber operations. Since late 2023, the MIVD and AIVD have observed that these groups are increasingly willing to deploy offensive cyber capabilities against Western countries. The services have also determined that all the pro-Russian hacktivist groups they investigated maintain links with the Russian state, including the Russian intelligence and security services. Research by Pointer found that this includes the hacktivist group NoName057(16), which reportedly receives assistance from a Russian state censorship bureau operating under Kremlin supervision.[136] The cyber actor Laundry Bear, which the intelligence services identified as a new actor in 2025, is also highly likely to be state-backed.[137] This group was responsible, among other things, for the hack on the Dutch police (see Annual Review). Compared with some other Russian actors, Laundry Bear has proved particularly successful.[138]

The level of support these groups receive from the Russian state varies, meaning they exist on a spectrum – and can move along it. The AIVD and MIVD have visualised this spectrum as follows, see next page.

Because pro-Russian hacktivists should, in practice, be regarded as an extension of the Russian state and its intelligence and security services, the threat they pose is greater than previously assumed. If these hacktivists have access to the technical expertise of a state actor, for example, their capabilities – and therefore the potential impact of their cyberattacks – increase significantly. This means that the threat to the Netherlands from such hacktivist groups may be higher than was earlier assessed.

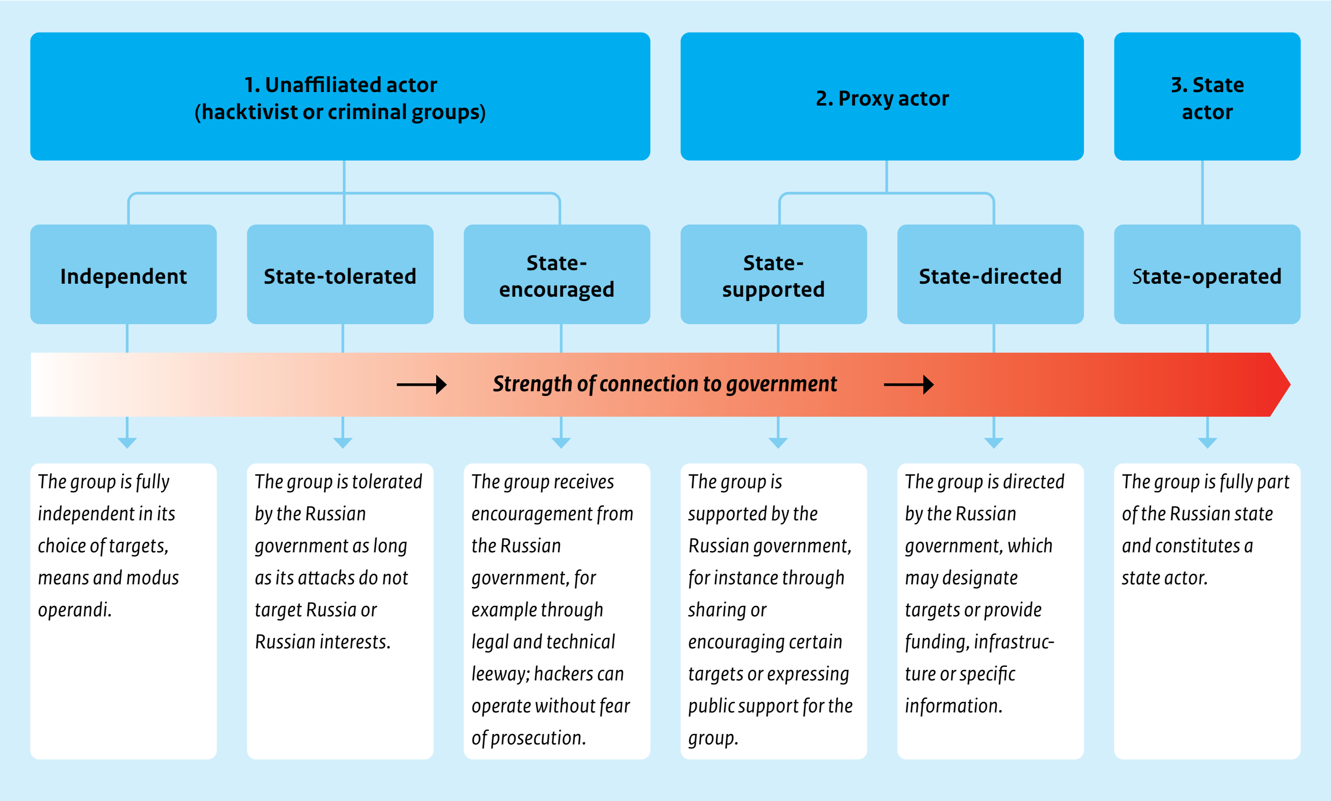
Chinese companies and knowledge institutions supporting Chinsese state cyber programmes

China increasingly relies on organisations outside the state apparatus. According to the AIVD and MIVD, China's cyber ecosystem shows tight links between intelligence and security services, knowledge institutions and companies. During the past reporting period, it emerged for the first time that a medium-sized, publicly listed Chinese company was directly involved in conducting cyber operations. Previously, investigators had identified other Chinese companies that ran offensive operations, but these were front organisations for the Chinese intelligence and security services or relatively small, obscure firms. Until now, large and mid-sized Chinese companies had mainly been seen providing support – for example, training, research and development, or supplying attack infrastructure, malware and exploits for known and unknown vulnerabilities. Chinese state actors also benefit from large-scale Chinese research programmes that identify vulnerabilities in edge devices. This helps them to hack Western governments and companies consistently and successfully. Growing attention to this modus operandi has not yet reduced the threat. The MIVD assesses that attackers can exploit edge-device vulnerabilities within hours or days of disclosure,[139] leaving (potential) victims very little time to apply patches before exploitation.

North Korean state hackers motivated by financial gain and targeting the cryptocurrency sector

North Korea is an example of a state actor that uses techniques and conducts attacks normally associated with non-state actors. While part of North Korea's cyber activity focuses on espionage, a large share is financially motivated – a motive generally linked to criminal cyber actors. The cryptocurrency sector is a particular target. This year, North Korean hackers reportedly stole nearly 1.5 billion US dollars in digital currency (see Annual Review). The country also deploys North Korean freelance IT workers who are hired abroad by companies under false identities to generate income for the regime, including through data theft or the misappropriation of cryptocurrency.[140] Over the past year, North Korea has also expanded its already highly advanced offensive cyber capabilities.[141] It has long been known that North Korean cyber actors steal cryptocurrency to fund the regime, but it remains notable that North Korea is the only state actor with such a developed offensive cyber programme that uses it on a large scale for financial gain. This also demonstrates that the boundaries between different actors and motives are not clear-cut; they can overlap.

Figure 1 Strength of connection to government



Independent	State-tolerated	State-encouraged	State-supported	State-directed	State-operated
The group is fully independent in its choice of targets, means and modus operandi.	*The group is tolerated by the Russian government as long as its attacks do not target Russia or Russian interests.*	*The group receives encouragement from the Russian government, for example through legal and technical leeway; hackers can operate without fear of prosecution.*	*The group is supported by the Russian government, for instance through sharing or encouraging certain targets or expressing public support for the group.*	*The group is directed by the Russian government, which may designate targets or provide funding, infrastructure or specific information.*	*The group is fully part of the Russian state and constitutes a state actor.*

Preparations for digital sabotage by Russia and China observed, but no disruptive attacks so far

During the past reporting period, both Russia and China were observed carrying out preparatory actions for digital sabotage. These activities have not had a disruptive impact in the Netherlands to date.

The MIVD reports that Russia is displaying an increased risk appetite, which is reflected in more brazen, aggressive and provocative actions in both the physical and cyber domains.[142] In the Netherlands, the AIVD and MIVD identified cyber operations and preparatory activities that could potentially have led to sabotage. In 2024, the Netherlands also fell victim to deliberate cyber sabotage by a Russian state-backed group for the first time.[143]

Chinese hacker groups have also taken steps that indicate preparations for sabotage. In the United States, two groups – Volt Typhoon and Salt Typhoon – have in recent years managed to infiltrate deeply into parts of US critical infrastructure (see Annual Review and Chapter 3). The stages of these cyber campaigns suggest preparatory activity for digital sabotage. This demonstrates that there is a broad Chinese cyber threat that extends beyond the traditional perception of China being focused solely on economic espionage. Some activities appear to involve non-economic espionage and may also be forward-looking: by embedding themselves within critical infrastructure, Chinese actors could later exploit those positions for sabotage, for example in times of conflict. China likely sees the United States as its primary adversary in cyberspace, but it could use its significant cyber-sabotage capabilities against European targets in the future as well.[144]

Unpredictable threat assessment as more countries develop offensive cyber programmes

In 2024, the AIVD observed a further increase in the number of countries developing offensive cyber programmes – a sharp rise over the past three years.[145] This trend cannot be separated from the growing geopolitical tension in a world that is increasingly in open conflict. Although new cyber actors have so far rarely, if ever, targeted the Netherlands directly, they threaten the digital security of its partners, allies, the EU and NATO.[146] After all, digital processes transcend national borders and are highly interconnected and interdependent. A cyberattack on a digital process in another country can therefore have knock-on effects, potentially affecting the Netherlands or Dutch interests. The emergence of new state cyber actors also contributes to a more unpredictable cyber landscape overall, making it increasingly difficult to gain and maintain a clear picture of the threat.[147]

Media reports moreover show that a wide and diverse group of state actors are purchasing spyware.[148] Because commercial spyware is available to any state actor with sufficient financial means, it provides an accessible way to acquire offensive cyber capabilities Such actors do not need technical expertise or an extensive intelligence apparatus. The emergence of commercial spyware developed by private companies has ended governments' monopoly on advanced offensive cyber capabilities, increasing the risk of cyber proliferation.

Complex and unpredictable threat assessment requires a broad notion of resilience

The developments described in this chapter each contribute to an increasingly complex and unpredictable threat landscape. There is a proliferation of cyber capabilities, notably by Russia, China and North Korea. Russia views itself as engaged in a broader conflict with the West and has conducted at least one (attempted) act of cyber sabotage in the Netherlands. China operates through a wider cyber ecosystem, enabling it to exploit vulnerabilities extremely quickly, leaving organisations little time to apply patches. Chinese actors are also carrying out (preparatory acts for) sabotage in other parts of the world, which could eventually extend to Europe. North Korea continues to expand its capacity to conduct cyberattacks and steals ever-larger amounts of cryptocurrency, which is used, among other things, to finance the regime. In addition to these known state actors with offensive cyber programmes, other countries are now developing such programmes of their own. Some of them purchase commercial spyware to do so. State actors also deploy non-state actors and organisations, blurring the distinction between them. In addition, the blending of actors also leads to the mixing or obscuring of motives, as illustrated by North Korea. Moreover, some (state or state-supported) actors are showing greater risk appetite to deploy offensive cyber capabilities against Western targets.

All these developments are unfolding at the same time and on an increasing scale, creating a threat landscape that is highly opaque and unpredictable. Despite this complexity, the basic digital principles still provide an effective barrier against many types of cyberattacks. It is equally crucial that organisations design their resilience not only to prevent incidents, but also to ensure robustness and strengthen other elements of resilience. This includes detecting cyber incidents, limiting damage when they occur, facilitating recovery, and ensuring that fallback options and procedures are in place.

A successful attack on the telecommunications sector could have a major impact, partly because many other sectors depend on the proper functioning of telecommunications.

3 Real threat to the telecom sector – the Netherlands is also a target

There has long been justified attention to the resilience of critical infrastructure. After all, the continuity of a critical process such as telecommunications is crucial to the functioning of society. Incidents in the US telecom sector show that the threat is tangible. The Netherlands was also targeted in Salt Typhoon's espionage campaign but suffered no impact. The sector is of interest to actors for various reasons, making it a potential target. Although major incidents have so far not occurred in the Netherlands and resilience within the sector is strong, major incidents abroad, such as those in the United States, demonstrate the need for continued attention to both resilience and the evolving threat.

Incidents in the United States show that the threat to the telecom sector is real

Salt Typhoon attacks the US telecom sector and the Netherlands is also targeted

A large-scale and far-reaching cyber campaign in the United States has shown that the threat to the telecom sector is real. In October 2024, it emerged that at least nine US telecom companies had been compromised by a campaign carried out by a Chinese APT called Salt Typhoon.[149] The cyber actor infiltrated multiple telecom companies using stolen login credentials and by exploiting vulnerabilities in edge devices, some of which had been known for some time.[150] The exact duration of the actor's intrusion is unclear. Initial reports indicated that the actor had been active since March 2024, while other US sources suggested that the campaign began as early as 2021.[151] [152] The cyber actor also reportedly penetrated deeply into the infrastructure of the US telecom network. Several US media outlets reported that the hackers stole call records and private communications, including those of current US President Trump and Vice President Vance.[153] The group also allegedly gained access to the US government's wiretapping platform in an attempt to identify Chinese agents under surveillance.[154] [155] It remains unknown whether the Chinese hackers have been fully removed from the affected systems. Salt Typhoon's campaign[X] was described by one US senator as 'the worst telecom hack in American history'.[156] Salt Typhoon also targeted a number of smaller Dutch internet service and hosting providers.[157] [158] In August 2025, the AIVD and MIVD reported that the attackers had gained access to routers belonging to these providers but, as far as is known, had not penetrated their internal networks. One possible explanation is that the Dutch targets received less focused attention from the hackers. The FBI stated that Salt Typhoon had attacked more than 200 companies across 80 countries.[159]

[X] According to the US Cyber Infrastructure and Security Agency (CISA), cyber actor Salt Typhoon is a Chinese state-backed hacker group.

The situation in the United States cannot be compared directly to that in the Netherlands. The US telecom infrastructure, unlike that of many European countries and certainly the Netherlands, is outdated and, according to the chair of the Senate Intelligence Committee, consists of 'a patchwork of interconnected networks'.[160] The patchwork of interconnected networks is so outdated that it cannot always be properly patched, leaving vulnerabilities unresolved and persisting, or requiring complex mitigating measures to be implemented.[161] The campaign in the US demonstrates both the depth and breadth of the actor's access to and across telecom networks and the strong interest state actors have in penetrating them. Although the Dutch context differs from that of the US, critical sectors in the Netherlands face risks stemming from high dependency on foreign suppliers and the growing complexity of their infrastructures.

The Salt Typhoon campaign demonstrates that the threat remains persistent and real. Moreover, the same cyber actor appears to be targeting multiple telecom providers and other critical infrastructure and to be expanding operations to other countries. In June 2025, for example, the US satellite company Viasat announced that it had been hacked by Salt Typhoon, although few details were released.[162] The satellite company provides satellite broadband services to governments worldwide and to clients in the aviation, defence, energy, maritime and corporate sectors. The Canadian Cyber Security Agency also reported that a Canadian telecom company had been the victim of a cyberattack, most likely by Salt Typhoon.[163] [164] Europe has also seen several cyberattacks on the telecoms sector in the past year, as also reflected in the Annual Review. The Danish Centre for Cyber Security (CFCS) had already warned of increasing interest from state actors in the European telecom sector. In March 2025, the CFCS thus raised the threat level for the Danish telecom sector from 'medium' to 'high'.[165] The French National Agency for Security and Information Systems (ANSSI) reported similar attacks on the telecom sector in its annual report,[166] noting that telecom companies are persistently targeted for espionage purposes and advising entities in the sector to remain alert to ongoing threats to this type of infrastructure.[167] [168]

All critical sectors are potential targets; specific characteristics of the telecom sector

All critical sectors[XI] can be attractive targets for malicious actors, as described in previous CSANs. Services and processes within critical sectors form the foundation on which Dutch society operates, making continuity essential. Prolonged outages or disruptions can have wide-ranging societal effects.[169] Interest from malicious actors in critical sectors – particularly telecommunications – is heightened by the sector's defining characteristics, which influence its overall resilience and the potential gains attackers may achieve. The recent targeted campaign against the US telecom sector confirmed that this interest and the long-standing threat to the sector are genuine. The telecom sector's defining features relate to its critical role, its inherent connectedness to the outside world and its users, and competition among providers within this essential sector.

The telecom sector covers all public communication services, including mobile and fixed services and networks, satellite connections and undersea cables. Its crucial role is to enable communication between companies, governments and citizens by providing access to the digital world.[170] A distinctive feature of the sector is that many other sectors, including critical sectors, depend on it. For example, the financial sector relies on telecom infrastructure for millions of daily transactions, while in logistics, the telecom infrastructure is essential for stock management and supply chains.[171]

Another defining feature of the telecom sector is the constant balancing act that it performs between security and accessibility. To provide communication services, the sector must grant users access to its networks. With millions of network users – each connecting multiple, diverse devices – the attack surface of those networks, and therefore of the entire sector, increases accordingly. The way in which the sector must deliver services inherently expands this attack surface, requiring additional security measures. Because the telecom infrastructure is fully connected to the outside world, some security measures that are feasible for other organisations cannot be applied within the telecom sector. The networks process highly sensitive user data, meaning that large-scale incidents could have severe and wide-ranging consequences. Major disruptions in the telecom sector could also cause cascading effects in other critical sectors that depend on its networks but may lack fallback options. In extreme cases, this could result in social disruption. Fortunately, the Netherlands has not experienced incidents that have had such an impact in recent years.

Telecom sector an attractive target for malicious actors, successful attacks could have major impact

For both criminal and state actors, the telecom sector is attractive partly because it processes vast amounts of personal data – including call records, location data, customer details and internet traffic.[172] State actors can misuse access to such data to track, monitor and influence individuals, such as members of diaspora communities, activists or dissidents. The sector is also of interest to state actors because of the options for espionage.[173] According to the AIVD, hacks on telecommunications providers are among the most valuable intelligence positions for state actors.[174] For this reason, the use of IT products and services from countries known to run offensive cyber programmes against Dutch interests is considered undesirable in critical parts of the telecom network.[175] Espionage can lead to the acquisition of data and of (technical) knowledge about the infrastructure. This knowledge may serve espionage objectives, but can also be used to reconnoitre networks. A reconnaissance can be part of (preparations for) later sabotage. Preparatory acts allow actors to carry out acts of sabotage with little or no warning.[176] In cases of sabotage affecting the telecom sector, the sector itself does not necessarily have to be the target. Sabotage may also be directed against (specific) customers using the network, or may aim at broader social disruption. In 2023, for instance, a Russian APT succeeded in disabling the network of the Ukrainian provider Kyivstar, leaving millions of users without mobile access for days.[177] DDoS attacks also affect telecom networks, as the attack traffic uses the infrastructure of these networks – even when the telecom provider itself is not the target. For cybercriminals, the large volumes of personal data processed in the sector are particularly appealing. Such data can be stolen and sold, or used for (or as a stepping stone for) future attacks. As with all critical sectors, the telecom sector is an attractive target for cybercriminals because continuity is crucial. While continuity is vital for all critical sectors, the telecom sector has no analogue, publicly accessible fallback option. If the financial sector is attacked and electronic payments become impossible, for example, cash transactions can – at least in part and despite practical challenges – provide an alternative. For the telecom sector, there is no analogue, large-scale and publicly available fallback option.

Resilience of telecoms sector in the Netherlands is robust, although successful attacks cannot be ruled out

Resilience means the ability to prevent incidents by reducing (relevant) risks to an acceptable level, to limit damage and to recover once an incident has occurred.[178] Various measures are continuously being developed to protect critical processes and enhance the resilience of critical sectors.[179] Some resilience measures affecting the telecom sector are or will be enshrined in national legislation, such as the Telecommunications Act and the forthcoming Cyber Security Act (Cbw), which implements the Network and Information Security Directive (NIS2 Directive).[180]

Major efforts are being made to strengthen resilience within the telecom sector, and the resilience of the Dutch telecom sector is robust.[181] Nevertheless, challenges always remain. As in many other countries, telecom operators in the Netherlands are legally required to include facilities that enable wiretapping (lawful interception) on the instructions of the Public Prosecution Service (OM) or intelligence services. These facilities must meet strict security requirements, as they may contain classified or criminal-law information.[182] However, an inspection by the Dutch Authority for Digital Infrastructure (RDI) at KPN (2022) and Vodafone (2024) revealed that the security of their interception systems did not meet statutory requirements in some areas.[183] [184] Both providers fully resolved the shortcomings following the inspections. While this does not mean that a sophisticated attack campaign like those seen in the United States would necessarily succeed in the Netherlands, the investigation by the AIVD and MIVD shows that Dutch companies could also fall victim to such campaigns.[185] This illustrates the persistent and dynamic nature of the threat, and the importance of continuously improving digital resilience in the telecom sector – as well as in other critical sectors.

[XI] The following sectors have been identified as critical in the Netherlands: energy, telecommunications, transport, drinking water, water, chemicals, nuclear, finance, government, public order and security and defence.

The HNLMS Van Amstel escorts the Russian frigate Admiral Grigorovich in the North Sea (photo: defensie.nl). This is done to deter them from carrying out sabotage and espionage activities.

4 Geopolitical developments expose dependencies

Europe, and therefore the Netherlands, depends on providers from other, often non-European, countries for a wide variety of digital processes and services. Public organisations across different sectors, for instance, are increasingly dependent on services from a few large technology companies in the US. Digital dependencies that were not previously considered risky can become so later, for example as a result of geopolitical developments. In this context, it is important to identify potential risks of digital dependencies in order to increase resilience.

Digital dependencies can introduce risks

Like most other countries, the Netherlands depends on other countries and foreign companies. This applies in particular to many digital services and processes. Interdependencies can have positive effects, such as enabling specialisation and stimulating innovation.[186] However, Europe's position in digital technology is increasingly under pressure.[187] For instance, the global market share of European companies fell from 22 per cent in 2013 to 11 per cent in 2022.[188] As a result, Europe – and therefore the Netherlands – is becoming increasingly dependent on non-European companies for digital technology. This dependency can introduce risks. National security can come under pressure when imported technology gives companies or state actors access to sensitive information and processes. Similarly, if critical digital government processes are disrupted, there is a risk that government processes and operations could come to a halt, threatening the functioning of the democratic state under the rule of law and public services.[189] In addition, (digital) dependencies can be used as strategic or economic leverage. Economic influence for geopolitical purposes is increasingly being exercised by major economic powers, and EU member states can also be targets. In that context, states could also actively use bottlenecks in digital supply chains as (geo)political instruments of pressure.[190]

In the current geopolitical context, we must take into account that countries are weighing their own interests more sharply, which can lead to the Netherlands being confronted with dependencies that can be used as leverage. It is precisely these geopolitical developments that make or can make reliance on digital services and processes from other countries risky.[191]

The Netherlands is highly dependent on the United States, a shifting political landscape may affect digital security

During the past reporting period, it became clear that the Netherlands is strongly dependent on information and services from the United States[192] in several respects. For instance, the US is a key partner in cybersecurity and the related partnerships, including intelligence sharing and joint action against state and criminal actors. Cooperation and information sharing are crucial in the cyber domain, as cyberattacks do not stop at national borders. Sharing information is essential to obtain a broader view of threats and to intervene where necessary. However, current US policy could lead to a reduced role for the US in international cooperation or to lower financial investment. Given the United States' important role in cybersecurity partnerships, among others, continued active participation is crucial for digital resilience, including that of the Netherlands. The implications of US policy changes became evident, for example, when it was announced that funding for Mitre – the organisation managing the widely used Common Vulnerabilities and Exposures (CVE) database – would be discontinued.[193] The CVE provides an international standard for naming and documenting digital vulnerabilities. Without this standard, information sharing, analysis and coordination become more complex, slowing down responses to incidents. The loss of the database would therefore weaken global digital resilience. Eventually, the US Cybersecurity and Infrastructure Security Agency (CISA) announced that it would temporarily take over funding to prevent the CVE programme from being discontinued.[194]

The Netherlands also relies on many processes and services provided by US technology companies. Around 70 to 80 per cent of the European cloud services market is in the hands of US firms.[195] However, the digital dependency on US technology companies extends far beyond cloud services. Public organisations across different sectors of society are increasingly reliant on the services of a few large US technology companies (Big Tech) that provide software, AI tools and equipment.[196] This dependence can introduce risks (see box below).

Large-scale purchase of services from Big Tech can create risks

- Digital dependencies can increase, which has implications for the Netherlands' open strategic digital autonomy.XII For instance, laws may have extraterritorial effects, and Dutch oversight capabilities may be limited.
- Large-scale concentration can create a single point of failure. A malfunction or cyber incident could have global repercussions. Critical sectors may depend on a single provider, meaning an incident could have significant impact.
- The dominant position of large providers can be reinforced from both the supply and demand sides. On the supply side, providers can create their own ecosystems of interlinked services, making it difficult for organisations to exit (*vendor lock-in*). On the demand side, organisations often choose the largest providers mainly because (European) alternatives may be unavailable or offer fewer features. This also strengthens the providers' market power.
- Organisations may gradually lose control over core processes, for instance because knowledge drains away, oversight of system functionality decreases or negotiating power in relation to Big Tech weakens.

One of the risks associated with using services from Big Tech firms based in non-European countries such as the United States is that their legislation can have extraterritorial effect. The CLOUD Act allows US federal law enforcement authorities to compel technology companies to hand over user data by means of a warrant or subpoena, even when those data are stored abroad. Many experts assume that this does not apply when data are processed by a European service provider, especially within Europe. Legally, however, the situation is more nuanced: the US CLOUD Act can also apply to data processing outside the United States, including within the EU.[197] Although Microsoft has stated that this has never happened, employees have acknowledged that, because of this legislation, they cannot guarantee that data belonging to European companies will always remain within Europe.[198] Moreover, (geo)political developments can also affect the availability of digital services. When organisations or sectors depend on such services from third countries, risks can arise. It is therefore essential to assess risks continuously, as new ones may emerge that were not previously considered realistic. This means the issue is not only a technical matter or one confined to specific (critical) sectors. It can affect IT strategies more broadly and is therefore also a governance and risk management issue for organisational and corporate leadership.

Lagging resilience in the Caribbean part of the Kingdom, partly due to the impact of digital dependencies

Because of its geographic location and small scale, the potential risks described above cannot be applied directly to the Caribbean part of the Kingdom.[XIII] The digital infrastructure differs from that of mainland Netherlands, partly because it is outdated in some respects. Owing to the islands' location, it is also more logical that the United States is often the first point of reference for products and services. As in mainland Netherlands, governments and other organisations make extensive use of services from US Big Tech companies, such as email services. A key difference from mainland Netherlands, however, is that (internet) connectivity largely depends on submarine cables running through Puerto Rico to an internet exchange in the United States. There is also strong interdependence between the six Caribbean islands of the Kingdom in terms of connectivity. Bonaire, for example, relies on two connections routed through Curaçao, while Sint Eustatius and Saba depend mainly on connections through Sint Maarten.[199] The combination of these factors makes the Caribbean part of the Kingdom highly dependent for its digital infrastructure on non-European Big Tech and on some connections that additionally run to non-European countries.

Digitalisation on the islands is increasing, but it has not yet reached the level of the mainland Netherlands. The population is also less digitally skilled and less aware of digital risks.[200] Interaction with the government and businesses, for example, often still takes place through paper and at service counters. Various initiatives have been launched to address this, including in healthcare.[201] A new law aims to ensure that citizens and businesses in the Caribbean Netherlands can use government digital services safely and reliably.[202] The goal is to bring the digital services of government and semi-government bodies in the Caribbean Netherlands as much as possible up to the same level as in mainland Netherlands. This link with mainland Netherlands introduces new digital risks for both the Caribbean and European parts of the Kingdom. After all, the Caribbean part of the Kingdom could serve as a stepping stone for attackers seeking access to central government systems. Such access could expose data belonging to citizens and businesses and could be used to penetrate other systems in mainland Netherlands. The increasing integration with government systems means that connected systems must meet minimum requirements[XIV]. Unlike the regulations arising from this specific wave of digitalisation, legislation aimed at improving the security and reliability of digital services and critical infrastructure is lagging behind. EU directives such as NIS2, which are or will be in force in mainland Netherlands, do not apply there[XV], including the requirement for companies to take measures to secure their supply chains and ensure business continuity. By contrast, the Digital Resilience (Enhancement) Act has been declared applicable to the Caribbean Netherlands, allowing for general and specific (threat) information to be shared.

Compared with mainland Netherlands, little research is conducted into digital threats targeting the Caribbean part of the Kingdom. No specific threat has been identified, but the threats described in this CSAN also apply there. As in the rest of the world, vulnerable systems form an attractive target for malicious actors, making timely and proper patching of such systems essential. Statistics show that the Caribbean countries have a higher number of potentially compromised systems per capita than mainland Netherlands – at times more than three times as many. Although the number of vulnerable systems is higher in mainland Netherlands, its digital infrastructure is also far larger[XVI]. Several incidents illustrate that attacks seen elsewhere in the world also occur on the islands. For example, the Curaçao Tax and Customs Administration was hit by a ransomware attack; the Joint Court of Justice suffered a malware-related outage; and the email accounts of Aruban Members of Parliament were compromised [203],[204].

Digitalisation is currently gaining momentum, leading to the development and purchase of more digital services in the Caribbean part of the Kingdom. However, legislation and awareness of digital risks lag behind. Even more than in mainland Netherlands, small scale and interdependence in the Caribbean can introduce strategic dependencies that entail risks. Given the islands' geography and limited fallback options, disruptions to digitalised critical processes can have greater local impact than in mainland Netherlands, underscoring the importance of developing fallback options.

Greater autonomy and developing fallback options can reduce risks

As described in this chapter, geopolitical dynamics influence the level of risk associated with digital dependencies. The extent and likelihood of those risks materialising vary by case. What is certain, however, is that geopolitics are shifting and relations between countries are affected. In today's rapidly changing geopolitical reality, it is particularly crucial to understand which dependencies may pose risks and what the consequences might be. Efforts to limit those risks may, for example, involve pursuing a higher degree of open strategic digital autonomy. An important element of digital resilience is also having fallback options for digital services and processes. Such options not only reduce the potential impact of cyber incidents but also mitigate the risks arising from dependencies.

Research shows that central government organisations rely heavily on a small number of suppliers for digital processes, with little to no consideration of concentration risks. The possible consequences of such risks are also insufficiently weighed up at governance level.[205] This can lead to digital monocultures in which many organisations depend on a small number of providers.

The far-reaching and unforeseen effects of an incident within such a monoculture became clear during the outage at the US cybersecurity company CrowdStrike in July 2024.[206] Moreover, government organisations do not adequately assess or manage the (strategic) risks associated with their suppliers and service providers, and several have no effective fallback options in place.[207] The above shows that the central government has not yet given sufficient attention to resilience and needs to make progress. Improvements can be achieved, among other ways, by ensuring that dependencies remain a standing topic on governance agendas and by conducting thorough risk analyses at that level.

[XII] Open strategic autonomy is defined as the EU's ability to act as a global player – in cooperation with international partners – based on its own insights and choices, to safeguard public interests and be resilient in an interconnected world.

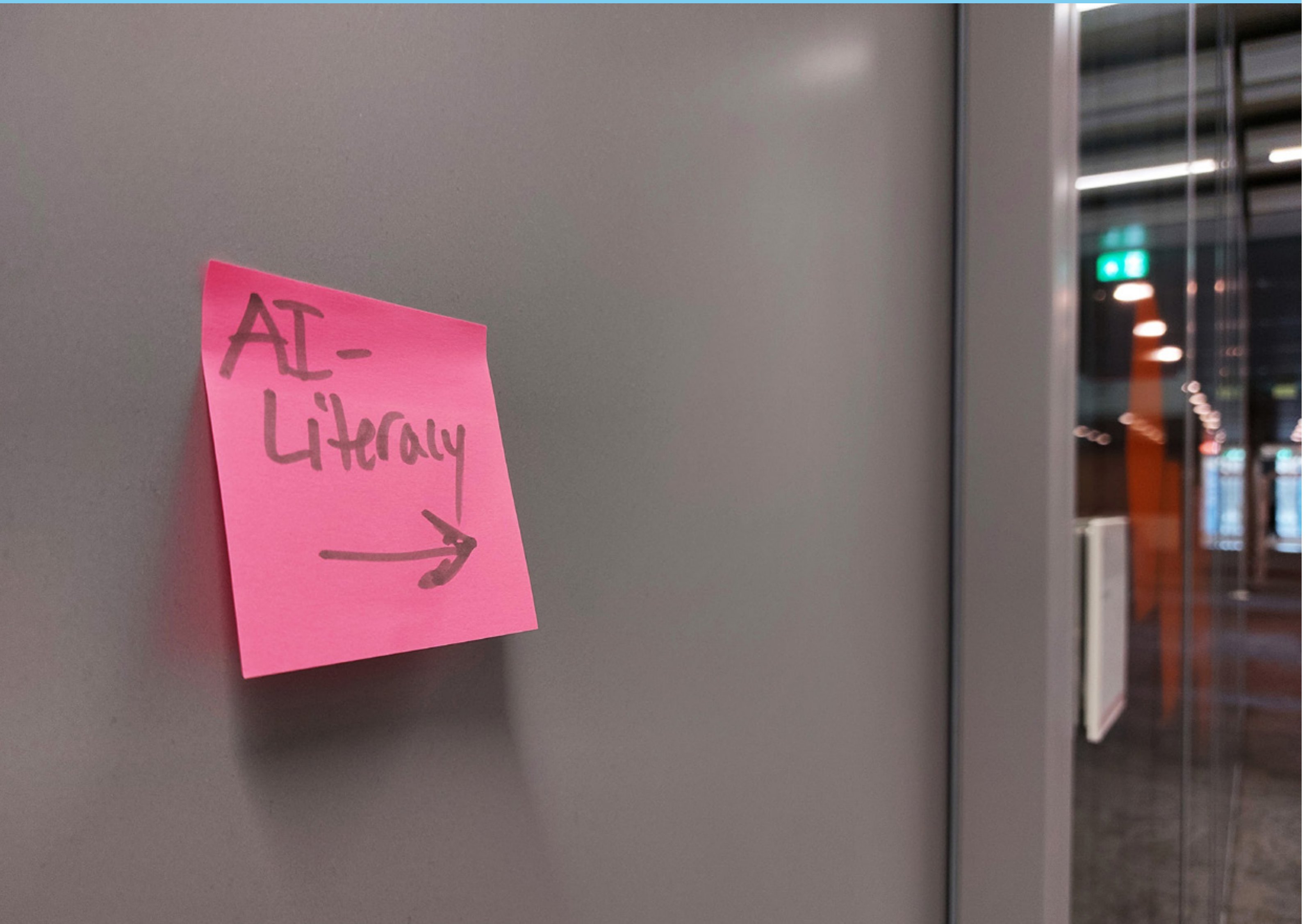
[XIII] The Caribbean part of the Kingdom includes the autonomous Caribbean countries of Aruba, Curaçao and Sint Maarten as well as the Caribbean Netherlands (Bonaire, Sint Eustatius and Saba).

[XIV] These include the Baseline Information Security (BIO) and the DigiD connection requirements.

[XV] NIS2 and the Cyber Security Act (Cbw) apply only to central government organisations operating in the Caribbean Netherlands.

[XVI] Data from Shadowserver.org, there are no separate data for Caribbean Netherlands.

Applications of generative AI are accessible to a wide audience, including malicious actors. AI offers new opportunities but also amplifies existing digital threats.



5 Generative AI amplifies existing threats to digital security

In recent years, the development of generative AI has accelerated. The technology behind it does not constitute a threat, but specific applications – combined with the intent of the actor using it – can give rise to new risks. Generative AI can be used in multiple ways: both to support malicious activity and as a defence against threats. At present, generative AI primarily amplifies existing digital threats.

Generative AI amplifies existing digital threats

Artificial intelligence (AI) is a broad technology that will fundamentally change our society.[208] One underlying form of it is generative AI – a type of AI that can create new content from existing data based on user prompts or questions.[209] Many AI applications that affect national security fall under this category. Generative AI includes large language models (LLMs) used to generate text. In recent years, several LLMs and their applications – such as ChatGPT, Gemini and Llama – have become publicly available. Reports soon followed about (potential) misuse of these systems by malicious actors in cyber operations.[210]

Generative AI can be used for offensive and defensive operations

Cyber actors can use generative AI in several ways:[211]

1. Information gathering and target detection
Cyber actors can use LLMs to quickly and automatically identify attractive targets, gather information about potential targets and find new vulnerable systems. Researchers, for example, have shown that ChatGPT can be used to rapidly gather information about a bank's IT system.[212] Although such information is often publicly available online, LLMs can greatly accelerate the process of collecting and analysing it.

2. Social engineering
Cyber actors can use LLMs to conduct social engineering[XVII]. LLMs can produce error-free text in multiple languages, even if the actor does not speak the language.[213] This makes it possible to generate convincing spam and phishing messages automatically and at high speed. LLMs are now advanced enough to interpret audio and video conversations, generate a response, and even 'speak' it to the victim. Using AI in this way increases the likelihood that the victim will perceive the attacker as trustworthy. [214] LLMs allow cyber actors

---

[XVII] Social engineering comprises the techniques that cybercriminals use to trick victims into revealing sensitive data through psychological manipulation. The attacker influences the other to then get the desired result or advantage.

to respond contextually, mimic writing or speaking styles, and convincingly impersonate specific individuals.

3. Generating malware and conducting cyberattacks
LLMs enable cyber actors to conduct cyberattacks that they might otherwise lack the technical ability to perform without the help of AI. Those who already possess this technical expertise can use AI to do so faster and more efficiently.[215] Several LLMs are (also) trained on multiple programming languages, enabling cyber actors to use them or have them assist in writing malware.[216] In practice, cyber actors can use the model as a sounding board to draft effective code and/or to find vulnerabilities in code. Although some knowledge of programming or vulnerabilities is still required,[217] malware itself can also become more intelligent through AI by acquiring self-learning properties that allow it to independently find new vulnerabilities and then exploit them. As attacks become better disguised, malware can remain undetected on a device for extended periods and spread to other devices and networks.[218] AI can also assist malware by rapidly analysing large data volumes to determine what is valuable.

4. Defensive applications
The ability of AI algorithms to quickly analyse large amounts of data and detect anomalies can also be used in defence against cyberattacks.[219] AI can, for example, monitor network traffic to identify irregularities that signal potential cyber threats. It can also help acquire and process threat intelligence and analyse malware.[220]

Besides using generative AI for offensive and defensive operations, generative AI itself can become a target. Attacks may aim to disrupt or mislead AI systems, for instance by attempts to influence training data or improperly manipulate the model.[221] AI systems can be affected by adversarial attacks, which are very complex to detect. These attacks can, for example, enable attackers to retrieve the contents of a model's training data.

Generative AI amplifies existing threats; its use by malicious actors is likely

Generative AI technology in itself does not pose a threat to national security. The danger lies in how it is specifically applied and the intent of the actor behind its use.[222] However, as the perspectives described above show, cyberattacks carried out with the help of generative AI require less technical knowledge and capability, enabling a broader range of actors to carry them out. Using generative AI also allows (preparation for) attacks to be executed faster and on a much larger scale.

Cybersecurity firm Symantec has reported an increase in cyberattacks by criminals using LLMs to generate malware code.[223] According to cybersecurity firm Talos, cybercriminals are increasingly turning to 'uncensored LLMs' – models that operate without restrictions or guardrails. Some of these uncensored LLMs are explicitly promoted for creating malware or phishing pages.[224] Given the widespread availability and rapid development of generative AI, it is likely that criminal actors will continue to use it and may intensify their use over time.

Based on their own intelligence, the MIVD and AIVD have observed several state actors using generative AI. Google has also reported that several APTs – including groups from Iran and Russia – use LLMs in various (early) stages of cyberattacks.[225] It remains difficult to predict how AI will alter the methods of state actors globally. Intelligence services have information indicating that state cyber actors are interested in using AI, including for conducting digital influence operations. As AI becomes operationally integrated, these cyber actors' ability to carry out such operations is likely to grow significantly. This will make it more difficult to identify and counter influence campaigns – a development the intelligence services consider highly concerning

Recently, several DDoS attacks caused (temporary) disruptions to services. Between January and March 2025, there were four attacks that rendered DigiD unavailable for an hour or more. This also limited the availability of related services and temporarily prevented users from logging in.

28-08-2024 | Storing MijnOverheid

Vanwege een storing op MijnOverheid zijn momenteel een aantal functionaliteiten niet beschikbaar. We werken aan een oplossing om het probleem zo snel ...

Appendix

1 Explanatory notes

Purpose and scope

The Cybersecurity Assessment Netherlands, 2025 (CSAN 2025) 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. The CSAN 2025 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, 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 a standalone Core Chapter setting out the main messages. The Core Chapter is based on the in-depth thematic chapters and therefore does not include source references. This structure allows readers from different target groups to browse through the CSAN and focus on the topics relevant to their professional role or interests. The in-depth chapters cover the following themes:

- Chapter 1, the Annual Review, provides a summary of relevant incidents from July 2024 to August 2025. The chapter also includes interpretation of these incidents, summarised in overarching trends.
- Chapter 2 describes an increase in state cyber capabilities and how states are merging with non-state actors and/or private organisations.
- Chapter 3 outlines the interest of malicious actors in the telecom sector as a critical sector, following a cyber campaign elsewhere in the world.
- Chapter 4 discusses the risks that may arise from digital dependencies and how changing geopolitical circumstances can influence the risk assessment of those dependencies.
- Chapter 5 explains that generative AI amplifies existing threats to digital security and how large language models (LLMs) can be used for both offensive and defensive operations.

Explanation of the preparation method

The National Coordinator for Security and Counterterrorism (NCTV) adopts the Cybersecurity Assessment Netherlands (CSAN) each year. The information, insights and expertise of government services, organisations in critical 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:

- Which relevant incidents occurred in the Netherlands or in comparable countries from July 2024 to August 2025, and what new insights do they provide?
- 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?
- Which changes can be identified in digital threats that affect national security? Consider their nature, scale, targets, actors, vulnerabilities, types of disruption and the modus operandi of the actors.
- Which changes can be identified that affect interests that could be compromised when cyber incidents occur? And what could be the impact?
- Which changes can be identified in the extent to which the Netherlands is resilient against these digital threats?
- To what extent are changes occurring in the greatest risks to the national security of the Netherlands?

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 and supplemented with additional insights. Experts were also consulted on specific parts of this CSAN, such as the threat to the telecom sector and the state of digital security in the Caribbean Netherlands.

2. Writing and peer review
After completing the analysis phase, individual authors wrote draft chapters. Colleagues from the NCTV, NCSC and at the AIVD and MIVD have since reviewed the Annual Review. Various sections were co-written by the Public Prosecution Service (OM), the High Tech Crime Team (THTC), the Ministry of Foreign Affairs and the AIVD and MIVD.

3. Validation.
The CSAN undergoes an extensive validation process, in which the draft text is submitted for comment to internal and 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

Explanation of figures in Annual Review from Melissa partnership project

The Melissa Annual Review compiles information on ransomware incidents at larger organisations (from about 100 FTEs). It is based on incident data from the Public Prosecution Service (OM), the police, the NCSC, Cyberveilig Nederland and several private-sector partners. The participating companies specialise in incident response to ransomware attacks. Incidents are assessed by security experts who apply a specific definition of ransomware. Melissa defines ransomware as: '… attackers hold a victim's data hostage and use coercive means to persuade the victim to comply.'[226] 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.[227] It should be noted that 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.[228]

The Ransomware Annual Review 2024 recorded 121 ransomware attacks: 76 were reported to the police, 20 were identified by incident response companies, and 25 were known to both incident response companies and the police.

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

The figures are based on an analysis of data breaches reported to the DPA in 2024.[229] 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 DPA identified 112 ransomware attacks in 2024.

The actual number may be higher than 112 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 ransomware attacks recorded by Melissa is higher than that reported by the DPA. One explanation for this could be that no personal data were affected in the incidents reported by the DPA. In addition, the difference in figures could be due to the use of slightly different definitions of ransomware.

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

3 Sources and references

1 ‘Logius wil nieuwe aanpak voor “slimmere en minder voorspelbare” ddos-aanvallen’ , Tweakers, 28-03-2025, https://tweakers.net/nieuws/233350/logius-wil-nieuwe-aanpak-voor-slimmere-en-minder-voorspelbare-ddos-aanvallen.html.

2 ‘Jaarbeeld Ransomware 2024’, NCSC, 17-02-2025, https://www.ncsc.nl/documenten/publicaties/2025/02/17/jaarbeeld-ransomeware-2024.

3 ‘Rapportage Datalekken 2024’, Dutch Data Protection Authority, 03-07-2025 https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024.

4 ‘Veranderende wereldorde bevestigt belang van een weerbaar Nederland’, NCTV, 17-07-2025, https://www.nctv.nl/actueel/nieuws/2025/07/17/veranderende-wereldorde-bevestigen-belang-van-een-weerbaar-nederland.

5 Cyber Security Assessment Netherlands, 2024, NCTV, 28-10-2024, https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/nieuws/2024/10/28/cybersecuritybeeld-2024-turbulente-tijden-onvoorziene-effecten.

6 ‘Openbaar jaarverslag 2024 Militaire Inlichtingen- en Veiligheidsdienst, MIVD’, 22-04-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen-en-veiligheidsdienst.

7 ‘Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware’, Politie.nl, 23-05-2025, https://www.politie.nl/nieuws/2025/mei/22/11-internationale-politiediensten-pakken-met-operation-endgame-door-in-bestrijding-ransomware.html.

8 ‘Internationale opsporingsdiensten ontmantelen infostealers’, politie.nl, 29-10-2024, https://www.politie.nl/nieuws/2024/oktober/29/internationale-opsporingsdiensten-ontmantelen-infostealers.html.

9 https://www.politie.nl/nieuws/2025/mei/7/11-opnieuw-wereldwijde-politieacties-tegen-ddos.html, politie.nl, 07-05-2025, https://www.politie.nl/nieuws/2025/mei/7/11-opnieuw-wereldwijde-politieacties-tegen-ddos.html.

10 ‘Internationale cybercrime aangepakt: Politie Amsterdam en FBI ontmantelen proxydienst Anyproxy’, politie.nl, 12-05-2025 , https://www.politie.nl/nieuws/2025/mei/9/internationale-cybercrime-aangepakt-politie-amsterdam-en-fbi-ontmantelen-proxydienst-anyproxy.html.

11 ‘Sleuteldienst voor ontwikkelaars van malware onderuitgehaald’, politie.nl, 30-05-2025, https://www.politie.nl/nieuws/2025/mei/30/11-sleuteldienst-voor-ontwikkelaars-van-malware-onderuitgehaald.html.

12 ‘BKA and FIOD shut down cryptocurrency swap service eXch. € 34 million in cryptocurrency has been seized during the operation’, FIOD, 09-05-2025, https://www.fiod.nl/bka-and-fiod-shut-down-cryptocurrency-swap-service-exch-e-34-million-in-cryptocurrency-has-been-seized-during-the-operation/.

13 ‘Nederland lanceert internationaal netwerk voor daderpreventie cybercrime: InterCOP’, politie.nl, 15-06-2023, https://www.politie.nl/nieuws/2023/juni/15/11-nederland-lanceert-internationaal-netwerk-voor-daderpreventie-cybercrime-intercop.html.

14 ‘Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware’, politie.nl, 23-05-2025, https://www.politie.nl/nieuws/2025/mei/22/11-internationale-politiediensten-pakken-met-operation-endgame-door-in-bestrijding-ransomware.html.

15 ‘Internationale opsporingsdiensten ontmantelen infostealers’, politie.nl, 29-10-2024, https://www.politie.nl/nieuws/2024/oktober/29/internationale-opsporingsdiensten-ontmantelen-infostealers.html.

16 ‘Internationale operatie tegen hackgroep NoName057(16)’, Police, 16-07-2025, https://www.politie.nl/nieuws/2025/juli/16/06-internationale-operatie-tegen-hackgroep-noname05716.html.

17 ‘Onze aanvallen gaan door!”: Pro-Russische hackers willen wraak na internationale politieactie’, Pointer, 08-08-2025, https://pointer.kro-ncrv.nl/aanvallen-gaan-door-pro-russische-hackers-wraak-internationale-politieactie.

18 ‘ECLI:NL:RBROT:2025:2492’, uitspraken.rechtspraak.nl, 21-02-2025, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2492&showbutton=true&idx=3.

19 ‘ECLI:NL:RBROT:2025:2515’, uitspraken.rechtspraak.nl, 21-02-2025, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2515&showbutton=true&idx=2.

20 ‘Cyber-attacks: Council extends sanctions and legal framework’, European Council, 12-05-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/12/cyber-attacks-council-extends-sanctions-and-legal-framework/.

21 ‘MIVD waarschuwt: Russen hebben het gemunt op westerse hulp aan Oekraïne’, MIVD, 05-09-2024, https://www.defensie.nl/actueel/nieuws/2024/09/05/mivd-waarschuwt-russen-hebben-het-gemunt-op-westerse-hulp-aan-oekraine.

22 ‘Cyber-attacks: three individuals added to EU sanctions list for malicious cyber activities against Estonia’, European Council, 27-01-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia/.

23 ‘Onbekende Russische groep achter hacks Nederlandse doelen’, AIVD, 27-05-2025, https://www.aivd.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen.

24 ‘Russian hybrid threats: EU lists further 21 individuals and 6 entities and introduces sectoral measures in response to destabilising activities against the EU, its member states and international partners’, European Council, 20-05-2025, https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/.

25 ‘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/.

26 ‘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.

27 Cyber Security Assessment Netherlands, 2024, NCTV, 28-10-2024, https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024.

28 ‘Ook ministerie van Buitenlandse Zaken getroffen door storing’, NRC, 19-06-2024, https://www.nrc.nl/nieuws/2024/07/19/ook-ministerie-van-buitenlandse-zaken-getroffen-door-storing-a4860171.

29 ‘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.

30 ‘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.

31 ‘Evaluatie NAFIN storing’, House of Representatives, 20-03-2025, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025Z06099&did=2025D14107.

32 ‘Kamerbrief update hack bij politie’, rijksoverheid.nl, 09-10-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/10/09/tk-update-over-hack-bij-de-politie.

33 ‘Onbekende Russische groep achter hacks Nederlandse doelen’, Ministerie van Defensie, 27-05-2025, https://www.defensie.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen.

34 ‘Fortinet bevestigt cyberaanval, mogelijk 440GB aan bedrijfsgegevens gestolen’, Tweakers, 13-09-2024, https://tweakers.net/nieuws/226550/fortinet-bevestigt-cyberaanval-mogelijk-440gb-aan-bedrijfsgegevens-gestolen.html.

35 Based on internal information from the NCSC.

36 Based on internal information from the NCSC.

37 ‘Storing bij gemeenten, afspraken vallen uit’, De Gelderlander, 10-10-2024.

38 ‘Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)’, Google Mandiant, 24-10-2024, https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575.

39 ‘Datalek bij gemeente Velsen’, Noordhollands Dagblad, 23-10-2024.

40 ‘E-mailadressen honderden gezinnen op straat door hack bij jeugdzorgmedewerker’, RTL, 09-10-2024, https://www.rtl.nl/nieuws/binnenland/artikel/5474670/e-mailadressen-gezinnen-jeugdzorg-eindhoven-brabant-hack.

41 ‘Clop ransomware is now extorting 66 Cleo data-theft victims’, Bleepingcomputer, 24-12-2024, https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/.

42 ‘Russische cybercriminelen konden data Centric stelen door softwarelek’, FD, 24-01-2025, https://fd.nl/bedrijfsleven/1543474/russische-cybercriminelen-konden-data-centric-stelen-door-softwarelek.

43 ‘Amersfoort slachtoffer van aanval op testomgeving Centric’, iBestuur, 27-01-2025, https://ibestuur.nl/artikel/amersfoort-slachtoffer-van-aanval-op-testomgeving-centric/.

44 ‘Ahold Delhaize getroffen door grote ransomware-aanval, claimt aan Rusland gelieerde hackersgroep’, BNR, 17-04-2025, https://www.bnr.nl/nieuws/tech-innovatie/10571730/ahold-delhaize-getroffen-door-grote-ransomware-aanval-claimt-hackersgroep.

45 ‘Ahold waarschuwt duizenden medewerkers na datadiefstal’, Tweakers, 23-04-2025, https://tweakers.net/nieuws/234224/ahold-waarschuwt-duizenden-medewerkers-na-datadiefstal.html.

46 ‘Cyberaanval Amerikaanse tak Ahold trof 2,2 miljoen mensen’, Tweakers, 28-06-2025, https://tweakers.net/nieuws/236716/cyberaanval-amerikaanse-tak-ahold-trof-2-komma-2-miljoen-mensen.html.

47 ‘Gegevens 100.000 inwoners Amersfoort gelekt na hack bij softwareleverancier’, Tweakers 03-12-2024, https://tweakers.net/nieuws/229362/gegevens-100000-inwoners-amersfoort-gelekt-na-hack-bij-softwareleverancier.html.

48 ‘Gemeente Arnhem lekt gevoelige persoonsgegevens tientallen inwoners’, security.nl, 28-02-2025, https://www.security.nl/posting/878120/Gemeente+Arnhem+lekt+gevoelige+persoonsgegevens+tientallen+inwoners.

49 ‘Gemeenten Tubbergen en Dinkelland lekken gegevens inwoners’, security.nl, 02-12-2024, https://www.security.nl/posting/867600/Gemeenten+Tubbergen+en+Dinkelland+lekken+gegevens+inwoners.

50 ‘Rumoerige jaarwisseling met heftige incidenten’, politie.nl, 03-01-2025, https://www.politie.nl/nieuws/2025/januari/1/00-jaarwisseling.html.

51 ‘Noodknop politie haperde tijdens Nieuwjaarsnacht: “Door oog van naald gekropen”’, nu.nl, 02-01-2025, https://www.nu.nl/tech/6340992/noodknop-politie-haper-de-tijdens-nieuwjaarsnacht-door-oog-van-vnaald-gekropen.html.

52 ‘Update cyberaanval: dinsdag nog geen onderwijs’, tue.nl, 13-01-2025, https://www.tue.nl/nieuws-en-evenementen/nieuwsoverzicht/13-01-2025-update-cyberaanval-dinsdag-nog-geen-onderwijs.

53 ‘TU/e handelde goed bij cyberaanval, maar er zijn ook leerpunten’, TU/e, 19-05-2025, https://www.tue.nl/nieuws-en-evenementen/nieuwsoverzicht/19-05-2025-tue-handelde-goed-bij-cyberaanval-maar-er-zijn-ook-leerpunten.

54 ‘Storing DigiD werd veroorzaakt door grote ddos-aanval’, NOS.nl, 15-01-2025, https://nos.nl/artikel/2551874-storing-digid-werd-veroorzaakt-door-grote-ddos-aanval.

55 ‘SURF en onderwijsinstellingen opnieuw getroffen door ddos-aanval’, Tweakers, 16-01-2025, https://tweakers.net/nieuws/230886/surf-en-onderwijsinstellingen-opnieuw-getroffen-door-ddos-aanval.html.

56 ‘Opnieuw computerprobleem in ziekenhuis Rijnstate: ‘Maar zorg kan nu gewoon doorgaan’’, AD/Algemeen Dagblad, 16-01-2025, https://www.gelderlander.nl/arnhem/opnieuw-softwareprobleem-in-ziekenhuis-rijnstate-maar-zorg-kan-nu-gewoon-doorgaan~a32a715c/.

57 ‘Computerstoring bij ziekenhuis Arnhem verholpen’, nos.nl,14-01-2025, https://nos.nl/artikel/2551724-computerstoring-bij-ziekenhuis-arnhem-verholpen.

58 ‘Gegevens van 2.200 gebruikers buitgemaakt bij hack website raad Almere, dader onbekend’, Omroep Flevoland, 23-01-2025, https://www.omroepflevoland.nl/nieuws/412942/gegevens-van-2-200-gebruikers-buitgemaakt-bij-hack-website-raad-almere-dader-onbekend.

59 ‘UAC-0063: Cyber Espionage Operation Expanding from Central Asia’, Bitdefender, 12-02-2025, https://www.bitdefender.com/en-us/blog/businessinsights/uac-0063-cyber-espionage-operation-expanding-from-central-asia.

60 ‘Italië: WhatsApp-gebruikers met Nederlands nummer doelwit spyware-aanval’, security.nl, 06-02-2025, https://www.security.nl/posting/875185/Itali%C3%AB%3A+WhatsApp-gebruikers+met+Nederlands+nummer+doelwit+spyware-aanval.

61 ‘WhatsApp says it disrupted a hacking campaign targeting journalists with Paragon spyware, techcrunch.com, 31-01-2025, https://techcrunch.com/2025/01/31/whatsapp-says-it-disrupted-a-hacking-campaign-targeting-journalists-with-spyware/.

62 ‘Politienummer 0900-8844 tijdelijk niet bereikbaar door een storing’, nu.nl, 25-02-2025, https://www.nu.nl/tech/6347195/politienummer-0900-8844-tijdelijk-niet-bereikbaar-door-een-storing.html.

63 ‘DigiD heeft last van storing door “terugkerende ddos-aanvallen”’, Tweakers, 03-03-2025, https://tweakers.net/nieuws/232452/digid-heeft-last-van-storing-door-terugkerende-ddos-aanvallen.html.

64 ‘DigiD was door ddos-aanval korte tijd ‘beperkt beschikbaar’’, security.nl, 13-03-2025, https://www.security.nl/posting/879866/DigiD+was+door+ddos-aanval+korte+tijd+%27beperkt+beschikbaar%27.

65 ‘DigiD kampt met slimmere ddos-aanvallen: ‘Vaak werk van verveelde tieners’’, nu.nl, 27-03-2025, https://www.nu.nl/tech/6350621/digid-kampt-met-slimmere-ddos-aanvallen-vaak-werk-van-verveelde-tieners.html.

66 ‘ICT-storing OM verholpen’, om.nl, 02-04-2025, https://www.om.nl/actueel/nieuws/2025/04/02/ict-storing-om-verholpen.

67 ‘Crowdstrike Global Threat Report 2025’, crowdstrike.com, 27-02-2025, https://www.securityweek.com/wp-content/uploads/2025/02/CrowdStrikeGlobalThreatReport2025.pdf.

68 ‘DigiD is opnieuw “beperkt beschikbaar” door ddos-aanvallen’, Tweakers, 09-04-2025, https://tweakers.net/nieuws/233740/digid-is-opnieuw-beperkt-beschikbaar-door-ddos-aanvallen.html.

69 ‘Kamerbrief over datalek in gepubliceerde documenten Rijksoverheid’, rijksoverheid.nl, 18-04-2025, https://www.rijksoverheid.nl/documenten/kamerstukken/2025/04/18/kamerbrief-over-datalek-in-gepubliceerde-documenten-van-de-rijksoverheid.

70 ‘Betalingsbedrijf Adyen meerdere keren getroffen door cyberaanval’, RTL, 22-04-2025, https://www.rtl.nl/nieuws/artikel/5505378/betalingsbedrijf-adyen-meerdere-keren-getroffen-door-cyberaanval.

71 ‘Ruim vijftig websites Nederland deze week doelwit pro-Russische hackersgroep’, NOS, 03-05-2025, https://nos.nl/artikel/2565889-ruim-vijftig-websites-nederland-deze-week-doelwit-pro-russische-hackersgroep.

72 ‘MIVD: Nederland ook doelwit spionagecampagne Russische hackers’, Ministerie van Defensie, 21-05-2025, https://www.defensie.nl/actueel/nieuws/2025/05/21/mivd-nederland-ook-doelwit-spionagecampagne-russische-hackers.

73 ‘Tiental organisaties in Nederland op de korrel van Russische hackersgroep, meldt NCSC’, AG Connect, 23-06-2025, https://www.agconnect.nl/maatschappij/security/nederlandse-organisaties-aangevallen-door-russische-hackers.

74 ‘Websites van gemeenten en provincies slechter bereikbaar door mogelijke aanval’, Nu.nl, 23-06-2025, https://www.nu.nl/tech/6360048/websites-van-gemeenten-en-provincies-slechter-bereikbaar-door-mogelijke-aanval.html.

75 ‘International Criminal Court targeted by new “sophisticated” attack’, The Record, 01-07-2025, https://therecord.media/international-criminal-court-cyberattack-2025.

76 ‘OM van internet af vanwege ‘kwetsbaarheid’, misbruik niet uitgesloten’, NOS, 18-07-2025, https://nos.nl/artikel/2575495.

77 ‘Advocaten hebben last van hack OM en zijn kritisch: “Post is geen oplossing”’, NOS, 26-7-2025, https://nos.nl/artikel/2576449.

78 ‘Openbaar Ministerie gaat geleidelijk weer online’, NOS, 04-08-2025, https://nos.nl/artikel/2577569.

79 ‘Casus: Citrix kwetsbaarheid’, NCSC, 22-07-2025, https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid.

80 ‘Onderzoek informatiebeveiliging’, DJI, 29-07-2025, https://www.dji.nl/actueel/nieuws/2025/07/29/onderzoek-informatiebeveiliging.

81 ‘Disrupting active exploitation of on-premises SharePoint vulnerabilities’, Microsoft, 22-07-2025, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/#storm-2603.

82 ‘Casus: Microsoft SharePoint Server kwetsbaarheden’, NCSC, 23-07-2025, https://www.ncsc.nl/actueel/nieuws/2025/07/23/casus-microsoft-sharepoint.

83 ‘SharePoint-servers 145 organisaties wereldwijd getroffen bij aanvallen’, security.nl, 29-07-2025, https://www.security.nl/posting/898699/SharePoint-servers+145+organisaties+wereldwijd+getroffen+bij+aanvallen.

84 ‘Z-CERT over de ransomware-aanval bij Clinical Diagnostics NMDL (Eurofins)’, Z-CERT, 11-08-2025, https://z-cert.nl/actueel/nieuws/ransomware-aanval.

85 ‘Minister en Kamerlid in datalek laboratorium: adres, bsn en medisch onderzoek op straat’, RTL, 12-08-2025, https://www.rtl.nl/nieuws/binnenland/artikel/5522904/ministers-kamerleden-datalek-laboratorium-hack-woonadres-bsn.

86 ‘Hackersgroep Nova wil geen losgeld meer van gehackte Clinical Diagnostics’, BNR, 21-08-2025, https://www.bnr.nl/podcast/tech-update/10581247/hackersgroep-nova-wil-geen-losgeld-meer-van-gehackte-clinical-diagnostics.

87 ‘Gehackt laboratorium heeft losgeld betaald: ‘Miljoenen euro’s geëist’’, RTL, 13-08-2025, https://www.rtl.nl/nieuws/binnenland/artikel/5523036/hack-laboratorium-cybercriminelen-ransomware-losgeld-betaald-data.

88 ‘Werkzaamheden instanties Caribische eilanden verstoord door hacks’, NOS, 02-08-2025, https://nos.nl/artikel/2577274-werkzaamheden-instanties-caribische-eilanden-verstoord-door-hacks.

89 ‘Hack bij KLM; gegevens van klanten gestolen, AD, 06-08-2025, https://www.ad.nl/amsterdam/hack-bij-klm-gegevens-van-klanten-gestolen~aca46219/.

90 ‘Nederlandse providers doelwit van Salt Typhoon’, Defensie, 28-08-2025, https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

91 ‘Frankrijk beschuldigt Rusland van cyberaanvallen bij verkiezingen en Spelen’, Nu.nl, 29-4-2025, https://www.nu.nl/buitenland/6354185/frankrijk-beschuldigt-rusland-van-cyberaanvallen-bij-verkiezingen-en-spelen.html.

92 ‘Cyprus’ critical infrastructure targeted by coordinated cyberattacks linked to pro-Palestine groups’, The Record, 21-10-2024, https://therecord.media/cyprus-critical-infrastructure-cyberattack-israel-palestine.

93 ‘Meet NailaoLocker: a ransomware distributed in Europe by ShadowPad and PlugX backdoors’, orangecyberdefense.com, 18-02-2025, https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors.

94 ‘Windows Remote Desktop Protocol: Remote to Rogue’, Google, 07-04-2025, https://cloud.google.com/blog/topics/threat-intelligence/windows-rogue-remote-desktop-protocol.

95 ‘Ransomware attack hits German pharmaceutical wholesaler, disrupts medicine supplies’, The Record, 01-11-2024, https://therecord.media/ransomware-attack-hits-german-pharmaceutical-wholesaler-disruptions.

96 ‘Blue Yonder SaaS giant breached by Termite ransomware gang’, bleepingcomputer.com, 06-12-2024, https://www.bleepingcomputer.com/news/security/blue-yonder-saas-giant-breached-by-termite-ransomware-gang/.

97 ‘Softwareleverancier van Jumbo en HEMA is gehackt, “geen hinder voor klanten”’, Tweakers, 27-11-2024, https://tweakers.net/nieuws/229168/softwareleverancier-van-jumbo-en-hema-is-gehackt-geen-hinder-voor-klanten.html.

98 ‘U.S. Wiretap Systems Targeted in China-Linked Hack; AT&T and Verizon are among the broadband providers that were breached’, The Wall Street Journal, 05-10-2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

99 ‘White House Says at Least 8 US Telecom Firms, Dozens of Nations Impacted by China Hacking Campaign’, securityweek.com, 05-12-2024, https://www.securityweek.com/white-house-says-at-least-8-us-telecom-firms-dozens-of-nations-impacted-by-china-hacking-campaign/.

100 ‘US agencies confirm Beijing-linked telecom breach involving call records of politicians, wiretaps’, The Record, 14-11-2024, https://therecord.media/us-agencies-confirm-china-telecom-hack-wiretaps.

101 ‘U.S. Wiretap Systems Targeted in China-Linked Hack’, The Wall Street Journal,05-10-2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b?mod=hp_lead_pos1.

102 ‘The cyber threat against the Danish water sector’, cfcs.dk, 04-02-2024, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/-the-cyber-threat-against-the-danish-water-sector-february-2025-.pdf.

103 ‘Datahandelaar lekt locatiegegevens van mogelijk miljoenen mensen’, security.nl, 13-01-2025, https://www.security.nl/posting/872156/Datahandelaar+lekt+locatiegegevens+van+mogelijk+miljoenen+mensen.

104 ‘Italiaans ziekenhuis via lek in firewall getroffen door ransomware-aanval’, security.nl, 24-01-2025, https://www.security.nl/posting/873753/Italiaans+ziekenhuis+via+lek+in+firewall+getroffen+door+ransomware-aanval.

105 ‘Cyber threat bulletin: People’s Republic of China cyber threat activity: PRC cyber actors target telecommunications companies as part of a global cyberespionage campaign’, Canadian Centre for Cyber Security, 19-06-2025, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

106 ‘FBI: Noord-Korea is verantwoordelijk voor hack cryptobeurs Bybit’, Tweakers, 27-02-2025, https://tweakers.net/nieuws/232310/fbi-noord-korea-is-verantwoordelijk-voor-hack-cryptobeurs-bybit.html.

107 ‘North Koreans finish initial laundering stage after more than $1 billion stolen from Bybit’, The Record, 04-03-2025, https://therecord.media/north-koreans-initial-laundering-bybit-hack.

108 https://www.standaard.be/politiek/wallonie-getroffen-door-grootschalige-cyberinbraak/58953114.html.

109 https://research.checkpoint.com/2025/apt29-phishing-campaign/.

110 ‘Norway spy chief blames Russian hackers for dam sabotage in April’, Reuters, 13-08-2025, https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/.

111 ‘Britse supermarktketen Co-op meldt lege schappen door cyberaanval’, 12-05-2025, Security.nl, https://www.security.nl/posting/887521/Britse+supermarktketen+Co-op+meldt+lege+schappen+door+cyberaanval.

112 ‘Co-op boss confirms all 6.5m members had dates stolen’, BBC, 16-07-2025, https://www.bbc.com/news/articles/cqlopleo66po.

113 ‘Scattered Spider Behind Cyberattacks on M&S and Co-op, Causing Up to $592M in Damages’, 21-06-2025, The Hacker News, https://thehackernews.com/2025/06/scattered-spider-behind-cyberattacks-on.html.

114 ‘CrowdStrike Services Observes SCATTERED SPIDER Escalate Attacks Across Industries’, CrowdStrike, 02-06-2025, https://www.crowdstrike.com/en-us/blog/crowdstrike-services-observes-scattered-spider-escalate-attacks/.

115 ‘Orange, France’s largest telecoms company, hit by cyberattack’, The Record, 29-07-2025, https://therecord.media/orange-telecom-france-cyberattack.

116 ‘Orange Telecom bevestigt publicatie van gestolen data op internet’, security.nl, 23-08-2025, https://www.security.nl/posting/901877/Orange+Telecom+bevestigt+publicatie+van+gestolen+data+op+internet.

117 ‘Luxembourg probes reported attack on Huawei tech that caused nationwide telecoms outage’, The Record, 01-08-2025, https://therecord.media/luxembourg-telecom-outage-reported-cyberattack-huawei-tech.

118 ‘Orange België meldt hack waarbij gegevens van 850.000 klanten zijn gestolen’, Tweakers, 20-08-2025, https://tweakers.net/nieuws/238256/orange-belgie-meldt-hack-waarbij-gegevens-van-850000-klanten-zijn-gestolen.html.

119 ‘Gegevens van 6,4 miljoen klanten van Bouygues Telecom gestolen bij datalek’, Tweakers, 07-08-2025, https://tweakers.net/nieuws/237874/gegevens-van-6-komma-4-miljoen-klanten-van-bouygues-telecom-gestolen-bij-datalek.html.

120 ‘Google: data potentiële Ads-klanten gestolen bij inbraak Salesforce-omgeving’, Security.nl, 11-08-2025, https://www.security.nl/posting/900106/Google%3A+data+potenti%C3%ABle+Ads-klanten+gestolen+bij+inbraak+Salesforce-omgeving.

121 ‘Cisco lekt persoonlijke gegevens van gebruikers op Cisco.com’, Security.nl, 05-08-2025, https://www.security.nl/posting/899574/Cisco+lekt+persoonlijke+gegevens+van+gebruikers+op+Cisco_com.

122 ‘Verzekeraar Allianz slachtoffer in golf Salesforce-hacks’, Techzine, 13-08-2025, https://www.techzine.nl/nieuws/security/568452/verzekeraar-allianz-slachtoffer-in-golf-salesforce-hacks/.

123 ‘Colt Telecom attack claimed by WarLock ransomware, data up for sale’, Bleepingcomputer, 15-08-2025, https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/.

124 ‘Widespread Data Theft Targets Salesforce Instances via Salesloft Drift’, Google, 26-08-2025, https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift.

125 ‘BREAKING: UNC6395 – The Biggest SaaS Breach of 2025’, Obsidian, 28-08-2025, https://www.obsidiansecurity.com/blog/unc6395-salesloft.

126 ‘Zscaler, Palo Alto Networks Breached via Salesloft Drift’, DarkReading, 02-09-2025, https://www.darkreading.com/cyberattacks-data-breaches/zscaler-palo-alto-networks-breached-salesloft-drift.

127 ‘Cloudflare bevestigt impact Salesloft Drift-datalek op klanten’, Techzine, 03-09-2025, https://www.techzine.nl/nieuws/security/569168/cloudflare-bevestigt-impact-salesloft-drift-datalek-op-klanten/.

128 ‘Statement on cyber incident’, Jaguar Land Rover, 02-09-2025, https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident.

129 ‘Statement on cyber incident’, Jaguar Land Rover, 10-09-2025, https://media.jaguarlandrover.com/news/2025/09/statement-cyber-incident-1.

130 ‘M&S hackers claim to be behind Jaguar Land Rover cyber attack’, BBC, 03-09-2025, https://www.bbc.com/news/articles/c4gqepe53550.

131 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

132 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

133 ‘Dreigingsbeeld Statelijke Actoren (DBSA) 2025’, AIVD, MIVD, NCTV, 17-07-2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

134 ‘Veranderende wereldorde bevestigt belang van een weerbaar Nederland’, NCTV, 17-07-2025, https://www.nctv.nl/actueel/nieuws/2025/07/17/veranderende-wereldorde-bevestigen-belang-van-een-weerbaar-nederland.

135 ‘Openbaar jaarverslag 2024’, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

136 ‘‘Onze aanvallen gaan door!’: Pro-Russische hackers willen wraak na internationale politieactie’, Pointer, 08-08-2025, https://pointer.kro-ncrv.nl/aanvallen-gaan-door-pro-russische-hackers-wraak-internationale-politieactie; ‘“I’ll be back”: pro-Russische hackersgroep is ondanks grote Europol-actie actiever dan ooit, ook in België’, VRT, 08-08-2025, https://www.vrt.be/vrtnws/nl/2025/08/06/check-pro-russische-hackers-noname-actief-europol/.

137 ‘AIVD en MIVD onderkennen nieuwe Russische cyberactor’, AIVD & MIVD, 27-05-2025, https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor .

138 ‘AIVD en MIVD onderkennen nieuwe Russische cyberactor’, AIVD & MIVD, 27-05-2025, https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor.

139 ‘Openbaar jaarverslag 2024’, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

140 ‘Dreigingsbeeld Statelijke Actoren (DBSA) 2025’, AIVD, MIVD, NCTV, 17-07-2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

141 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

142 ‘Openbaar jaarverslag 2024’, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

143 ‘Openbaar jaarverslag 2024’, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

144 ‘Openbaar jaarverslag 2024’, MIVD, 22-05-2025, https://www.defensie.nl/downloads/jaarverslagen/2025/04/22/openbaar-jaarverslag-2024-militaire-inlichtingen--en-veiligheidsdienst.

145 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

146 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

147 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

148 ‘The most notorious instances of commercial spyware’, Kaspersky, 21-03-2024, https://www.kaspersky.com/blog/commercial-spyware/50813/; ‘Buying Spying: How the commercial surveillance industry works and what can be done about it’, Google Threat Analysis Group, 06-02-2024, https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

149 ‘Strengthening America’s Resilience Against the PRC Cyber Threats’, Cybersecurity and Infrastructure Security Agency (CISA), 15-01-2025, https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats.

150 ‘Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks’, The Hacker News, 21-02-2025, https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html.

151 ‘China used three private companies to hack global telecoms, U.S. says’, NBC News, 22-09-2025, https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543.

152 ‘At least 8 US telcos, dozens of countries impacted by Salt Typhoon breaches, White House says’, The Record, 05-12-2024, https://therecord.media/eight-telcos-breached-salt-typhoon-nsc.

153 ‘Chinese Hackers Are Said to Have Targeten Phones Used by Trump and Vance’, The New York Times, 25-10-2024, https://www.nytimes.com/2024/10/25/us/politics/trump-vance-hack.html.

154 ‘How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons’, The Wall Street Journal, 04-01-2025, https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?msockid=30240.

155 ‘Panorama de la Cybermenace 2024’, ANSSI, 11-03-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

156 ‘Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history’, The Washington Post, 21-11-2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

157 ‘Nederlandse providers doelwit van Salt Typhoon’, Defensie.nl, 28-08-2025, https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

158 ‘Kleine Nederlandse providers waren volgens AIVD doelwit van Chinese hackersgroep’, Tweakers.net, 28-08-2025, https://tweakers.net/nieuws/238510/kleine-nederlandse-providers-waren-volgens-aivd-doelwit-van-chinese-hackersgroep.html.

159 ‘China used three private companies to hack global telecoms, U.S. says’, NBC News, 22-09-2025, https://www.nbcnews.com/tech/security/china-used-three-private-companies-hack-global-telecoms-us-says-rcna227543.

160 ‘Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history’, The Washington Post, 21-11-2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/

161 ‘Top senator calls Salt Typhoon ‘worst telecom hack in our nation’s history’, The Washington Post, 21-11-2024, https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/.

162 ‘Telecom giant Viasat breached by China’s Salt Typhoon hackers’, BleepingComputer, 19-06-2025, https://www.bleepingcomputer.com/news/security/telecom-giant-viasat-breached-by-chinas-salt-typhoon-hackers/.

163 ‘Cyber threat bulletin: People’s Republic of China cyber threat activity: PRC cyber actors target telecommunications companies as part of global espionage campaign, 19-06-2025, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

164 ‘China’s Salt Typhoon Hackers Target Canadian Telecom Firms’, SecurityWeek, 23-06-2025, https://www.securityweek.com/chinas-salt-typhoon-hackers-target-canadian-telecom-firms/.

165 ‘Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector‘, Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK, 13-03-2025, https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/.

166 ‘Panorama de la cybermenace 2024’, ANSSI, 11-03-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

167 ‘Panorama de la cybermenace 2023’, ANSSI, 23-02-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/.

168 ‘Panorama de la cybermenace 2024’, ANSSI, 11-03-2025, https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-003/.

169 ‘Dreigingslandschap Vitale Infrastructuur (2025)’, 24-07-2025, NCTV, https://www.nctv.nl/documenten/publicaties/2025/07/23/dreigingslandschap-vitale-infrastructuur.

170 ‘De staat van de digitale infrastructuur’, EZ, 22-01-2024, https://open.overheid.nl/documenten/9c5f2d91-fafc-405e-b330-96d6211677bc/file.

171 ‘Vooral jongeren en ouderen pinnen vaker aan de kassa’, De Nederlandsche Bank, ’01-04-2025’, https://www.dnb.nl/algemeen-nieuws/nieuws-2025/vooral-jongeren-en-ouderen-pinnen-vaker-aan-de-kassa/.

172 ‘Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector‘, Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK, 13-03-2025, https://www.cfcs.dk/da/nyheder/2025/ny-trusselsvurdering---telesektoren/.

173 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

174 ‘Jaarverslag 2024’, AIVD, 24-04-2025, https://www.aivd.nl/onderwerpen/jaarverslagen/jaarverslag-2024.

175 https://zoek.officielebekendmakingen.nl/kst-30821-92.html.

176 ‘Cybertruslen mod telesektoren i Danmark/De cyberdreiging voor de telecommunicatiesector‘, Styrelsen for Samfundssikkerhedspressekontakt/SAMSIK.

177 ‘Russian hackers infiltrated Ukrainian telecom giant months before cyberattack’, The Record, 04-01-2025, https://therecord.media/russians-infiltrated-kyivstar-months-before.

178 ‘Cyber Security Assessment Netherlands 2024’, NCTV, 28-10-2024, https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024.

179 “Toenemende en veranderende dreigingen op infrastructuur”, 24-07-2025, NCTV, https://www.nctv.nl/actueel/nieuws/2025/07/24/toenemende-en-veranderende-dreigingen-op-vitale-infrastructuur.

180 https://www.nctv.nl/onderwerpen/cyberbeveiligingswet.

181 Interview with the RDI, 2025.

182 ‘Aftapvoorziening Vodafone niet voldoende beveiligd: boete van €2,25 miljoen voor Vodafone, RDI, 22-10-2024.

183 ‘Aftapvoorziening Vodafone niet voldoende beveiligd: boete van €2,25 miljoen voor Vodafone, RDI, 22-10-2024, https://www.rdi.nl/actueel/nieuws/2024/10/22/aftapvoorziening-vodafone-niet-voldoende-beveiligd.

184 ‘Tekortkomingen in beveiliging van aftapvoorziening’, RDI, 30-08-2022, https://www.rdi.nl/actueel/nieuws/2022/08/30/tekortkomingen-in-beveiliging-van-aftapvoorziening-kpn.

185 https://www.defensie.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon, Ministerie van Defensie, 28-08-2025.

186 ‘Voortgang kabinetsaanpak risicovolle strategische afhankelijkheden’, Ministerie van Economische Zaken, 21-10-2024, https://open.overheid.nl/documenten/18329adb-dac7-45ab-bba4-0c777758528f/file.

187 Aanbieden Agenda Digitale Open Strategische Autonomie, Ministerie van Economische Zaken en Klimaat, 17-10-2023, https://www.rijksoverheid.nl/documenten/kamerstukken/2023/10/17/kamerbrief-aanbieden-agenda-digitale-open-strategische-autonomie-coco-5-oktober.

188 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Long-term competitiveness of the EU: looking beyond 2030, Europese Commissie, 16-03-2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1668.

189 ‘Agenda digitale open strategische autonomie’, Ministerie van Economische Zaken en Klimaat, 17-10-2023, https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa.

190 ‘Agenda digitale open strategische autonomie’, Ministerie van Economische Zaken en Klimaat, 17-10-2023, https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa.

191 Short address by Prime Minister Dick Schoof at the opening of the One Conference, The Hague, 30 September 2025, https://www.rijksoverheid.nl/documenten/toespraken/2025/09/30/toespraak-minister-president-schoof-bij-opening-one-conference-den-haag.

192 ‘Samenleving kwetsbaar: digitale afhankelijkheid is meer dan cloud bij de overheid’, Rathenau Instituut, 09-07-2025,https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/samenleving-kwetsbaar-digitale-afhankelijkheid-meer-dan-cloud-bij-de-overheid?utm_source=Laposta&utm_campaign=Nieuwsbrief%20juli&utm_medium=email; ‘Minister: volledige afhankelijkheid niet-Europese techbedrijven onwenselijk’, Security.nl, 07-07-2025, https://www.security.nl/posting/895166/Minister%3A+volledige+afhankelijkheid+niet-Europese+techbedrijven+onwenselijk; ‘Overheid leunt veel meer op Amerikaanse cloud dan bekend: ‘Meelezen is makkelijk’’, NOS, 31-05-2025, https://nos.nl/artikel/2569392; ‘Amerikaanse bedrijven domineren Europese markt voor cybersecurity’, Security.nl, 30-04-2025, https://www.security.nl/posting/886170/Amerikaanse+bedrijven+domineren+Europese+markt+voor+cybersecurity; ‘Bedrijven onderzoeken ontsnapping uit de Amerikaanse cloud’, Financieel Dagblad, 21-04-2025, https://fd.nl/bedrijfsleven/1552548/bedrijven-onderzoeken-ontsnapping-uit-amerikaanse-cloud; ‘Europese techbedrijven willen ‘radicale actie’ tegen afhankelijkheid van Amerikaanse Big Tech’, NRC, 18-03-2025, https://www.nrc.nl/nieuws/2025/03/18/europese-techbedrijven-willen-radicale-actie-tegen-afhankelijkheid-van-amerikaanse-big-tech-a4886724.

193 ‘Beheer van CVE-bugs komt in gevaar door verlopen contract met Mitre Corporation’, Tweakers, 16-04-2025, https://tweakers.net/nieuws/233988/beheer-van-cve-bugs-komt-in-gevaar-door-verlopen-contract-met-mitre-corporation.html.

194 ‘Amerikaanse cybersecurityagentschap redt CVE-programma met financiering’, Tweakers, 16-04-2024, https://tweakers.net/nieuws/234022/amerikaans-cybersecurityagentschap-redt-cve-programma-met-financiering.html.

195 ‘Nederland en de EU: Zet in op cloudsoevereiniteit’, Clingendael, 16-4-2024, https://www.clingendael.org/publication/nederland-en-de-eu-zet-op-cloudsoevereiniteit#:~:text=Amerikaanse%20bedrijven%2070%2D80%20procent%20van%20de%20Europese%20markt%20voor%20clouddiensten.

196 ‘Samenleving kwetsbaar: digitale afhankelijkheid is meer dan cloud bij de overheid’, Rathenau Instituut, 09-07-2025, https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/samenleving-kwetsbaar-digitale-afhankelijkheid-meer-dan-cloud-bij-de-overheid?utm_source=Laposta&utm_campaign=Nieuwsbrief%20juli&utm_medium=email.

197 ‘De werking van de CLOUD-Act bij dataopslag in Europa’, NCSC, 16-08-2022, https://www.ncsc.nl/actueel/weblog/weblog/2022/de-werking-van-de-cloud-act-bij-dataopslag-in-europa.

198 ‘Microsoft admits it ‘cannot guarantee’ data sovereignty’, the Register, 25-07-2025, https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee/.

199 https://www.submarinecablemap.com/, https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/09/23/kamerbrief-voortgangsupdate-onderzeese-datakabels-kamerbrief-voortgangsupdate-onderzeese-datakabels.

200 https://www.digitaleoverheid.nl/kabinetsbeleid-digitalisering/werkagenda/versterken-digitale-samenleving-op-caribisch-deel-koninkrijk/.

201 https://www.rijksoverheid.nl/documenten/kamerstukken/2025/06/19/kamerbrief-over-voortgang-digitalisering-van-de-zorg-in-caribisch-nederland-2025.

202 https://www.eerstekamer.nl/wetsvoorstel/36639_wet_invoering_bsn_en.

203 https://belastingdienst.cw/beperkte-dienstverlening-belastingdienst-na-ransomware-aanval/.

204 https://nos.nl/artikel/2577274-werkzaamheden-instanties-caribische-eilanden-verstoord-door-hacks, https://therecord.media/aruba-curacao-governments-cyberattacks.

205 ‘Van kwetsbaar naar weerbaar’, Algemene Bestuursdienst, 12-09-2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar.

206 ‘Cyber Security Assessment Netherlands 2024’, NCTV, https://www.nctv.nl/documenten/2024/10/28/cybersecuritybeeld-nederland-2024.

207 ‘Van kwetsbaar naar weerbaar’, Algemene Bestuursdienst, 12-09-2025, https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar.

208 ‘AI versterkt bestaande dreigingen voor nationale veiligheid’, NCTV, 10-12-2024, https://www.nctv.nl/actueel/nieuws/2024/12/09/ai-versterkt-bestaande-dreigingen-voor-nationale-veiligheid.

209 Cyber Security Assessment Netherlands 2023, NCTV, 03-07-2023, https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023.

210 'OPWNAI: Cybercriminals starting to use ChatGPT', Check Point Research, 06-01-2023,; 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

211 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

212 'Beyond the Safeguards: Exploring the Security Risks of ChatGPT', Erik Derner & Kristina Batistic, 13-05-2023, https://arxiv.org/abs/2305.08005.

213 'Beyond the Safeguards: Exploring the Security Risks of ChatGPT', Erik Derner & Kristina Batistic, 13-05-2023, https://arxiv.org/abs/2305.08005. 'ChatGPT and large language models: what's the risk?', National Cyber Security Centre, 10-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

214 'Phishing and Social Engineering in the Age of LLMs', S. Gallagher et al., in 'Large Language Models in Cybersecurity', A. Kucharavy, O. Plancherel, V. Mulder, A. Mermoud, and V. Lenders (eds.)., Springer, 2024, https://library.oapen.org/bitstream/handle/20.500.12657/90897/978-3-031-54827-7.pdf#page=94.

215 Cyber Security Assessment Netherlands 2023, NCTV, 03-07-2025, https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023.

216 'ChatGPT and large language models: what's the risk?', National Cyber Security Centre, 10-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

217 'ChatGPT and large language models: what's the risk?', National Cyber Security Centre, 10-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

218 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

219 'Human-competitive AI will disrupt the cyber security industry; prepare now!', Partnership for Cyber Security Innovation, 19-09-2023, https://pcsi.nl/nl/nieuws/vision-paper-human-competitive-ai-will-disrupt-the-cyber-security-industry-prepare-now/.

220 'Human-competitive AI will disrupt the cyber security industry; prepare now!', Partnership for Cyber Security Innovation, 19-09-2023, https://pcsi.nl/nl/nieuws/vision-paper-human-competitive-ai-will-disrupt-the-cyber-security-industry-prepare-now/.

221 'Generatieve AI: een transformatieve impact op cybersecurity', AIVD en RDI, 17-10-2024, https://www.aivd.nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity.

222 'Versterkte dreigingen in een wereld vol kunstmatige intelligentie', AIVD, MIVD, NCTV, 10-12-2024, https://www.nctv.nl/documenten/publicaties/2024/12/09/versterkte-dreigingen-in-een-wereld-vol-kunstmatige-intelligentie.

223 'Growing Number of Threats Leveraging AI', Symantec, 25-07-2024, https://www.security.com/threat-intelligence/malware-ai-llm.

224 'Cybercriminal abuse of large language models', Cisco Talos, 25-05-2025, https://blog.talosintelligence.com/cybercriminal-abuse-of-large-language-models/.

225 'Adversarial Misuse of Generative AI', Google Threat Intelligence, 29-01-2025, https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.

226 'Jaarbeeld Ransomware 2024', Project Melissa, 17-02-2025, https://www.ncsc.nl/documenten/publicaties/2025/02/17/jaarbeeld-ransomeware-2024.

227 'Jaarbeeld Ransomware 2024', Project Melissa, 17-02-2025, https://www.ncsc.nl/documenten/publicaties/2025/02/17/jaarbeeld-ransomeware-2024.

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

229 'Datalekkenrapportage 2024: datadiefstal bijna verdubbeld', Autoriteit Persoonsgegevens, 03-07-2025, https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2024.

Publication details

The Cybersecurity Assessment Netherlands, 2025 (CSAN 2025) provides insight into the digital threat, the interests that it may affect, digital resilience and, lastly, digital risks. In addition, the CSAN 2025 serves as a substantive basis for evaluating the action plan under the Netherlands Cybersecurity Strategy 2022–2028. The CSAN focuses on national security.

The National Coordinator for Security and Counterterrorism (NCTV) prepares the CSAN. The NCTV has gratefully drawn on the information, insights and expertise of government services, providers of critical processes, scientists and other parties. The General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) also make substantial contributions to the CSAN. 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. As coordinator, the NCTV provides a strategic link between all relevant partners in the security domain to reduce national security risks and – when necessary – to manage national crises.

The NCSC helps strengthen the Netherlands' digital resilience and, in doing so, creates a favourable digital climate for organisations and society as a whole. The NCSC does this through cooperation with 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 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

November 2025