National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

Cyber Security Assessment Netherlands 2023

The development of "Generative AI," a form of AI that can create new content from existing content based on prompts or questions that are entered by users, is rapidly advancing. Its impact on society is still unclear. This topic will also be addressed in this CSAN (p.41). In order to illustrate its capabilities, the cover image of this CSAN was generated using Midjourney. Midjourney creates images from natural language descriptions called prompts. The following prompt was used for this cover image: Skyline of Zuidas from above, digital ecosystem with technology and connections. Daylight, Photorealistic photography, real life. A real photo of the Zuidas was placed below for comparison.

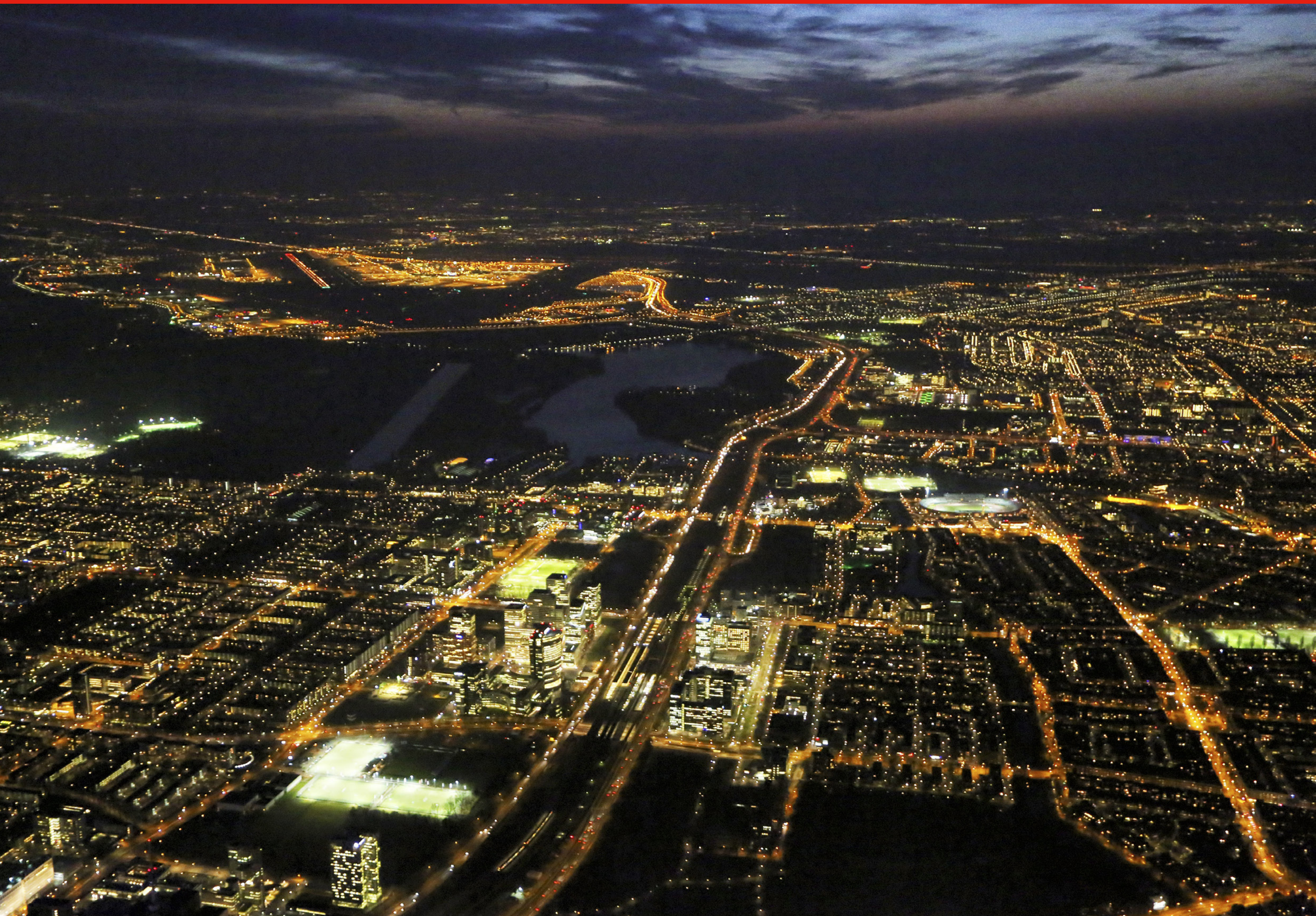

Table of contents

Expect the unexpected

If there is one area in which experiences from the past do not provide guarantees for the future it is digital security. Digital security demands a continuous and complex balancing act in order to bring or keep in balance the divergent interests, digital threats and digital resilience. Many parties make efforts to increase digital resilience and remain free from cyber incidents. For organisations it is still the case that implementing basic measures in the area of cybersecurity can already have a great impact. However, cyber incidents cannot always be prevented. They can occur unexpectedly and they can have an unexpected cause, nature and impact.

This chapter contains the main messages of this CSAN. Further substantiation is provided in chapters two up to and including five.

Principal findings CSAN 2023

1. The security of digital processes is and remains essential in our highly digitised society and is therefore linked inextricably to national security.
2. The digital threat for the Netherlands remains as high as ever. That threat does however change continuously. Geopolitics are hardening with the Russian war against Ukraine as a prime example. That war, among other factors, has contributed to a revival of hacktivism: carrying out cyberattacks for ideological reasons. If further escalation of the war occurs, the digital threat may change abruptly and Dutch interests may be affected.
3. The strategic themes set out in the CSAN 2022 still fully result in complications for risk control. Several changes when compared to last year stand out:
   - the additional digital security requirements that arise, inter alia, from new European legislation and regulations;
   - the insurability of digital risks is under pressure;
   - the ever-increasing interwovenness within a broader, not just digital, ecosystem;
   - the opportunity structure for cyberattacks formed by the digital ecosystem.
4. Reduction of the imbalance between the digital threat and resilience referred to in the CSAN 2022 remains a major task. The nature of the digital risks to national security has not fundamentally changed.
5. Operational technology (OT) is a vulnerable building block for vital processes. OT plays a central role within the control, monitoring and management of physical processes within (vital) organisations. OT security is of vital importance, but faces important challenges. There is room for improvement despite the growing attention for the resilience of OT.
6. The special characteristics of digital risks demand a broader method of risk management than other risks. For example digital risks form part of a broader, dynamic and complex range of risks and cyberspace is a highly complex system that is difficult to understand fully. A broader method of risk management could be an approach in which digital risks are perceived as an integral part of the risks to national security. Furthermore, the angle of 'assume breach' (assume that there is a cyber incident) could be useful.

Digital threat as great as ever

The digital threat to the Netherlands remains as high as ever, especially as a result of:

1. The interaction with other, partially non-digital threats and developments. For example, cyber incidents can be the result of a disruption to the energy supply. They can in turn become the cause of a disruption to the energy supply. In addition, there is a whole tangle of developments that has an impact on digital threats. One example concerns the technological developments in what is known as 'Generative AI', including ChatGPT, Quantum computing and 'the metaverse'. Threats may also accumulate steadily without being noticed until a tipping point is reached. It is very difficult to reverse those threats once that point has been reached. Such a steady accumulation may occur for example in the case of dependencies of companies with a dominant position in the services and/or digital markets.

2. The complexity and interwovenness of digital processes, systems and networks and the large (growing) attack surface combined with widespread outdated information systems. This results in vulnerabilities that can be exploited by cyber actors. The probability of large-scale failure is also increasing.

3. Geopolitical tensions as a result of which state actors use cyberattacks as a means of promoting their interests, resulting in chain effects for example. The war against Ukraine is a prime example of that hardening (see below in this chapter).

4. The attractive revenue model for cybercriminals. For example, criminals not only earn money from ransom payments and illegal services such as Cybercrime-as-a-Service (CaaS). Enrichment of stolen information with other information and the sale thereof are also lucrative for criminals.

5. International conflicts and socially-controversial subjects as a possible reason for hacktivism.

6. The concentration of information and digital processes, which are very attractive to exploitation by malicious actors and may have major consequences in case of failures. This applies to cloud service providers for example.

7. The limited chance for malicious actors of being caught and/or extradited for carrying out a cyberattack.

Cyber incidents in 2022/2023 in line with the assessment of the digital threat

Cyber incidents that occurred in the period from March 2022 up to and including February 2023 match the assessment of the digital threat over the past years. There were no cyber incidents in the Netherlands or other EU countries that disrupted society. The nature of the cyber incidents remained diverse. Ransomware again formed a prominent part of the cyberattacks. This was sometimes accompanied by publication of the information stolen. Failure of digital processes also occurred relatively often. Cyberattacks carried out by hacktivists - mainly from abroad, but also a few from within the Netherlands - stood out when compared to previous years. Several cyber incidents also made extra clear that organisations are part of a broader ecosystem and may be confronted with cyber incidents within that ecosystem.

The war against Ukraine: extensive cyber campaign, less impact than expected

Russia invaded Ukraine in February 2022. Russian cyberattacks focused mainly on Ukraine and the region. It concerned espionage and (acts in preparation of) sabotage. Russia also spread disinformation. The Ukrainian and western digital defence were able to limit the impact of Russia's continuous attack attempts.

Russian cyber operations focus on espionage in order to obtain military, diplomatic and economic information from both Ukraine and NATO Member States. With regard to NATO, the Russian need for intelligence focuses, inter alia, on the military support being provided to Ukraine via the NATO Member States. The Russian cyber sabotage campaign against Ukraine is the most large-scale and intensive in history, according to the Dutch General Intelligence and Security Service (AIVD) and the Dutch Military Intelligence and Security Service (MIVD).

The involvement of criminal and hacktivist actors within the context of the war stands out. One further characteristic element of the development of the war is that private companies provide support to Ukraine. This often takes place in cooperation with states that provide support to Ukraine. Russia is also involved in influencing public opinion in western countries by spreading disinformation, among other things.

Disruptive cyberattacks that harm Dutch national security have not (yet) occurred. The digital threat may change abruptly if the war escalated further. Cyberattacks could start affecting national security if this is the case. The Netherlands may also be affected by chain effects that have an impact on vital processes and (continue to) be confronted with attacks by, for example, pro-Russian criminals.

Strategic themes still fully result in complications for risk control

In the CSAN 2022, the NCTV, in cooperation with partners, identified six strategic themes that will be relevant to the digital security of the Netherlands in the coming years. These themes still apply in full. Several changes stood out during the reflection on these themes. They are discussed below.

Strategic themes indicated in the CSAN 2022

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

Additional requirements for digital security, but it will take time before they become effective

The additional requirements for digital security constitute an important change that can increase digital resilience in the coming years. They arise from new European legislation and regulations, the Dutch Cybersecurity Strategy 2022-2028 and the action plan derived from it. Awareness and further development and implementation of all of the above will however take some time.

Hardening of geopolitical tensions

Geopolitical tensions increased further over the past year. Sectors and organisations may experience the consequences of this hardening, but can do little about it. It does constitute a factor that must be taken into account when determining the desired level of digital resilience. For example, a state actor could attack an ICT service provider of a vital organisation as a springboard to that digital organisation.

Insurability digital risks under pressure

Although organisations can do a lot with regard to digital resilience, cyber incidents can nevertheless occur and/or damage cannot always be prevented. The insurability of digital risks is under pressure for various reasons. The first reason mentioned by insurers is the increase in digital risks. A second reason is that cyber incidents can grow into what is known as a systemic crisis and therefore become uninsurable. In addition, the market for cybersecurity insurance in the Netherlands is limited in size and in its infancy. The result of that pressure is or could be: exclusion of organisations with an increased risk profile, premiums that are too high for organisations or the exclusion of damage resulting from many types of cyber incidents. All of the above may ultimately result in financially-healthy organisations collapsing due to damage they sustain as a result of cyber incidents.

Being part of a broader ecosystem complicates risk control

Whether it concerns countries, sectors or organisations, few will be able to function independently of a broader ecosystem. This includes things like outsourcing parts of the business operations, such as the salary administration, access pass management or market research. Being part of a broader ecosystem has advantages, such as benefiting from economies of scale and specialist knowledge, including in the area of cybersecurity.

At the same time, being part of a broader ecosystem also complicates risk control. Insight into dependencies and vulnerabilities in the broader ecosystem does not always exist. Moreover, it is difficult to get these under control. Those dependencies and vulnerabilities can form a substantial part of the digital risks. One prominent example of this occurred in 2023. Large organisations hired research agencies to carry out a customer survey. Several research agencies in turn used the same software supplier. When a data breach occurred at that software supplier, the data of an estimated two million Dutch citizens were made public. This example therefore involved the customers of an organisation falling victim to a data breach at a service provider of the service provider of the organisation, i.e. in the third line.

The digital ecosystem forms an opportunity structure for cyberattacks

Cybercriminals are part of a broader mala fide and bona fide digital ecosystem and therefore depend on it. This ecosystem therefore forms an opportunity structure for them. The increasing specialisation among cybercriminals means they also become more dependent on each other's (online) services within the context of cyber-crime-as-a-service. Other actors, sometimes state actors, also make use of these services. This dependency also applies to the purchase of legal services, such as webhosting and communication services such as VPN or domain registrations. By contrast, this dependency also provides opportunities for increasing digital resilience. Where it concerns internet services in the broader sense, principles such as acceptable use, know-your-customer, the principle of due diligence and anti-exploitation provisions are often still without obligation, resulting in ample scope for compliance or non-compliance. This offers cybercriminals many opportunities to work anonymously and in a scalable manner - opportunities which they take.

OT: a vulnerable building block for vital processes

Operational technology (OT) within industrial networks, also referred to as 'Industrial Automation and Control Systems' (IACS), plays a central role within the control, monitoring and management of physical processes within organisations. It therefore also functions as the engine of vital sectors. OT is becoming ever more intertwined with information technology (IT). In addition, the 'Industrial Internet of Things' (IIoT) plays an increasingly important role in industrial environments. This implies benefits for process optimisation, but it also implies risks. For example, this development increases the attack surface and therefore the risk that OT systems become compromised. It also implies challenges with respect to securing such systems. Detection and mitigation of digital attacks among other things play an ever more important role in this connection. There is room for improvement in this and other areas. This requires specific knowledge, competencies and cooperation. Over the past years, the government has developed multiple initiatives to support this process. Organisations are increasingly able to work together in this connection. This provides opportunities to build on in order to safeguard the resilience of vital processes.

Reducing the imbalance between the digital threat and resilience is still a major task

Reducing the imbalance between the digital threat and resilience referred to in the CSAN 2022 remains a major task: the reason being that the digital threat is undiminished and the complications to risk control continue to apply in full.

The nature of the digital risks has not changed fundamentally when compared to CSAN 2022. There are four risks to national security (see the frame below). They also apply directly or indirectly to specific sectors and organisations and individual citizens.

Four national security risks

1. Unauthorised access to information (and possibly its publication), in particular through espionage. Examples include espionage targeting communications within the central government or the development of innovative technologies. It also involves access to information about employees or business processes as a springboard for cyberattacks or other malicious purposes.
2. Inaccessibility of processes, due to sabotage of processes responsible for the energy supply, or from cybercrime, including the application of ransomware and DDoS attacks.
3. Breaches of (the security of) cyberspace, such as through the misuse of global chains of ICT service providers, the exploitation of internet protocols or the sabotage of cables.
4. Large-scale outages: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action.

All digital processes, organisations and sectors are vulnerable

All digital processes, organisations and sectors are potentially vulnerable to cyber incidents. They may be confronted directly with cyberattacks by malicious actors. This applies in particular to unauthorised access to information (and its possible publication). This also applies to the inaccessibility of processes resulting from (the preparation for) sabotage, the application of ransomware and DDoS attacks. And all countries, sectors and organisations may be confronted indirectly with the consequences of a cyberattack on a different organisation or large-scale failure within the broader ecosystem, such as when a global service provider is affected.

One argument that is often heard is that “states are not interested in my organisation”, “there is nothing to get from me” or “there are few incidents in our sector”. However, this fails to take into account for example that criminals continuously attempt to open all ‘digital doors’ irrespective of the organisation, with all related consequences for the victims. State actors actively search for organisations within chains as a stepping stone to (more) interesting targets. For example, the AIVD discovered in 2022 among other things that various countries with an offensive cyber programme were attempting to steal data within the (European) travel and aviation sector. They combine that information with other data in order to identify, trace or follow people who are interesting to them. Organisations that process a lot of data are therefore an attractive target to cyber actors. Another example concerns ICT service providers that work for many organisations. Organisations can also be attacked if systems contain a vulnerability, without a malicious actor checking to see what kind of organisation it concerns. Symbolic Dutch targets, such as internationally-known Dutch multinationals or authorities, may also be a target, with the underlying motive of revenge against the Netherlands or the Dutch government. For example, support for Ukraine from the Netherlands could be reason for hacktivists to carry out DDoS attacks or digital defacement of websites.

Special characteristics of digital risks require a broader method of risk management

Digital risks have several special characteristics that demand a broader method of risk management than other risks. This applies at the level of organisations, but certainly at the sectoral and national level as well. Firstly, digital risks form part of a broader, dynamic and complex range of risks. There is for example interaction with other, certainly also non-digital threats and developments. Reference was also made to risks that arise from the broader ecosystem of which countries, sectors and organisations form part. It is also the case that cyberspace is an extremely complex system when compared to other risks. Although information about cyber incidents is sometimes available, it is not nearly available to everyone. It is only comparable to a limited extent and difficult to interpret. For example, for the purpose of controlling floods a lot more information is available and over a longer period of time. Simulating incidents or building models in order to analyse the progress and consequences of incidents is useful to risk management in general, but highly complex where it concerns digital risks. Because who can oversee the impact of large-scale disruption of internet services in the Netherlands over several days on digital processes and the consequences thereof for society, sectors and organisations? And it goes without saying that the internet cannot be disconnected for a day to see what will happen.

It follows from the nature of the importance of digital security and the nature of the digital threat that controlling digital risks is certainly not only an issue for technical experts. It is also, or perhaps mainly, an issue of governance and/or risk management for politicians and managers at the level of organisations, sectors and countries. Digital risks are an integral part of a broader range of risks and therefore require integral risk management. New European legislation and regulations mean that directors of many organisations within the EU have a larger responsibility for digital security laid down in law.

If there is one area in which experiences from the past do not provide guarantees for the future it is digital security. This is the reason for the appeal to look beyond incidents that have occurred and beyond the requirements that legally must be met. This applies for example to anticipating the possible consequences to digital security of generative AI, which is undergoing rapid development, and Quantum computing. Another useful perspective is assuming that a cyber incident is already happening. This results in a broader scope than for example performing a check to establish whether technical measures have been implemented to prevent customer or employee information from being accessed by unauthorised persons. Focussing on a situation in which customer or employee information was actually manipulated or placed on the internet can be helpful to risk control. What would the perspective for action be then? What could the scope of the consequences be and how could those consequences still be limited at that time? And then the ultimate question of whether the existing balance between threat, interest and resilience is actually the desired one. In short: “expect the unexpected” and be prepared for it.

Due to a technical failure, a tunnel has to be closed off. As a result, traffic on the highway is jammed. This may cause traffic congestion in the surrounding cities.

1 Introduction

Purpose and scope

The Cybersecurity Assessment Netherlands 2023 (CSAN 2023) provides insight into the digital threat, the interests that may be affected by this, digital resilience and finally the digital risks. CSAN 2023 also aims to provide insight into the possible changes to the strategic themes that were elaborated in the CSAN 2022. These themes formed a substantive basis for the Dutch Cybersecurity Strategy 2022-2028. This CSAN in turn forms a substantive basis for the evaluation of the action plan that is derived from this strategy.

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

The CSAN is intended primarily for strategic planning and policy making at national level (governance). It aims to provide the

Explanation of key concepts

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

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

Cabinet, the members of the Upper and Lower Houses of Parliament, civil servants, policymakers, other public administrators and leaders of organisations with an insight 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 the risk management process. Finally, the CSAN can also be accessed by the general public.

Structure

This CSAN consists of the preceding chapter in which the main messages are set out and of five chapters providing more in-depth information. The chapter preceding this introduction contains the main messages. This structure is intended to allow readers from various target groups to navigate the CSAN easily and focus on subjects that align with their professional role or interest. The chapters providing more in-depth information have the following themes:

- Chapter 2, Annual review, provides an overview of relevant incidents in the Netherlands in the period from March 2022 up to and including February and their interpretation.
- Chapter 3 looks back at the cyber component in the war against Ukraine and assesses what consequences resulted and could result therefrom.
- Chapter 4 addresses the importance of Operational technology (OT) further as well as the risks inherent therein.
- Chapter 5 describes new insights and/or changes that occurred in six strategic themes that constitute complications to strategic risk control.
- Chapter 6 sets out three scenarios in which a cyber incident in a digital ecosystem not only results in problems in the business operations of the organisation where the incident occurs, but also in damage for citizens or other organisations within the ecosystem. This chapter is mainly intended to help the reader anticipate possible incidents.

Appendix 1 provides an explanation of the creation of the CSAN.
Appendix 2 provides the sources and references.

A power outage brings life to a (partial) standstill. Streetlights shut off and household appliances cannot be used. In a hospital, patient care cannot always continue.

2 Annual review

The cyber incidents that occurred in the period from March 2022 up to and including February 2023 match the assessment of the digital threat over the past years. There were incidents in the Netherlands or other EU countries that causes social disruption. The nature of the cyber incidents remained diverse. Cyberattacks were mainly carried out by state and criminal actors. Failure of digital processes occurred relatively often. Cyberattacks carried out by hacktivists mainly from abroad, but some also carried from within the Netherlands, stood out when compared to previous years. Several cyber incidents also made extra clear that organisations are part of a broader ecosystem and may be vulnerable within that ecosystem.

Incidents in the Netherlands are in line with the assessment of digital risks and the type of targets.

Disrupted digital processes predominantly as a result of ransomware attacks

During the reporting period, actors deliberately rendered digital processes inaccessible. This mainly concerned ransomware attacks. These attacks stopped focusing on merely encrypting data a long time ago. Criminals now often also steal data to commit other crimes, such as pressuring victims to pay a ransom by threating to publish these stolen data. Several ransomware attacks actually involved publication of the information and sensitive information was made available to third parties.

The Netherlands was also affected by DDoS attacks by hacktivists

During this reporting period there were several news reports of DDoS attacks, which (briefly) disrupted digital processes. This mainly concerned attacks from outside the Netherlands and by hacktivists. One example is the DDoS attack against the European Parliament in November 2022. Besides that, pro-Russian hacktivists called for DDoS attacks against (inter alia) Dutch hospitals and several hospitals in the Netherlands did actually fall victim to DDoS attacks for a short period of time. In addition to pro-Russian hacktivists, religious hacktivists allegedly carried out DDoS attacks against Dutch websites in retaliation for the tearing up of a Quran. It should be noted in this connection that such groups want media attention and deliberately exaggerate claims and even claim things that did not happen. The attribution of hacktivist activities is difficult as well.

Data breaches by malicious actors and unintentional human action

More than once during this period, we have seen that there was unauthorised access to information and sometimes also publication of stolen information, resulting in data breaches. It often concerned ransomware actors. For example, there was an incident during this period in which an attacker was able to gain access to a healthcare platform and access sensitive information. Unintentional human action can also result in sensitive information being leaked. For example, a technical act by the ICT supplier of the municipality of Veenendaal meant that confidential documents were unintentionally temporarily accessible to the public.

Failure due to technical causes

Large-scale failure of vital processes as a result of technical malfunctioning did not occur during this reporting period, but there were various failure incidents. Failure can have several causes, including technical problems unintentional human action. During this period, technical causes resulted in failures on more than one occasion. An ICT malfunction and failing back-up system that resulted in a considerable train service failure in the Rotterdam region, was reported prominently in the news.[2]

Attacks against non-vital companies can nevertheless affect vital sectors and the Central Government

Incidents illustrate that the broader ecosystem (see chapter 5) presents risks to many organisations because they are highly connected and intertwined with the processes of other organisations. A cyber incident at a non-vital organisation can therefore also have consequences for vital sectors and the Central Government. The ransomware attack against ID-ware is illustrative of how a cyberattack against a non-vital company can nevertheless have an impact on the providers of vital services and the Central Government. Personal data of members of the House of Representatives and the Senate among others were leaked as a result of the attack against this company.

Cyberattacks against municipalities form a risk to sensitive information

A cyberattack against public organisations can have major consequences for the services and operation of these organisations. In addition, sensitive information of several municipalities became public knowledge following cyberattacks. Data breaches at public organisations can affect citizens among others. After all, a lot of sensitive information concerning them is recorded at the municipalities for the performance of statutory tasks. This makes a cyberattack during which information is stolen and leaked extra problematic. Malicious actors can exploit that information for fraud or espionage for example.

Incidents abroad can also occur in the Netherlands

Geopolitical situation impacts threat landscape of the Netherlands

The CSAN 2022 argues that cyberattacks by state actors are the new normal and that countries use cyberspace to obtain geopolitical benefits. During this reporting period, cyber operations were discovered that were related to state actors, including espionage, theft of intellectual property and the use of destructive malware. These cyber operations must certainly be considered in light of geopolitical developments (see further chapter 5).

Exploitation spyware by foreign actors against journalists, politicians and/or dissidents is also conceivable in the Netherlands

Spyware being used to digitally follow journalists, activists, politicians and dissidents for example has been reported on in the news for years. A lot of attention was devoted during this reporting period to the deployment (and exploitation) of spyware in and by European countries. A report from a European investigative committee shows that spyware is also purchased and used in Europe. [3] The main concern in this connection is the exploitation of such software, in which connection the instrument is applied without legal safeguards and used against minorities or people who oppose those in charge. It became known for example that spyware was used against politicians and activists in Poland and Spain, among other places. It is conceivable that foreign powers use spyware against Dutch journalists, activists, dissidents or even politicians. It is also conceivable that criminals use spyware against asset managers for example in order to be able to benefit from their knowledge of sensitive transactions.

Destruction of data by wiperware can also occur in the Netherlands

During the first half of 2022, investigators of cybersecurity companies identified an increase in the use of wiperware, parallel to the war between Russia and Ukraine.[4] New wiperware variants were also discovered later during the reporting period.[5][6] The application of wipers is not limited to the war, however. Various wipers were observed outside the war as well. It became known for example that an advanced cyber actor used a new wiper in attacks against the supply chain of organisations in Israel among other places.[7] It appears criminals are also adding wiper functionalities to their operations. One example is the LokiLocker ransomware, which has a complicated, embedded wiper functionality that can be deployed to extort victims.[8]

Although the scope and impact still appears to be limited in a general sense, several exceptions show that this category is very dangerous due to the characteristics of the malware. After all, this malware renders infected computers inoperable by overwriting and deleting all files. Wipers can take down computers of companies or vital organisations and thus cause social disruption. The fact that it appears that this type of malware occurs more frequently means that in time it could turn up more often in the Netherlands as well, possibly unintentionally.

Cyberattacks against the energy sector also conceivable in the Netherlands

Although companies are not always open about the type of cyberattack, incidents do show that both state and criminal actors carried out attacks against the energy sector. For example, several energy companies in Europe were affected by ransomware and it was revealed that state actors carried out attacks against companies in the oil and gas sector.[9] The energy sector in the Netherlands could be affected as well. This already occurred indirectly when several windmills at the Oude Maas wind park could not conduct test runs as a result of a ransomware attack against German windmill manufacturer Nordex.

An advanced state actor, which the AIVD attributes to an intelligence and/or security service, has since a few years been interested in European and western government information concerning the energy sector. The activities of this actor concern espionage activities in these cases.

National governments are the target of disruptive cyberattacks

During this period, several (disruptive) cyberattacks were carried out against public organisations and (national) governments. Government institutions all over the world were affected by cyberattacks. In addition to ransomware attacks in Latin America, which caused great disruptions in Costa Rica, there were also incidents with drastic consequences in Europe. Montenegro for example had difficulty restoring its government services following an attack with Cuba ransomware. Albania took a large part of its government websites and services offline following a cyberattack. Albania and other NATO Member States attributed the attack to Iran. These and other incidents show that national governments are in the sights of malicious actors and illustrate the risks to the Central Government.

2022

March

- Railway delays due to a bug in Alstom software
- Personal data belonging to customers of housing cooperatives leaked following a ransomware attack against ICT supplier
- Thousands of files encrypted and leaked following a ransomware attack against an energy company
- Dutch windmills could not conduct test runs due to a ransomware attack
- Espionage at a Dutch defence company by Lazarus APT

April

- Personal data leaked following a ransomware attack against an airport security company
- Files of the Gelderland municipalities of Buren and Neder-Betuwe published on the dark web following a ransomware attack

- Physical sabotage of French fibre-optic cables resulted in regional internet failure
- Pegasus spyware used against Catalan politicians and activists

September

- Care at Maastricht UMC+ virtually stopped due to an ICT failure
- Limited accessibility of DigiD for hours due to DDoS attacks
- Data of employees of the Senate and the House of Representatives leaked following ransomware attack against supplier of access passes
- Production facilities of a Dutch vaccine company partially disrupted due to a ransomware attack, stolen data leaked on the dark web

- Operation of the Bosnia-Herzegovina parliament disrupted following cyberattack

October

- Telephone number of National police and tip lines difficult to reach due to outage
- Tens of thousands of medical files and personal data stolen from digital healthcare platform

- IT systems German energy supplier disrupted by cyberattack

November

- Website European Parliament offline following a DDoS-attack by pro-Russian hacker group Killnet

December

- Data stolen and limited accessibility of office systems following hack of work placement company
- Data of tens of thousands of customers of mobile providers leaked
- Operational problems at wholesalers Makro and parent company following a ransomware attack

- City services and civil affairs municipality of Antwerp offline following a ransomware attack at ICT partner of the municipality

- *Incidents in the Netherlands*
- *Incidents abroad*

May

- Dataset leaked by pro-Russian hacktivist group XakNet Team contains data of government employees
- Spanish Prime Minister target of Pegasus spyware
- National emergency in Costa Rica due to failure of several government systems following a ransomware attack

June

- Confidential documents and personal data of the municipality of Veenendaal leaked due to human error at software supplier
- ICT systems ARTIS encrypted by ransomware

July

- Interruption of activities in the social domain of the municipality of Noordenveld due to a ransomware attack
- Railway traffic disrupted by inoperative ProRail back-up system
- Polish officials attacked with Pegasus spyware
- Albania closed government websites and services due to a cyberattack
- Greek opposition leader and Member of the European Parliament target of Predator spyware.
- Data stolen and systems rendered inaccessible during a ransomware attack against Luxembourg energy companies

Augustus

- 120 Dutch dental practices inoperative for several days due to a ransomware attack
- Confidential data of five Limburg municipalities inaccessible due to hack at software supplier
- Personal data leaked following cyberattack against energy service provider
- Montenegro government services disrupted by ransomware attack

2023

January

- Websites of various Dutch hospitals temporarily inaccessible due to DDoS attacks

February

- Various websites of Dutch organisations target of hacktivist DDoS attack after Quran was torn up

2022

March 2022

Railway delays due to a bug in the Alstom software: A bug in the software of the railway signalling system of French supplier Alstom caused problems to the railway system. The bug resulted in delays and cancellation of trains in the Netherlands, Poland, Sweden, Italy, India, Thailand and Peru, among other places. The impact in the Netherlands was minimal.[10]

Personal data belonging to customers of housing cooperatives leaked following ransomware attack against ICT supplier Multiple housing cooperatives fell victim to a data breach after their ICT supplier The Sourcing Company (TSC) became the target of an attack with Conti ransomware. The attackers encrypted the TSC servers, stole data and published it online. Among other things, the personal data of part of the tenants were disclosed as a result.[11]

Thousands of files encrypted and leaked following a ransomware attack against an energy company: Energy company NV GEBE Sint-Maarten fell victim to BlackByte ransomware. During that attack, thousands of files were encrypted, stolen and published by the attackers on their leak site. The attack had an impact on the GEBE computer systems, but did not affect the supply of power, water or other vital processes.[12]

Dutch windmills could not conduct test runs due to a ransomware attack: Several windmills at the Oude Maas wind park could not conduct test runs as a result of a ransomware attack against German windmill manufacturer Nordex. Following the attack, the manufacturer took down its ICT systems at multiple locations as a precautionary measure. The attack did not have an impact on the hardware that has access to the operation of the windmills. The attack was claimed by criminals who were behind the Conti ransomware.[13]

Espionage of a Dutch defence company by Lazarus APT: Investigators of the ESET security company claim that Lazarus APT[I] carried out an espionage attack against a Dutch defence company. Employees of the company opened malware from an actor pretending to be an Amazon recruiter via LinkedIn. The attack was allegedly part of a campaign whereby Lazarus also attacked aviation, space and defence companies in other countries.[14]

[I] Lazarus APT is a digital actor involved in digital espionage, cybercrime and sabotage. APT stands for Advanced Persistent Threat. It often means that the group is able to deploy advanced tools to be able to operate without being noticed for a prolonged period of time. APT is therefore often linked to (foreign) governments.

April 2022

Personal data leaked following a ransomware attack against an airport security company: The I-SEC airport security company, which provides services at Schiphol among other places, fell victim to Conti ransomware. The data that were stolen were published on the Conti leak site. The dataset included the personal data of current and former I-SEC employees among other things.[15]

Files of the Gelderland municipalities of Buren and Neder-Betuwe published on the dark web following ransomware attack: Two Gelderland municipalities fell victim to a data breach after attackers were able to steal files using SunCrypt ransomware. The attackers stole 130GB of data and published it on the SunCrypt leak site. The leaked data included identity documents among other things. According to forensic investigation, the attackers broke in by abusing the stolen login details of a supplier.[16]

May 2022

Dataset leaked by Russian hacktivist group XakNet Team contains data of government employees: The Russian hacktivist group XakNet Team leaked a dataset consisting of thousands of files via the Telegram channel that is accessible to the public. According to the MIVD, this dataset contained communication and personal data from a large number of persons, including several Dutch government officials.

June 2022

Confidential documents and personal data of the municipality of Veenendaal leaked due to human error at software supplier: A technical act of a software supplier of the municipality of Veenendaal meant that confidential documents and documents containing personal data were accidentally placed online for a short period of time. Documents from 2016 were inspected from eight IP addresses. The supplier repaired the breach quickly following a report by an observant citizen.[17]

ARTIS ICT systems encrypted by ransomware: Cybercriminals penetrated the ARTIS zoo network, which meant that ICT systems went offline and visitors were unable to purchase online tickets. The zoo did not comply with the hackers' demand to pay a million euros in crypto currency. Instead, the zoo was able to restore the systems using back-ups. No personal or other data were stolen or accessed according to the ARTIS ICT partners.[18]

July 2022

Interruption of activities in the social domain of the municipality of Noordenveld due to ransomware attack: The municipality of Noordenveld was the subject of a ransomware attack. Several servers and administrative systems were encrypted during the attack. The system's ICT supplier was able to restore data on the basis of a back-up resulting in merely a few days' loss of data production. The ransomware attack did not result in the loss of personal data or an interruption of benefit payments.[19]

Railway traffic disrupted by inoperative ProRail back-up system: An ICT failure at the ProRail traffic control post meant that railway traffic around Rotterdam had to be stopped for several hours on 31 July 2022. The failure meant that traffic control could not see where trains were located. ProRail should fall back to a back-up system in such cases, but this was impossible due to a software error.[20]

August 2022

Dental care 120 Dutch dental practices inoperative for several days due to ransomware attack: Dutch Colosseum Dental dental practices were closed for several days after the company fell victim to a ransomware attack. Patients could not be treated because their files were unavailable due to the attack. The company made arrangements with the attackers regarding restoration and non-publication of data.[21]

Confidential data of five Limburg municipalities inaccessible due to hack at software supplier: The software supplier of the municipalities of Eijsden-Margraten, Gulpen-Wittem, Kerkrade, Meerssen and Vaals was affected by a hack, which resulted in data of the municipalities becoming inaccessible. The hackers attacked an administrative system as a result of which municipal officers were unable to open data concerning social assistance benefits, youth care, the Social Support Act and energy allowances.[22]

Personal data leaked following cyberattack against energy service provider: Energy service provider Ista fell victim to a cyberattack. The company took all ICT systems that may have been affected offline in order to prevent damage to the ICT infrastructure. The attackers published the stolen data of 146,000 persons online. The published data included address details of customers, names and information about energy and water consumption. This does not include the personal data of Dutch citizens according to the company. Various housing cooperatives nevertheless reported potential data breaches.[23]

September 2022

Zorg Maastricht UMC+ virtually stopped due to an ICT failure: An ICT failure at the Maastricht UMC+ hospital meant that virtually all care at the hospital stopped. The hospital could not be reached and access to the electronic patient record system was not possible due to a technical failure. Some patients who came to the hospital at the time of the failure were sent home again. Urgent treatments did go ahead.[24]

Limited accessibility of DigiD due to DDoS attacks: DigiD fell victim to a DDoS attack on 12 September 2022. This meant that the service had limited accessibility for hours and citizens were sometimes unable to log in. It is not clear who is responsible for the attack.[25]

Data of employees of the Senate and the House of Representatives leaked following ransomware attack against the supplier of access passes: ID-ware, which is a large supplier of applications relating to authentication and access passes, became the victim of ALPHV/BlackCat ransomware. The attackers stole data from customers of ID-ware and published them on a leak site. The dataset included among other things access passes of members and employees of the Senate and the House of Representatives. The personal data and access passes of various Dutch educational institutions, government organisations and companies were leaked as well.[26]

Production facilities of a Dutch vaccine company partially disrupted due to ransomware attack, stolen data leaked on the dark web: The Dutch vaccine company Bilthoven Biologicals was attacked with ALPHV/BlackCat ransomware. The attackers were able to affect production facilities, such as machines for the production of vaccines. The machines were largely able to continue production during the attack. In addition, the attackers allegedly stole e-mails and documents containing scientific data, such as information about vaccines. The stolen data was published (in part) on the dark web.[27]

October 2022

National police telephone number and tip-off lines difficult to reach due to failure: A technical failure meant that the 0900-8844 police telephone number, the investigation tip-off line and Meldpunt 144 were difficult to reach for several hours on 18 October 2022. The problem occurred throughout the country. The 112 emergency number did work properly at the time of the failure.[28]

Tens of thousands of medical files and personal data stolen from digital healthcare platform: An attacker broke in and stole privacy-sensitive data via a vulnerability in the Carentzorg digital healthcare platform. Various Dutch healthcare institutions therefore reported a data breach to the Dutch Data Protection Authority. Approximately nine thousand healthcare providers and almost two million people use the Carentzorg digital healthcare environment.[29]

December 2022

Data stolen and limited accessibility of office systems following hack of work placement company: Office systems were rendered inaccessible or could be accessed only to a limited extent as a result of a hack of the Pantar work placement company, which is the largest social development company in the Amsterdam-Diemen region. The company also switched off a large number of systems as a precaution. The attackers stole data but no customer data was stolen according to the company.[30]

Data of tens of thousands of customers of mobile providers leaked: Several tens of thousands of customers of Caiway Mobiel and Delta Mobiel fell victim to a data breach. An attacker was able to gain access to the ordering environment for mobile subscriptions and was therefore able to download customers' names, addresses, e-mail addresses, dates of birth, telephone and bank account numbers. Login details such as passwords and credit card details were not stolen according to the providers.[31]

Operational problems at wholesalers Makro and parent company following ransomware attack: Metro, which is the parent company of Makro wholesalers, encountered problems during recovery activities following a ransomware infection. Metro found new malicious files during the recovery work whereafter the company switched off its ICT systems. This meant that several operations of subsidiary Makro also stopped. The attack resulted inter alia in problems relating to the distribution of advertising leaflets from seventeen branches in the Netherlands. The criminals also stole personal data of Metro employees during the attack.[32]

2023

January 2023

Websites of various Dutch hospitals temporarily inaccessible due to DDoS attacks: During the last weekend of January, several hospitals, including the UMCG, LUMC and MUMC+, were confronted with DDoS attacks which meant that websites were temporarily inaccessible.[33] [34] The attack against the UMCG stood out most because some of the hospital's websites were offline for several days. The hospital's business operations were not affected and the patient portal remained available. [35] The attacks were claimed by pro-Russian Killnet hacktivists, after they had placed Dutch hospitals (among others) on a list calling on other parties to attack them in connection with Dutch support for Ukraine.[36]

February 2023

Various websites of Dutch organisations targeted by hacktivist DDoS attack after Quran was torn up: Several Dutch government organisations and companies became the target of hacktivist DDoS attacks against their websites. Groups which claimed to have been involved in the attacks included 'Mysterious Team Bangladesh' and 'Turk Hack Team'. The attacks were allegedly a response to a Quran being torn up in The Hague at the end of January. The attacks were allegedly part of the #OpHolland and #OpSweden campaigns.[37]

Remarkable incidents abroad

April 2022

Physical sabotage of French fibre-optic cables resulted in regional internet failure[38]

Pegasus spyware used against Catalan politicians and activists[39]

May 2022

Spanish Prime Minister target of Pegasus spyware[40]

National emergency situation in Costa Rica due to the failure of several government systems following ransomware attack[41]

July 2022

Polish officials attacked with Pegasus spyware[42]

Albania closed government websites and services due to cyberattack[43]

Greek opposition leader and Member of the European Parliament target of Predator spyware[44]

Data stolen and systems rendered inaccessible during ransomware attack against Luxembourg energy companies[45]

August 2022

Montenegro government services disrupted by ransomware attack[46]

September 2022

The operation of the Bosnia-Herzegovina parliament disrupted following cyberattack[47]

October 2022

ICT systems German energy supplier disrupted by cyberattack[48]

November 2022

Website European Parliament offline following DDoS-attack by pro-Russian hacker group Killnet[49]

December 2022

City services and civil affairs municipality of Antwerp offline following ransomware attack at ICT partner of the municipality[50]

Over a year after the start of the war against Ukraine, the impact of cyberattacks has turned out to be smaller than expected. However, that does not mean that cyberattacks do not play a major role.

3 Russian war against Ukraine : extensive cyber campaign, less impact than expected

Well over a year after the start of Russia's war against Ukraine, Russian cyberattacks focused predominantly on Ukraine and the nearby region. It concerned espionage and (acts in preparation of) sabotage. Russia also spreads disinformation. Disruptive cyberattacks that harm Dutch national security have not (yet) occurred. The digital threat may change abruptly if the war escalates further. Cyberattacks could start affecting national security if this is the case. The Netherlands may also be affected by chain effects that have an impact on vital processes and may (continue to) be confronted with attacks by pro-Russian criminals and hacktivists.

Not the expected cyber war, but cyberattacks did occur

Cyberattacks have not (yet) had the disruptive and decisive impact that was expected, but they did play a supporting role for example in disrupting Ukrainian communication or the (attempted) theft of information concerning (international) decision-making. It was assumed at the start of the war against Ukraine that it would be the first war with a decisive role for cyberattacks. One important reason was that a country with advanced cyber capabilities started a war against a highly digitised country.[51] It also became clear in the past that Russia has both the capabilities and intention to carry out disruptive attacks against Ukraine.[52] It was also feared that attacks against Ukraine could spread to other countries or that countries that would support Ukraine would become the victim of retaliation by Russian cyberattacks.

Extensive offensive campaign, but limited impact partially due to assistance provided to and high resilience on the part of Ukraine

One year after the start of the war, it appears that the impact of cyberattacks is smaller than expected. This does not mean that cyberattacks do not play an important role.

The many hundreds of attacks on both sides show that there is a very impressive and persistent campaign.[53] However, there is no complete picture of the scope and impact of the attacks. This is caused for example by the violence of war in that location, which complicates estimation. In addition, victims may intentionally not disclose issues. Within the context of the war, the attacks are less than expected, but outside of that context there is an extensive, offensive campaign of cyberattacks. The Russian cyber sabotage campaign against Ukraine is even the most large-scale and intensive one in history.[54]

Open sources identify various examples of Russian cyber sabotage attempts against vital Ukrainian infrastructure, including the power supply. The MIVD holds information about many more such attack attempts against vital infrastructure that has not (yet) been made public. Russian state actors have strong intentions and develop a high level of activities in the area of cyber sabotage.

Large-scale and long-term disruption as a result of cyberattacks has however not yet materialised, and the consequences of cyber sabotage are insignificant when compared to the impact of physical military operations.[55] The relatively limited impact of Russian cyberattacks in general is attributable inter alia to Ukraine's high level of resilience.[56] Private companies played a large role in increasing that resilience, for example by offering services to and sharing threat information with Ukraine. Ukraine also receives significant help from western intelligence services.[57] It also became clear during the war that Russia has difficulty synchronising cyber operations with other military operations, such as airstrikes.[58] The success of Ukraine's digital defence is not guaranteed, however. It is likely that this success can only continue for as long as western support remains as intensive and adaptive as the cyber operations of the Russian intelligence services.[59]

Many wiperware attacks against Ukraine, also against vital infrastructure

Ukraine and the nearby region undeniably have Russia's attention. The Ukrainian digital infrastructure is under almost constant attack.[60] Russian hackers have used many different types of wiperware against Ukrainian targets, also within vital sectors (see chapter 2).[61] A known example is the attack against the American satellite company Viasat. This attack occurred several hours before the invasion and temporarily disrupted Ukrainian communication as a result of large quantities of data being wiped.[62] One of the largest internet providers in Ukraine was hacked in March 2022 as well. This resulted in failure of the internet in large parts of the country for about one day.[63]

Other actors hitch along on the theme of war

In addition to Russia, several other state actors have also carried out cyberattacks in connection with the war. For example, it appears that state actors, which are (or were) not directly involved in the war, acted opportunistically and hitched along on the theme of the war. Such as by using phishing when disseminating malware. Formulations in titles or descriptions related to the war were often used in this connection. This makes it easier to seduce victims to click on something or to open files.[64] State actors other than Russia mainly attempted to gain access to certain systems. It is likely that this was intended for (economic) espionage.[65] In addition, espionage by at least one other country was identified in respect of (pro) Ukrainian targets, in order to obtain information about the war.[66]

In general terms, cyberspace is used by state actors to obtain geopolitical gains. Broader geopolitical developments are used increasingly often to seduce victims to open malicious links or files. Taking advantage of geopolitical developments such as the war is therefore not unexpected.

Cybercriminals pick a side

Shortly after the invasion of Ukraine began, groups of cybercriminals posted messages in which they expressed support for Russia or Ukraine. The criminal Conti group expressed its support for Russia and indicated that cyberattacks against Russian targets would be answered with attacks against critical infrastructure.[67][68] This supports the notion that criminals deliberately select certain targets because they are in line with the geopolitical interests of certain states, or even that there are ties between governments and cybercriminals.[69] State actors may hire, tolerate or pressure cybercriminals to carry out cyberattacks against desired targets.[70] In addition, other parties such as state actors may represent themselves as criminal organisations.[71] This means that the dividing line between financially-motivated cybercriminals and state actors becomes vaguer and more difficult to distinguish. Cybercriminal groups from Russia in particular operate in a freer playing field. The many sanctions mean that it is likely that the Russian authorities will be less inclined to hinder cybercriminals that attack western interests.

Hacktivism made a comeback

Hacktivists also sprang into action during the war, while they carried out relatively few cyberattacks during the past years.[72] For example, Anonymous announced its opposition against Russia. After that, several cyberattacks were claimed by the collective, such as DDoS attacks against Russian government websites, the hacking of a Belarusian arms supplier, and the defacement of Russian television channels. Another well-known example of hacktivist efforts is the pro-Ukrainian IT Army. The Ukrainian Minister for Digital Transformation appealed to hackers worldwide to help the IT Army to carry out DDoS attacks against Russian targets for example. [73][74] And pro-Ukrainian hacktivists already claimed during the troop build-up in Belarus preceding the invasion that they had compromised the system of the Belarusian railway network. They threatened to disrupt the trains that were carrying Russian troops and equipment.[75] Pro-Russian hacktivists also made themselves heard. For example, the hacktivist group Killnet called for attacks against European hospitals with DDoS attacks, including several hospitals in the Netherlands (see Annual review).

Some comments should be made with respect to hacktivism. The measurable impact of hacktivist activities is often short and relatively limited. However, the consequences may include psychological impact on the population and the authorities. It should also be noted that hacktivist groups are generally loosely organised and that there is often no clear leadership. Participation generally takes place on a voluntary basis and participants do not follow a structured plan, communication often takes place via channels such as Telegram, and the cyber instruments used are relatively simple and low-threshold.[76] There are nevertheless also indications that state actors mix with hacktivists or operate under the flag of hacktivism.[77] [78]This makes it difficult to attribute hacktivist attacks. The danger is that the activities of hacktivists are interpreted incorrectly by countries that fall victim to their attacks, which could result in counter-reactions.[79]

Private companies support Ukraine with respect to digital resilience

One characteristic element of the development of the war is that private companies provide support to Ukraine often in cooperation with states that provide support to of Ukraine. This is often done by increasing the resilience of (Ukrainian) organisations and by keeping vital services accessible.[80] It became clear that Microsoft had been actively creating patches for malware aimed at Ukraine months before the invasion and that it was sharing threat information with the Ukrainian authorities. In addition, Amazon and Microsoft offered the Ukrainian government the possibility of transferring government data to the cloud and guaranteeing its security.[81] Furthermore, the SpaceX Starlink satellite network was activated above Ukraine.[82] This means that access to the internet was restored in areas where the internet infrastructure had been damaged by Russian physical and digital attacks.[83] [84] In addition to private companies, western intelligence services also provide significant assistance in increasing resilience, such as by assisting in monitoring, detection and response measures.[85]

Russia attempts to influence public opinion with disinformation

Information confrontation, including influencing by deception, disinformation and cyber operations, plays a central role in the Russian modus operandi. This is carried out to a large extent using digital tools in order to cause psychological damage among other things.[86] It is attempted in this connection to undermine Ukrainian efforts, to increase support for the war within Russia, and to shape international public opinion.[87] For example, Russian intelligence services were able on several occasions to temporarily take over control of the broadcasts of Ukrainian media and to broadcast Russian messages. The systems of these media were then sabotaged digitally.[88] Russian state media have also consistently published disinformation.[89] [90] Russia has deployed disinformation for a long time, also before the war. Although Moscow does not focus its efforts specifically on the Netherlands, Moscow has made far-reaching efforts since the start of the invasion to secretly influence the western public debate about the war and the political-administrative system.[91]

Russia also focuses on the Netherlands, but so far no disruptive impact

Russian espionage attempts identified in the Netherlands and vital infrastructure is secretly identified

For the time being, attacks related to the war have not resulted in major disruptions or impact on national security in the Netherlands. However, cyberattacks were carried out within the context of the war in which the Netherlands, NATO Member States, and/or ‘the west’ in general were a target of Russia.

The overwhelming majority of Russian cyber operations focus on espionage in order to obtain military, diplomatic and economic information from both Ukraine and NATO Member States.[92] It is likely that Russia’s need for intelligence increased during and as a result of the war against Ukraine. On the one hand because it could be very valuable to obtain information concerning possible decision-making, military support or the presence and/or support of weapons for example. And on the other hand, because ‘regular’ channels largely disappeared during the war as a result of sanctions and the expulsion of diplomats for example.[93] [94] These (attempts at) espionage take different shapes. Russia attempts to find out, inter alia by means of espionage, how NATO and the EU make decisions, and subsequently how it can undermine that decision-making.[95] Furthermore, the Russian need for intelligence focuses inter alia on military support being provided to Ukraine via the NATO Member States. The Dutch armed forces, Ministries and embassies were also the target of (unsuccessful) cyber espionage attempts over the past year. In addition, Russian cyber spies hacked routers of Dutch private citizens and small and medium-sized enterprises. This operation is cause for concerns because Russia can exploit these hacked routers to carry out secret cyber operations against Dutch interests or those of allies. [96] There may also be economic espionage, such as for the purpose of reducing the negative effects of sanctions and/or to obtain required knowledge.

The AIVD and MIVD furthermore see that Russia is secretly identifying parts of Dutch vital infrastructure. This means that Dutch internet cables among other things could be the target of sabotage.[97] Although it concerns physical components such as cables, sabotaging these could have an impact on the digital domain. This could result in breakdown or even disruption in the Netherlands. It cannot be excluded either that the physical acts are or become part of a digital sabotage campaign.

Russia’s focus probably on Ukraine and the region

It is likely that advanced Russian cyberattacks will mainly continue to focus on Ukraine and the nearby region. Cyberattacks that disrupt society usually cost a great deal of capacity; creating malware, surveying systems, embedding, and subsequently rolling out malware can take many months. In addition, an actor such as Russia cannot deploy such capacity everywhere at the same time, and has to make choices in terms of target selection. Dutch organisations can however be affected by chain dependencies as a result of attacks related to the war against Ukraine. Previous attacks by Russian actors have resulted in collateral damage.

So far, Dutch national security has not been impacted by cyberattacks, but it cannot be excluded

The probability of targeted attacks against Dutch interests is estimated as possible by the NCSC.[98] Although not affected thus far, it cannot be excluded that cyberattacks as a consequence of the war against Ukraine will start affecting national security. As set out in previous CSAN's and the previous paragraph, Russian actors carried out espionage activities and parts of the Dutch vital infrastructure are being secretly analysed. Russia has had an offensive cyber programme against the Netherlands, among other countries, for years. The ever-worsening relationship with Russia and the geopolitical isolation of the country may contribute further to an increase in cyberattacks against the Netherlands or to more advanced attacks taking place.

It should be taken into account that a cyberattack in the Ukraine or the region could have consequences for the Netherlands or other western countries, which for example could result from chain effects within digital ecosystems (see chapter 5 for a further explanation of chain effects and digital ecosystems). Also, a cyberattack not carried out with the underlying motive of disruption can actually lead to this. In this way a cyberattack can nevertheless have a significant impact or even impair national security.

In the event hackers carry out cyberattacks from or via the Netherlands against foreign targets, the Netherlands could also be affected by a counter-reaction. In addition, Dutch citizens may participate in actions by hacktivists and thus become involved in the war or other conflicts. That involvement can have unforeseen circumstances and, moreover, is punishable by law.[99]

All things considered, it can be argued that the unexpected should be expected as regards cyberattacks within the context of the war against Ukraine. Russian cyberattacks with a disruptive impact may not have happened as yet, but that is no guarantee for the future. The threat could change abruptly as a consequence of further escalation of the war.

In our daily lives, we mainly pay by card. We rarely carry cash in our wallets. That is why a nationwide failure of payment terminals would inconvenience people and lead to unrest.

VANWEGE EEN LANDELIJKE PINSTORING KUNT U OP DIT MOMENT NIET PINNEN
ONZE EXCUSES VOOR HET ONGEMAK
BUITEN BIJ DE ING AUTOMAAT KUNT U WEL GELD PINNEN
Deze kassa is gesloten

4 Operational technology: a vulnerable building block for vital processes

Operational technology (OT), within industrial networks also referred to as 'Industrial Automation and Control Systems' (IACS), plays a central role within the control, monitoring and management of physical processes within (vital) organisations. Large-scale failure and problems relating to the availability of these systems can have major social consequences. It has become clear that cyber actors are interested in compromising OT. Controlling the related risks requires specific knowledge, competencies and cooperation. There is room for improvement despite the growing attention for the resilience of OT systems. It is important to focus further on this in order to guarantee the resilience of vital processes.

Key concepts

Operational technology (OT): the collective noun for digital systems (hardware and software) that initiate, monitor and control a physical process. Examples include IACS, access systems or building automation systems. Whereas the priority of IT is data confidentiality and integrity and to a lesser degree availability, this is the opposite for OT due to the possible physical consequences of disruption or failure.

Industrial Automation and Control Systems (IACS): form part of OT and are used to control, automate and monitor physical processes in the industrial sector, including in many vital sectors. IACS includes various forms of monitoring and control systems, such as Supervisory Control and Data Acquisition systems (SCADA) and Programmable Logic Controllers (PLC). In addition, various industrial communication protocols are used within IACS.

Industrial Internet of Things (IIoT): the application of the Internet of Things (IoT) in industrial environments for (among other things) process optimisation and diagnostics, which makes it possible to integrate systems and connect them directly or indirectly to the internet.

OT security is of vital importance, but faces important challenges

When compared to regular information technology (IT), relatively little attention is devoted within the public debate to the security of OT and the related challenges. This is caused on the one hand by the fact that the news focuses predominantly on the prominent digital breach of regular IT systems such as websites, servers and workplaces. On the other hand, there have been relatively few disruptive breaches of OT as far as is known. However, OT systems form the basis for important physical processes, such as the production and processing of raw materials, the purification of drinking water, operation of locks and the distribution of electricity. This means that the security of these systems is of vital importance to Dutch society and its economy.

Impact of cyber incidents is potentially large

Due to the important role of OT, large-scale failure and problems relating to the availability of OT systems could have major social consequences.[100] Incidents can result in social unrest, economic damage, and loss of confidence in digitisation.[101] Whereas incidents in an IT environment often result in reputational or financial damage, incidents in OT environments can also cause damage to industrial equipment and the nearby surroundings. And in extreme cases casualties are also possible.[102]

The probability of an incident occurring and the impact thereof depend highly on the type of comprise, the degree of resilience of the organisation affected and the sector in which the incident occurs. Chain effects may occur as well. The fact that OT systems are also vulnerable to digital attacks became clear several times over the past years, resulting in some cases in a large impact on the organisations affected and their environment.[II]

Resilience OT systems is a complex issue

Digital OT security is facing several important challenges.[103] OT systems have a longer service life and the costs of replacing them are often high. Information regarding vulnerabilities is often diffuse. A specific perspective for action on the part of suppliers to resolve vulnerabilities or prevent their exploitation is often lacking[104][105] And in practice it is also difficult to update OT systems to new software versions, because this can disrupt the availability and interoperability of OT systems. What is more, the development of representative testing environments for the purpose of testing patches before they are rolled out, is often expensive and complex. All of the above means that many processes depend on outdated and vulnerable software. In addition, many systems in OT networks are traditionally insecure-by-design.[III] In this connection, the importance of operational efficiency and being able to respond quickly to insecure situations outweigh the authentication of the user for example.[106][107] However, experience shows that there is a greater chance of incidents in networks without adequate internal controls. Moreover, the damage is often larger and more difficult to repair. This also applies to OT networks being used by attackers with the right knowledge to carry out an attack using standard functionalities, possibly without this involving a vulnerability.[108]

Threat increased due to large attack surface and interest of cyber actors

The fact that OT networks are traditionally insecure-by-design is becoming increasingly problematic because OT has become more intertwined with IT over the past years. Increased integration, also referred to as IT/OT convergence, is intended to improve the visibility, efficiency and speed of operational processes.[109] However, this also offers attackers more possibilities to gain access to an OT network via compromised IT systems.[110] This is reinforced by the emergence of the Industrial Internet of Things (IIoT).[111] This also increases the attack surface and offers attackers more opportunities to comprise operational systems.[112]

New malware also relevant for the Netherlands

The currency of the possibility for comprising operational systems is evident inter alia from the discovery of two new types of malware last year. It became clear that these types of malware can be used to sabotage OT systems.[IV] The first, Industroyer2, was deployed against a Ukrainian energy supplier, but could be neutralised in time. ESET and the Ukrainian CERT attribute Industroyer2 to Russian state actor Sandworm.[113][114] Industroyer2 is the first OT malware that builds on a previous variant.[115] The second type of malware, known as PIPEDREAM/INCONTROLLER, gives an attacker multiple options in case of a digital attack and creates, among other things, a bridge between IT and OT environments.[116] According to Mandiant, PIPEDREAM/INCONTROLLER was presumably developed by a state actor, but was discovered by investigators before it could be deployed.[117] It is remarkable that

[II] A well-known example includes the digital sabotage of operational systems of Ukrainian electricity plants in 2015 and 2016 using BlackEnergy en Industroyer-malware, as well as a digital attack against a petrochemical plant in Saudi-Arabia in 2017, during which a malware known as Triton/TRISIS was used, which specifically targets security systems. Furthermore, at the start of 2021, an attacker managed to gain access to the operational systems of a water board in Oldsmar (USA) which controls the addition of chemicals to the drinking water.

[III] Contrary to IT networks, OT networks make less use of authentication and authorization methods to control access to systems. The assumption is that there is no harm in this because OT environments are traditionally separated from other (IT) networks and in principle, legitimate network traffic can be assumed.

[IV] These two are on top of five already well-known OT-specific malware types: Stuxnet, HAVEX, BlackEnergy2, Industroyer/Crashoverride and Triton/TRISIS.

both malware variants can be deployed more broadly and can also be deployed beyond the initial target.

Such developments are also relevant to the Netherlands. It is a known fact that state actors focus inter alia on preparatory acts for sabotage against vital and other crucial infrastructure.[118] In addition to sabotage, gaining insight into industrial processes as a result of espionage can also be an important motive on the part of state actors.[V] An exploratory act can already result in disruption of industrial environments and is very undesirable for this reason alone.

Increased interest in OT systems on the part of ransomware actors not excluded

Ransomware actors also form a risk to the continuity of operational systems and physical processes. For example, a new ransomware variant named Luna was discovered in July 2022.[119] This variant includes a list of OT processes that if they are present are terminated before encryption takes place. Such a list is also referred to as a kill list. The use of a kill list was identified earlier in ransomware variants such as EKANS, MegaCortex and LockerGoga.[120] Kill lists are not by definition the result of a targeted attempt to disrupt OT networks. They often consist of broad and incoherent lists of programmes to be terminated within both IT and OT environments that are presumably drawn up randomly.[121] Another ransomware variant that used such a list, known as Clop, was reported in the news in August 2022 in connection with an attack against British company South Staffs Water. The attackers claimed that they had access to the drinking water company's OT systems.[122] The organisation itself indicated that the attack only involved the IT environment and that the drinking water supply was never in any danger.[123]

It is expected that ransomware actors will continue to develop new tactics in order to pressure their victims even more. Industrial environments are also increasingly often identified as revenue models for cyber actors.[124] Although attacks that are not directly aimed at OT can result in operational problems, a further and possibly more targeted disruption of OT systems cannot be excluded in this context.[VI] This is facilitated by the increasing intertwining of OT and IT.

Hacktivism mainly opportunistic and symbolic in nature

Hacktivists appear to be taking an increasing interest in compromising OT, because it can be used as a coercive measure to realise ideological objectives. This is evident from an increasing number of alleged attacks that are claimed by hacktivist groups.[125] The motives cited by hacktivists vary in nature. Reference is made among other things to the war against Ukraine, but also to other social issues and geopolitical developments worldwide.[126] However, such attacks are generally opportunistic in nature and aimed at systems of which the attackers themselves often have no specific knowledge. For example, hacktivists use exploit modules that are available to the public ('tools') and directed against OT systems connected to the internet.[127]

Its impact appears to be very limited for the time being and the outcome of attacks seems uncertain. It is often difficult to verify claims which mainly serve a symbolic purpose. Moreover, compromising a single OT system is insufficient to realise a targeted outcome. Because if attackers wish to realise a targeted effect, they have to know exactly how they can manipulate an entire network containing various systems.[128] Being able to carry out attacks that have prolonged physical consequences requires time, knowledge and capacity. It is therefore not likely that they can be carried out by a less-advanced actor.[VII] It should be noted in this connection that the capacity of hacktivists also depends on the degree of connection to state actors. Collaboration is possible or hacktivists can be used as cover to complicate the attribution of digital attacks.[129] The degree of connection is not always clear.

Room for improvement despite the growing attention for resilience

Challenges related to the resilience of OT systems

As set out above, most OT systems were designed during a time that no account was taken of (digital) exploitation. For a long time, the resilience against digital threats was not a priority because of the limited connection between OT and IT systems, but attention for this problem has been increasing over the past years. However, limited measures are being implemented in respect of OT networks out of concern for the unforeseeable (serious) consequences for the

[V] For example, on 24 March 2022 the American Department of Justice published two indictments against four Russian government officials who are being held responsible for multiple digital attacks directed against OT systems, including for the purpose of collecting intelligence from hundreds of companies within the energy sector in more than 135 countries. These attacks could possibly be related to preparatory acts for sabotage purposes.

[VI] Known examples of attacks against IT systems with large operational consequences are the NotPetya and WannaCry attacks (2017) during which wiperware was able to spread unchecked, as well as the ransomware attack against Colonial Pipeline, which is one of the largest oil pipelines in the US (2021). Various digital attacks against (oil) storage/transhipment locations in Germany, Belgium and the Netherlands occurred at the start of 2022. Although the attackers in this case were after the IT systems of the affected parties, the attack resulted as yet in the temporary disturbance of processing and distribution processes.

[VII] Organisations must therefore also take account of threats posed by insider threats, including employees and contracting parties. For example, in July 2022 the Spanish police announced the arrest of two former employees who used their knowledge between March and June 2021 to carry out digital attacks against sensors that are used to measure radioactive radiation.

correct functioning of (vital) operational processes. In practice this results in the absence of basic measures that are customary in an IT environment, such as authentication, authorisation and encryption. In addition, OT systems are not scanned or hardly ever scanned for vulnerabilities and as indicated above, vulnerable systems are not always patched (if a patch is available at all) in order to guarantee the correct operation of these systems. Furthermore, the detection and repression of digital attacks within an OT environment are not set up adequately at many organisations.[130] Organisations are therefore unable to detect (and respond in time to) an attack in time when an attacker gains access to the OT network.[131]

The limited set of measures within an OT network does not mean that OT environments are not resilient. For example, a lot of measures are being implemented to guarantee the security of the process in case of a (digital) emergency.[132] In addition, digital resilience is characterised by the measures intended to prevent attackers from gaining access to the OT network.[133]

Within IT and OT different starting principles, standards and priorities in the area of safety (damage to persons and/or the environment) and security (availability, integrity and confidentiality) are applied. Moreover, OT systems generally last many years longer than IT systems. These differences must be taken into account in the design of the interface between IT and OT environments (and the measures realised as a result). This does not always take place sufficiently, partly because traditionally the teams involved in IT and OT operate independently of each other.[134]

Growing attention for standards and public-private partnerships

Several organisations indicate with respect to legislation and regulations that they have difficulty interpreting the obligation to report incidents within the OT environment.[135] There are also organisations that experience (too) little control by the government, for example because mandatory cybersecurity audits are lacking in certain sectors.[136]

There is increased attention on the part of the government for helping organisations with the security of their OT environments. Priorities for the future have since been set by means of the Dutch Cybersecurity Strategy.[137] In addition, efforts were made during the past year to offer shared security standards. One example is the Basic Cybersecurity Measures for Industrial Automation & Control Systems (BIACS), which in turn is derived from the Objects Cybersecurity Implementing Directive 3.0 (CSIR), in which both the Government Information Security Baseline (BIO) and the IEC 62443 system of standards are processed.[138] [139] In addition, several starting points and tools are being developed in order to help organisations along with the security of their OT environments, such as the ‘Process Automation Security Check’.[140] The Cyber Resilience Act (CRA), which is the European Commission’s proposal for security requirements relating to digital products, several additional requirements are imposed for the suppliers of systems that are frequently used in OT environments, such as SCADA systems and PLCs.[141]

Private and public organisations are increasingly able to work together in this connection. Multiple partnerships have been initiated to provide insight into threats and risks and to jointly develop best practices.

Expertise and focus necessary for OT cybersecurity

And finally, resilience of OT environments is linked to the employees who realise this resilience. OT environments are different from IT environments and require different knowledge and competencies in the area of cybersecurity. There is often still insufficient attention within organisations for the usefulness and need for OT cybersecurity. For example, OT cybersecurity teams often have to work with limited means.[142] In addition, it is not easy to transfer knowledge between OT specialists due to the difference in OT environments in the various sectors. There is a limited number of specialists who have the required expertise. This is caused in part by the fact that training courses focus more on IT security. It is also due in part to the fact that traditionally there has been less attention for the security of OT environments because of the separation from other networks.[143] [144]

Although for a long period of time resilience against digital threats was not a priority, the threat of disruptions and the importance of digital resilience has become more necessary and is being acknowledged more broadly over the past years. In view of the growing attack surface and the potentially-disruptive consequences of a digital attack against OT systems, it is important to build on this. Investments, building up knowledge and supporting technological developments are essential in this connection.[145] [146]

An IT failure might bring train traffic to a halt. Travellers will be waiting in vain for their trains to arrive or they might be forced to spend the night at the train station.

5 Reflection strategic themes

In the CSAN 2022, the NCTV, in cooperation with partners, identified six strategic themes that will be relevant to the digital security of the Netherlands in the coming years. These themes still apply in full. Reduction of the imbalance between the digital threat and resilience referred to in CSAN 2022 therefore remains a major challenge.

Several changes stood out during the reflection on these themes:

- the additional digital security requirements that arise inter alia from new European legislation and regulations;
- the further hardening of geopolitical tensions;
- the insurability of digital risks being under pressure;
- the increasing interwovenness within the broader ecosystem;
- the structure of opportunity for cyberattacks formed by the digital ecosystem.

An additional 'new' insight is that digital risks form an integral part of a broader and complex range of risks and have several other special characteristics. This means that digital risks require a broader method of risk management than other risks.

The six strategic themes mentioned in CSAN 2022 are briefly explained in this chapter. New insights that have arisen or changes that have occurred are addressed in separate (sub)paragraphs. The heading of each (sub)paragraph contains the essence of the new insight or change.

Strategic themes indicated in CSAN 2022

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

New European legislation and regulations and the Dutch Cybersecurity Strategy 2022-2028 and the action plan derived from it impose further requirements on digital security. They deserve individual attention as these requirements have an impact on all strategic themes indicated in this chapter.

EU and the Netherlands increase requirements for digital security

EU increases requirements for digital security

The EU increases the requirements for digital security by means of European legislation and regulations. The EU attempts by means of the **Digital Services Act** (DSA) to regulate the responsibility and liability of internet providers, hosting companies, online platforms, search engines and market places. The EU **Digital Markets Act** (DMA) should result in additional market and merger supervision of and in competition rules for the world's largest online platforms. The agreements concerning the DMA and the DSA are intended to enter into effect in the Member States from the middle of 2024.[147] The EU attempts by means of the **Cyber Resilience Act** (CRA) to realise a safer European digital internal market and a society in which unsafe products can be barred and removed from the market.[148] The Netherlands aims to have implemented the CRA in 2024.[149] Furthermore, the Network and Information Security Directive (NIS) was revised, which has resulted in the **NIS2 Directive**. The NIS2 Directive regulates which companies must meet mandatory security requirements. The new NIS means that more organisations come under the operation of the Network and Information Security Act (Wbni) than is currently the case. The NIS2 Directive also tightens several other aspects of the existing directive. It concerns for example requirements pertaining to risk management, the use of encryption, an obligation for handling data breaches and reporting cybersecurity incidents. The NIS2 Directive will be implemented in the Netherlands in 2024 via the Wbni.[150]

Dutch Cybersecurity Strategy imposes stricter requirements on digital security

The new Dutch Cybersecurity Strategy 2022-2028 and the action plan linked to it impose stricter requirements on digital security and by extension digital resilience. The strategy aims for a future in which the imbalance between the digital threat and resilience is and remains as small as possible. The government thus increases the incentives for security in digital markets by imposing stricter requirements on digital products and services, risk management of organisations, etcetera. The strategy expressly builds on the European legislation and regulations referred to above. In addition to imposing requirements, the strategy also mentions numerous objectives, ambitions and activities to increase the digital resilience of the Netherlands.

Implementation takes time

Organisations, service providers and producers will have to comply with the new legislation and regulations. Awareness and further elaboration and implementation of all of the above will take some time. The requirements cannot be enforced in the short term until they have been converted in the legislation in the EU countries. A transitional arrangement applies to the security requirements for digital products for example. Certification and supervision still have to be set up. The current, partly insecure products will continue to be used for a considerable amount of time and new, insecure products will still enter the market.[151]

By contrast, several improvements have already been implemented or set in motion. For example, the NCSC has been permitted by law since 1 December 2022 to share threat information with non-vital companies as well. In addition, the first steps have been taken in joining the National Cybersecurity Centre (NCSC), the Digital Trust Center (DTC) and the Cybersecurity Incident Response Team for digital service providers (CSIRT-DSP) into a single central expert centre and information hub. This new institution will provide all organisations in the Netherlands, large or small, public or private, vital or non-vital, with appropriate information and knowledge.[152]

Risks form the downside of a digitised society

Explanation of the strategic theme

Dutch society is highly digitised and the COVID-19 pandemic further accelerated the digitisation of processes. This has a downside: the dependence on digital processes has also made us vulnerable to failure and activities of malicious actors. The high degree of digitisation of our society and the dependence on digital processes are a given. Getting and keeping vulnerabilities under control is part of risk control.

Digital threats are part of a dynamic, complex and broader threat landscape

Digital threats often do not exist in isolation and are part of a dynamic, complex and broader threat landscape. Cyber incidents can be the result of a disruption to the electricity supply for example. Conversely, they can become the cause of a disruption to the electricity supply.[153]

In addition, there is a whole tangle of developments that has an impact on threats that can strengthen or weaken each other. The energy transition for example increases the digital attack surface for malicious actors. The reason being that the operation of solar parks and the transport of energy generated by solar panels and wind turbines (and suchlike) depend on technology.[154]

Threats may also accumulate steadily without being noticed until a tipping point is reached whereafter it is very difficult to reverse those threats. These are known as dormant threats. Such a steady accumulation may occur for example in the case of dependencies on Big Tech. Whereas companies ‘automatically’ opt for large players in the market on the basis of economic logic, there is a risk that over time an undesirable dependency on the offer arises ‘automatically’.

In addition, dormant or new threats may arise from technological developments. For example, computing power is increasing due to Quantum computing. This may mean that in future protocols and sensitive data that are now adequately secured by means of encryption will no longer be so.[155] Companies fully invest in what is known as the metaverse. It is difficult to assess what this will look like and to what extent it will play a role in our society and economy. This also makes it difficult to estimate what the metaverse will mean for digital security. Experience shows that new technology implies both threats and risks.

Swift development and use of generative AI has an impact on digital security

One example that shows that other, in this case technological, developments can have an impact on digital security is 'Generative AI'. This is a form of AI that can create new content from existing content, based on prompts or questions that are entered by users. ChatGPT, which is an example of this, caused a hype in November 2022 and has been the subject of debate ever since. An improved version of the underlying language model (GPT-4), which delivers even more advanced results, was published in March 2023.

The use and possibilities of generative AI are still fully developing and the impact on society still has many uncertainties. So far, four relevant perspectives can be identified in any event:

1. The algorithms and data used to feed the algorithms may be manipulated deliberately. This is possible by means of cyberattacks, but not just by means of cyberattacks.

2. Users may (intentionally and unintentionally) grant access to search queries and/or sensitive information by means of the questions they ask, the information they enter or the information they feed into the applications.[156]

3. Generative AI can be used for cyberattacks. For example, phishing e-mails more tailored to the recipient can be created. This increases the chance that the recipient considers it to be reliable. Low-threshold malware can be developed as well.[157]

4. Generative AI can be used to defend against cyberattacks, for example by generating cybersecurity advice.

If these techniques are used on a large scale, it will become more difficult to determine the authenticity and authority of textual information, images, videos and audio. Generative AI may produce and disseminate factually-incorrect information, even without malicious intent.

Digital threat remains high

The nature of digital risks has not changed fundamentally

The digital risks already mentioned in CSAN 2022 still have the same nature (see below). The risks also apply directly or indirectly to specific sectors and organisations and individual citizens.

Four national security risks

1. Unauthorised access to information (and possibly its publication), in particular through espionage. Examples include espionage targeting communications within the central government or the development of innovative technologies. It also involves access to information about employees or business processes as a springboard for cyberattacks or other malicious purposes.
2. Inaccessibility of processes, due to sabotage of processes responsible for the energy supply, or from cybercrime, including the application of ransomware and DDoS attacks.
3. Breaches of (the security of) cyberspace, such as through the misuse of global chains of ICT service providers, the exploitation of internet protocols or the sabotage of cables.
4. Large-scale outages: situations in which one or more processes are disrupted due to natural or technical causes or unintentional human action.

Digital threats as great as ever

The collection of digital threats is undiminished. This has various causes. Firstly, there is the interaction with other, certainly also non-digital threats and developments referred to above. A second cause arises from the complexity and interwovenness of digital processes, systems and networks. The consequence thereof is a large and growing attack surface for malicious actors and an increased probability of failure. Attack surface refers to the ways in which a malicious actor is able to attack digital processes. This includes (components of) hardware, software and networks, as well as the embedding in the broader ecosystem (see below). Organisational or human vulnerabilities that are or could be exploited are found time and again in digital processes. The probability of large-scale failure is also increasing due to complexity and interwovenness. Outdated systems (legacy) also increase the risk of failure.

A third cause arises from geopolitical tensions between countries, and the war against Ukraine in particular. This means that state actors increasingly often carry out cyberattacks resulting in chain effects for example (see further in chapter 3).

A fourth cause is the attractive revenue model for cybercriminals. This certainly applies to ransomware attacks, 'commercialisation' of cyberattacks in the shape of Cybercrime-as-a-Service (CaaS) and the enrichment and sale of the stolen information (see below).

International conflicts and socially-controversial domestic subjects as a possible reason for hacktivism constitute a fifth cause. There was a revival of hacktivism in 2022 in particular as a result of the war against Ukraine (see chapters 2 and 3). There are disagreements between population groups in the Netherlands and abroad concerning many subjects, and hacktivists may involve themselves. Hacktivists appear to be taking an increasing interest in compromising OT, because it can be used as a coercive measure to realise ideological objectives (see chapter 4). However, as indicated above, it is the case that the impact of hacktivist activities is often short in duration and limited. Attribution is also difficult because hacktivist groups are generally loosely organised and, what is more, mixing with state actors cannot be excluded. Dutch citizens may be involved in hacktivism abroad because they join foreign hacktivist groups.

A sixth cause is the concentration of information and digital processes in the interest of the business operations. These are very attractive to exploitation by malicious actors. The Dutch Data Protection Authority points out the risks related to a central database containing all personal data provided by people in connection with a passport application, such as fingerprints, signatures and passport photos. Such a database with information concerning a large number of Dutch citizens entails major privacy risks and uncertainty could arise as to who is responsible for the security of the data.[158] Such a large concentration of information also constitutes an attractive target for cyber actors and the many related processes may come to a standstill in case of a failure.

The limited chance for malicious actors of being caught and/or extradited for carrying out a cyberattack constitutes a seventh cause. Malicious actors are sometimes charged, but they retain their freedom of movement in their own country or they are not extradited. It is not without reason that it was indicated in CSAN 2022 that cyberattacks by state actors appear to be the new normal. It is true that attempts are being made to formulate standards and values for conduct in cyberspace, but in practice, this is extremely difficult. The number of documented cases in which criminal actors were arrested and tried all over the world is very small.

Divergent threat sources

Similarly to previous years, state and criminal actors are responsible for the overwhelming majority of cyberattacks. It should be noted that state and criminal actors may cooperate in different ways (intentionally or unintentionally) and that it is not always possible to draw a clear dividing line. It is expected that cybercriminals will continue to form a prominent part of disruptive cyberattacks in the Netherlands with the use of ransomware attacks in particular. The consequence could be that stolen information is published or traded between criminals.

Although it appeals to the imagination to a lesser extent, failure also presents a threat. In addition to technical and human failures, this can also have physical causes, such as floods, wildfires, and failure of vital processes.

Hacktivists also pose a threat (see above). Cyberattacks by insiders should also be taken into account, such as an employee who was recently fired, script kiddies, actors who carry out cyberattacks just for fun or to show what they are capable of, and terrorists to a lesser degree.

All digital processes, organisations and sectors are attractive to cyber actors

Cyber actors focus actively on gaining access to and/or the collection of as much information as possible. For example, Dutch organisations are large-scale targets of various digital attack campaigns by states for the purpose of stealing high-level technology and knowledge.[159] The AIVD refers specifically to China, Iran, North Korea and Russia in the 2022 annual report. The service indicates that the risks of these attacks are enormous, for both the government, companies and institutions, and ultimately citizens.[160] The MIVD also warns of the cyber threat posed by state actors in the 2022 annual report.[161]

State actors actively search for weak links in chains as a stepping stone to (more) interesting targets. It is also the case that criminals continuously attempt to open all 'digital doors' irrespective of the organisation, with all resultant consequences for the victims. Actors can use stolen information a) as a stepping stone for cyberattacks or cybercrime, b) to blackmail victims with the threat of publication, c) by creating credibility for the spread of disinformation using stolen data.

Actors also focus on rendering digital processes inaccessible, such as by means of ransomware attacks, DDoS attacks or other (acts in preparation of) sabotage. Possible motives for this include blackmail, creating reputational damage, revenge or geopolitical considerations.

Sectors or organisations that do not appear to be interesting to attackers may nevertheless be attractive as a stepping stone towards a different primary target. Attackers focus predominantly on targets that could act as a springboard to other targets. Central targets on which many sectors, organisations and processes depend, such as ICT service providers, are also interesting targets. This in order to indirectly affect other processes, organisations and sectors. The fact that various suppliers of hardware and software have acquired a (semi) monopolistic position has resulted in global ecosystems with large concentrations of personal data. For example, organisations that carry out the salary administration of other organisations process information that can be very valuable to attackers. In 2022, the AIVD concluded that various countries with an offensive cyber programme were attempting to steal data within the (European) travel and aviation sector. They combine that information with other information in order to identify, trace or follow people who are interesting to them.[162] Organisations that process a lot of information are therefore an attractive target to cyber actors. The MIVD reported during the reporting year that state actors hacked routers of Dutch private citizens and small and medium-sized enterprises. This actor can exploit the hacked routers to carry out secret cyber operations against Dutch interests or those of allies.[163]

Symbolic Dutch targets, such internationally known Dutch multinationals or authorities, may also be a target, with the underlying motive of revenge against the Netherlands or the Dutch government (see the Annual review).

Cyberspace is a playing field for regional and global dominance

Explanation of the strategic theme

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

Hardening of geopolitical tensions

The geopolitical situation has hardened over the past year. State actors therefore increasingly use cyberattacks as a means of looking after their interests, which may result in chain effects. Such chain effects may occur unexpectedly. The war against Ukraine is a prime example of the geopolitical hardening (see chapter 3). The recent Threat Assessment State-sponsored Actors presents four key messages: 1) the territorial security of the EU, NATO and the Netherlands is under further pressure, 2) the social and political stability of the Netherlands is still being impacted by state sponsored interference, 3) the Netherlands is increasingly facing open and covert threats against its economic security, and 4) the international rule of law is increasingly coming under pressure. It is also argued that the Netherlands is still the target of offensive cyber programmes implemented by state actors.[164] The MIVD also warns against physical sabotage, such as the sabotage of internet cables. For example, Russia is mapping the vital maritime infrastructure in the North Sea, and is developing activities that indicate espionage and acts in preparation of disruption and sabotage.[165] This could have an impact on cyberspace if such activities are successful.

Sectors and organisations may experience the consequences of this hardening, but can do little about it. It therefore constitutes a factor that must be taken into account when determining the desired level of digital resilience.

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

Explanation of the strategic theme

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

Criminal extortion remains an attractive revenue model

Extortion by cybercriminals remains an attractive revenue model. This certainly applies to the encryption of files and/or the threat of publication of stolen information. The professionalisation and commercialisation of cybercrime tools and services continues to increase. It is not just the case that only technically advanced criminals are able to make money from this, the possibilities for a broader group of criminals to carry out cyberattacks are increasing as well. The police conclude for example that the manner in which criminals gain access to the network of victims is becoming ever more complex. This means that for example multi-factor authentication is not always sufficient anymore.[166] Enormous amounts of money are demanded and sometimes paid as part of ransomware attacks.

The risks to criminals of being caught or convicted remain relatively low. Whereas the pressure on for example the Russian government to deal with criminals in their own country was increasing by the middle of 2021, that pressure now effectively no longer exists as a result of the conflict between Russia and Ukraine and the subsequent geopolitical isolation of Russia. This creates space for cybercriminals in Russia to do as they please and remain relatively undisturbed.

Risks for cybercriminals do continue to exist however. Known ransomware groups change their name or divide up into smaller cells. This could have various causes. It may concern attempts to circumvent growing pressure applied by international investigative services and international sanctions. This is confirmed by the fact that rebranding or termination of a group often takes place following media attention for large incidents or attacks with a major impact. These groups may be afraid that the likelihood of internal conflicts is larger within large groups as a result of what are known as the Conti leaks. Leaked chat conversations from the Conti group revealed details of the size, leadership and the operations of the notorious ransomware group. The documents were likely leaked in retaliation for Conti's pro-Russian attitude.[167] The war means that the probability of disagreements or different loyalties between group members has increased. This also increases the risks of people defecting to other groups, or members who leak source codes of malware developed by the groups themselves for example.[168]

The number of registered cases of cybercrime, such as hacking, carrying out DDoS attacks or ransomware attacks, decreased slightly in the 2022 calendar year when compared to 2021. The police registered 13,949 incidents in 2022, which is a decrease of 2 percent when compared to 2021.[169]The number of ransomware attacks (also against Dutch organisations) also appeared to decrease temporarily in 2022, but increased again towards the end of the year. The impact of the Russian war against Ukraine on the cybercriminal ecosystem presumably plays a role in this. Both countries are important source countries of serious, organised cybercrime.[170] Criminals chose a side in the war, which put pressure on existing partnerships. This decrease – whether temporary or not – should be seen in the right perspective, however. The police figures are still worryingly high. Companies as well as municipalities and public institutions are faced with the undiminished risk of falling victim to ransomware or other forms of cybercrime. Matters are not always reported to the police in order to avoid reputational damage for example.[171]

Police investigation showed that criminals enrich stolen information with other information and sell it on. This has proven to be lucrative. The same investigation showed that criminals sometimes also enrich and sell stolen information even though the victim paid the criminals to prevent the information from being published.[172]

Criminals appear to be carrying out cyberattacks against vital sectors more often

Ransomware attacks, especially those in the US, appear to be increasingly often targeting vital sectors such as the energy sector.[173] In Europe, several companies in the energy sector became the victim of cyberattacks.[174 175] In one case, this also had an impact on a subsidiary in the Netherlands. In Belgium, a ransomware group managed to steal sensitive information from the police.[176] Ransomware attacks were also carried out against municipalities. This resulted inter alia in the fact that municipal tasks could not be performed or could only be performed to a limited extent for some time, while there are no alternatives to the performance of those municipal tasks (see the Annual review). On the one hand, vital sectors form an attractive target because the consequences of ransomware can be so large that those sectors might be more willing to pay. On the other hand, they are not an attractive target because such attacks result in more attention from the government, which could turn out negatively for the criminals.

Cybercriminals depend on the mala fide and bona fide digital ecosystem and are therefore vulnerable

Similarly to legal organisations, cybercriminals cannot avoid being part of a broader digital ecosystem. This ecosystem forms an opportunity structure for cybercriminals. The increasing specialisation among cybercriminals means they also become more dependent on each other's (online) services within the context of cyber-crime-as-a-service. This dependency also applies to the purchase of legal services. Webhosting is a good example. Bona fide Dutch hosting companies rent out space on the internet to host a website or cloud service for example. They often unknowingly rent out space on their servers to foreign companies, known as resellers. Mala fide, often Russian, resellers in turn rent out these servers knowingly and wilfully to criminals, as is concluded by the police. Ransomware gangs eagerly use this to carry out their attacks.[177] In addition, state actors have been using the Dutch digital infrastructure for many years.[178]

A cybercriminal who wishes to victimise the end user needs an entire chain to carry out his crimes. In addition to webhosting, the dependence of cybercriminals also applies to numerous other internet services such as communication services like VPN, domain registrations, and even regional internet registers and transit providers. These dependencies go hand in hand with the enormous scalability of cybercrime. Moreover: cybercriminals cannot operate without both the legal and the mala fide service providers (and the grey area in between).

The dependence on the broader digital ecosystem forms a weak spot for cybercriminals, but also for malicious state actors. This dependency provides opportunities for increasing digital resilience by creating barriers against mala fide use. Legislation and regulations are commonly used in the financial sector to counter money laundering in which connection unusual transactions have to be reported as a rule. Where it concerns internet services in the broader sense, principles such as acceptable use, know-your-customer, the principle of due diligence and anti-exploitation provisions are often still without obligation, resulting in ample scope for compliance or non-compliance. This offers cybercriminals many opportunities to work anonymously and in a scalable manner – opportunities which they take.

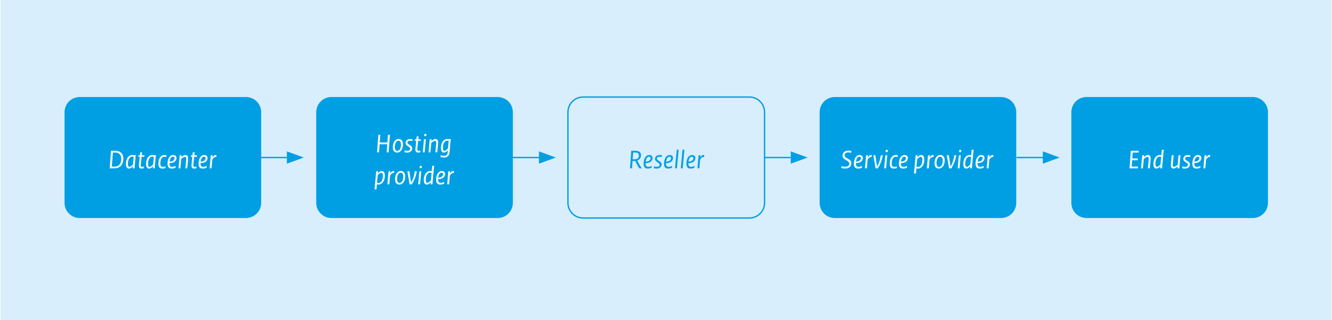

***Image 1** dependencies within webhosting*

Market dynamics complicate controlling digital risks

Explanation of the strategic theme

Supply and demand of digital services, hardware and hardware components, software and networks meet on digital markets. These markets have several unique characteristics, such as the monopoly or semi-monopoly status of certain suppliers, the high level of interwovenness and the focus on gathering as much data as possible. Moreover, incentives for digital security are not always decisive in these markets. Those characteristics complicate risk control for individual citizens, organisations, sectors and countries. This creates a paradox. On the one hand, individual decisions by citizens, organisations, sectors and countries can increase or decrease the risks for others. On the other hand, the scope for making autonomous choices with respect to risk management is actually limited due to a lack of realistic or safe(r) alternatives.

Insurability of digital risks under pressure

Although organisations can do a lot as regards digital resilience, cyber incidents can nevertheless occur and/or damage cannot always be prevented. Cyber insurance may cover damage in the event a cyber incident has occurred, provide support during a cyber incident and impose requirements with respect to resilience before insurance can be taken out.

The insurability of digital risks is under pressure for several reasons. The first reason mentioned by insurers is the increase in digital risks. The number of cyberattacks and consequently the damage caused by it has been increasing for years. The claims mean that insurers tighten their policy conditions and premiums increase. In addition, an increasing number of customers have to meet strict security requirements. Those whose score is insufficient do not get a policy.[179] Insurance is also under pressure because cyber incidents may evolve into a systemic crisis and therefore become uninsurable.[180] Past incidents such as Wannacry and NotPetya play a role in that insight. For example, an American insurance company has to compensate 1.4 billion Dollar in damage sustained by a pharmaceutical company due to NotPetya.[181] In addition, the market for cybersecurity insurance is limited in size in the Netherlands and in its infancy. According to De Nederlandsche Bank (DNB) this is related to a lack of historical data, which means that data concerning incidents and the resulting damage are limited. Furthermore, many companies and households are unaware of the potential damage digital risks entail. Combined with the unawareness of many incidents, this obstructs the further development of this insurance market.[182]

There is also often uncertainty about the cover of risks resulting from cyber incidents within existing (traditional) insurance. This is referred to as ‘silent cyber’, the cover of cyber damage in traditional policies, while this is not expressly provided for in these policies. As a result of this, European supervisory authority EIOPA identifies risks with respect to increasing uncertainty about the cover of risks resulting from cyber incidents. This uncertainty is caused in part by unclear definitions where it concerns cyber incidents. This could result in uncertainty for policyholders regarding the degree of cover provided by their policies and the usefulness and need for possible additional cyber insurance.[183]

DNB warns against exclusion of customers with an increased risk profile.[184] In addition to exclusion, organisations may also be faced with premiums that are so high or requirements that are so strict that they must decide against insurance. All of the above may ultimately result in financially healthy organisations collapsing due to damage they sustain as a result of cyber incidents.

Coordinated and integrated risk management is still in its infancy

Explanation of the strategic theme

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

New European legislation and regulations mean that directors of many organisations within the EU have a larger responsibility for controlling digital risks laid down in law.

Being part of a broader ecosystem complicates risk management

Whether it concerns countries, sectors or organisations, few will be able to function independently of a broader ecosystem. This complicates risk management.

Being part of a broader ecosystem has many benefits, inter alia with respect to digital security. This applies for example to cloud facilities, which provide the technical infrastructure. This has now become so complicated that outsourcing may be a rational choice and may actually contribute to digital security. What is known as 'network-as-a-service' therefore meets an ever-increasing need.[185]

Being part of a broader ecosystem also has its disadvantages. It is difficult to provide insight into the risks. It is no longer sufficient to merely consider the supply chain of the own organisation, sector or country. For example, sectors and service providers are becoming active in more partnerships and they therefore become connected at more layers and along more lines. This means that risks become connected as well.[186] It is rarely clear to an individual sector or organisation which dependencies and therefore which vulnerabilities exist. It is usually not clear until an incident occurs that a large part of the organisations within a sector purchases services from a single party. Incidents at such a party, irrespective of the nature or cause, may have a large-scale national or even cross-border impact.

One prominent example of this occurred in March 2023. Companies and organisations, including several big ones, purchase services from market research agencies, which in turn are customers of the same software supplier. An actor gained access to the network of the software supplier and allegedly actually stole data. As a result, the data of an estimated approximately 2 million Dutch citizens were leaked.[187] This example therefore involved the customers of companies and organisations falling victim to a data breach at the software supplier of market research agencies. This means they were victims in the third line.

Risks that are the consequence of incidents at third parties are more difficult to control. The interests of an organisation that has fallen victim to a cyber incident may clash for example with those of other organisations that depend on it. For example, an organisation may prioritise restoring the operation of digital processes following a ransomware attack. Gaining insight into what information of which customers was leaked and/or was already published as a means of exerting pressure, may not happen in such cases, but this could result in damage for customers in the chain. In addition, powers are not always clear with such incidents, as became apparent during the ransomware attack at a large supplier for applications relating to authentication and access passes[188] and from the above-mentioned case.[189] For example, is a cybersecurity company hired by a victim allowed to share findings with the NCSC and/or the police and/or the Chief Information Security Officer of a department that is a customer? What information are these parties allowed to request from the organisation affected and should it comply?

Limited insight into and unpredictability of the impact of the digital threat

There is limited insight into the possible impact of the digital threat and this impact is highly unpredictable. This also applies to the assessment of the consequences of cyber incidents that occur[VIII], especially for the level of national security and sectors.

Many actors and factors influence the assessment of the consequences of specific cyber incidents. For example, the consequences of a specific digital espionage campaign are difficult to assess: what was stolen, by whom, over which period, what is its value in use to the perpetrator and what is then the financial and/or reputational damage in the short or medium term (and suchlike)? Those questions are difficult if not impossible to answer. For the National Digital Crisis Plan it was decided to select several building blocks, because countless situations are conceivable where it concerns cyber incidents, especially when combined with a possible impact on the physical domain. These building blocks contain meaningful differences for the consequences of a cyber incident. It concerns the following building blocks: cause, source, actor, affected domain, area affected and technical solution perspective.[190]

The consequences of all cyber incidents within a sector or within the Netherlands are even more difficult to analyse objectively. For example, the consequences of a digital espionage campaign against several companies may appear to be less severe than expected. Over a prolonged period of time however, digital espionage can create a persistent 'leak' of high-level economic knowledge to foreign countries, which can have consequences for the vitality of the Dutch economy. The effect of such a 'leak' is uncertain, however, and unfolds over a long period of time.[191]

[VIII] Gevolgen wordt vooral gebruikt in combinatie met cyberincidenten. Impact wordt vooral gebruikt in combinatie met dreiging.

Digital risks demand a broader method of risk management

For several years, the CSAN has been devoting attention to the importance of risk management in order to make the Netherlands, sectors and organisations more resilient against the digital threat. One must bear in mind however that digital risks have several special characteristics that demand a broader control method than other risks. This applies at the level of organisations, but certainly also at the sectoral and national level. The six strategic themes that individually and jointly constitute complications to risk management specifically with respect to digital risks have been pointed out above. Furthermore, digital risks form part of a broader, dynamic and complex range of risks. It is also the case that cyberspace is an extremely complex system when compared to other risks. Although information about cyber incidents is sometimes available, it is not nearly available to everyone. It is only comparable to a limited extent and difficult to interpret. For example, for the purpose of controlling floods a lot more information is available and over a longer period of time. Simulating incidents or building models in order to analyse the progress and consequences of incidents is useful to risk management, but highly complex where it concerns digital risks. And it goes without saying that the internet cannot be disconnected for a day to see what will happen.

Another special characteristic is that at the national, sectoral and organisational level there is an incomplete image of the costs and benefits of investing in digital resilience and of the various uncertainties.[192] It became clear on many occasions that far from all politicians and directors appear to be aware of digital risks. Supervisory authorities identified a narrowing of scope within risk management. Focusing too much on certain types of threats, such as criminal actors, means that other risks to the continuity of services receive no or too little attention.[193] Incidents, such as the ransomware attack against Maastricht University in 2019 and that against the municipality of Hof van Twente in 2020, do however result in additional awareness and additional measures by similar organisations.

Digital security is an enormous challenge for municipalities

Professor Bibi van den Berg indicates in this connection: "*The risks remain abstract as long as things do not go wrong. You simply do not know what can happen, let alone how you may prevent 'it' from occurring. And if you implement certain measures, you often do not even know whether they are helping because they are hidden digitally in the technology. Contrary to a very large lock on the door for example, which you can simply see. This makes it more difficult to acknowledge the need to invest in digital security. It is quite complicated to determine whether a certain incident does not occur because you implemented measures or whether it is merely a coincidence. I can therefore easily imagine that municipal authorities say: we would rather spend the money on the social domain. Until things go wrong and you are confronted with how incredibly extensive digital systems actually are. And suddenly nothing works anymore. [....] In case of digital burglary, a perpetrator may sometimes have been inside for months without you noticing it. And it is often the case that your digital jewels have not disappeared; in the digital world stealing often means copying. This means that we have to think differently about security than we were used to for physical security.*"[196]

How could digital risks be controlled (even) better? Although the CSAN is not intended to outline a perspective for action or to propose measures, we have provided several considerations below.

Basic measures still appear to form an effective barrier against many forms of cyberattack. Microsoft argues that basic measures protect against no less than 98% of cyberattacks.[194] The NCSC also mentions several basic measures every organisation should implement in order to counter cyberattacks. The NCSC sees that organisations are vulnerable in the event of cyber incidents if these measures have not been implemented.

Professor Bibi van den Berg argues inter alia for increasing the resilience of organisations that are or were confronted with cyber incidents and for raising barriers to divergent cyber incidents. Segmenting networks is one example of a barrier that can help against various types of incidents.[195] Whereas segmentation is common in buildings in order to control the consequences of a possible fire, segmentation is not always customary in the technical infrastructure. Adequately-trained employees and citizens also form a barrier to divergent cyber incidents. Professor Jan van den Berg therefore argues for adequately training people for example so that they are able to carry out the right digital activities in their various roles.

It follows from the nature of the importance of digital security and the nature of the digital threat that controlling digital risks is certainly not only an issue for technical experts. It is also, or perhaps mainly, an issue of governance and/or risk management for politicians and managers at the level of organisations, sectors and countries. Moreover, digital risks are an integral part of a broader range of risks and therefore require integral risk management.

If there is one area in which experiences from the past do not provide guarantees for the future it is digital security. This is the reason for the appeal to look beyond incidents that occurred and beyond the requirements that must be met. This applies for example to anticipating the possible consequences of technological developments for digital security. Another perspective is that of 'assume breach', whereby one assumes a cyber incident already exists.

Restrictions in digital autonomy also restrict digital resilience

Explanation of the strategic theme

Restrictions in digital autonomy apply to European countries and the Netherlands (hereinafter the Netherlands). That autonomy includes the ability and resources the Netherlands has to make independent decisions about (further) digitisation and the required level of digital resilience. Restrictions in digital autonomy also involve restrictions concerning resilience. Autonomy is under pressure for various reasons, which are related to the other strategic themes. Those causes reduce the options to influence and make choices in terms of the digital resilience of the Netherlands and how to control this resilience.

This theme, as briefly explained in the frame above, still applies in full.

A technical failure in the water supply could be reason as to why there is little to no water coming from the faucet. The high demand for water makes for empty shelves in the stores.

Albert Heijn
Geachte Klant,
Wegens omstandigheden is het water uitverkocht.
Wij verwachten de nieuwe levering op maandag rond de klok van 14.00 uur
Excuus voor het ongemak
Albert Heijn Doesburg

6 Threat scenarios

The previous chapters devoted attention to digital threats, as well as to resilience and the interests that are in jeopardy when cyber incidents occur. Reference was made in this connection to risks that arise from the fact that organisations form part of a broader ecosystem. For the purpose of this chapter, the National Cybersecurity Centre and the Digital Trust Center formulated three fictitious scenarios in which a cyber incident in an ecosystem not only results in problems within the organisation where the incident occurs, but also in damage to society or other organisations within the ecosystem. The damage caused by cyber incidents is not just limited to direct financial damage, but may also constitute a danger to employees and the surrounding environment. The consequences of a cyber incident are often long term, particularly when trust in an organisation has been damaged.

You can use these scenarios to establish the degree of digital resilience of your organisation, customers and/or suppliers. You can find information on achieving greater control of digital risks on the website of the DTC[IX] and the NCSC.[X]

The scenarios below are fictitious. Any similarity to existing products, organisations, persons or events is based on pure coincidence and not intended as such.

[IX] Carry out the Basic Cyber Resilience Scan of the Digital Trust Center: https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid

[X] Read the 'Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt' of the Nationaal Cybersecurity Centrum: https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

No milk on the shelves

Description of the events

At the start of March 2022, just before the start of a long weekend, the planning department of transport company Negotium BV from Zwolle receives a report from drivers that they are at the wrong farm. Farmers are also reporting that their milk is not being collected. The planning department ensures that the empty lorries eventually go to the 'forgotten' farmers. Problem solved. The planning department enjoys the long weekend. The planning department opens its mailbox on Tuesday morning and it is full. At 7 a.m. the telephone starts ringing. Tank lorries are in the wrong place and farmers are forced to discharge milk because their storage capacity is full. The milk factories are on the phone. Their stocks for making daily fresh milk are nearly depleted because milk is no longer being delivered.

The Negotium BV IT department starts an investigation. The problem appears to be located in the planning system. This system is outdated and no update has been provided for 2 years. The director has to call supplier Aedificium BV for an on-site intervention. However, Aedificium BV has a bigger problem. It is being inundated with questions because their software package is being used by more transport companies and does not operate correctly there either.

Following days of investigation, in turns out the cause lies in a frequently-used library that records information provided by the user in the database. The data entered after 22-02-2022 proves to be unreliable. The library is unable to handle data correctly after this date entry and therefore no longer registers appointments correctly.

In the meantime, there is no more fresh milk on the shelves. There are also concerns about the quality of the surface water because farmers discharge their milk or indicate that they will be doing so. Negotium BV is able to schedule and send lorries manually, but the supervisory authority prohibits the milk factory from accepting the milk without full electronic registration. This means that the shelves for day fresh milk will remain empty for quite some time. The production of other dairy products has also stopped. There is a run on non-perishable products. It will take weeks before the supermarkets can be supplied with fresh milk and dairy as usual. Negotium BV and all other customers of Aedificium BV will start using a new planning system. Not everyone is able to do so at the same time. It takes longer than expected before everyone is convinced and proper planning can resume.

Explanation

If ain't broke, don't fix it. A truth that used to hold true, but certainly does not apply to a lot of software and hardware. Errors in these are discovered daily. Not just in the software or systems themselves, but precisely also in the underlying components. Nevertheless, not all companies and organisations are aware of the risks of using outdated software and hardware. In addition, organisations are often not aware either which systems they are using and which software components are processed in these. It even happens that the disruption of primary processes, especially in 24/7 business operations, has such an impact that all of the business operations stop. So it can have major consequences. In such a situation, it is difficult to find out why an error occurs, where it occurs and how it can be resolved. In addition, these types of errors can have a direct impact on not only the company itself, but also on the chain to which it is connected digitally. It may also have consequences in the physical world, such as with respect to dairy products on the shelves in this case.

Key questions for the reader

1. Do you know what software and hardware you use?
2. Do you know whether all of your software and hardware and underlying components are up to date?
3. Do you have a continuity plan in the event the IT support of your primary process is interrupted? And when was the last time you tested this?
4. What support arrangements did you make with your suppliers of IT, software and hardware?
5. How well do you know your chain and do you have insight into the joint risks in the event a link at your suppliers, service providers or customers in the chain is comprised and how are the responsibilities and powers arranged in case an incident occurs?

Not that smart after all, those devices

Description of the events

A client calls the M.M. Katz firm of civil-law notaries on Monday morning. It concerns an appointment scheduled for signing the deed of purchase of a large warehouse at a sheltered location at a 30-minute drive from the Maasvlakte. The client's voice contains a combination of fear and anger.

Two unknown and armed persons visited his home the previous night. They held a copy of his passport in order to be certain they were threatening the right person. A group of criminals had made up its mind to use a warehouse for illegal practices and the client was being forced to act as a cover by having the warehouse registered in his name, with some hush money in return. And failure to comply would be a 'mortal sin', according to the persons threatening him, because they were not playing games.

The client nevertheless called the civil-law notary on Monday morning. There is anger in his voice because he is convinced that his data were leaked via the civil-law notary. The civil-law notary is shaken and says that she will have a digital forensic investigation carried out.

The investigation shows that criminals had access to the civil-law notary's confidential information and copied and downloaded files for a prolonged period of time. They were able to do so because they acquired access to an administrative account. A Single Sign-On system allowed the civil-law notary to simply log in to consult different sources, such as the registers of the Land Registry Office and the Chamber of Commerce. This Single Sign-On system was not resilient against an attack and relinquished the password to an administrative account.

The first step of this attack was to establish a connection with the company network. A smart thermostat connected to the internet proved to be the weak link. The civil-law notary had installed it in the office to save energy. A visiting hacker found the device in an unguarded reception area and was able to manipulate it so that the thermostat gave remote access to the civil-law notary's network.

Investigators were unable to exclude the possibility that this attack crossed over to other parts of the notarial chain. And if it had not, it could still be repeated at other offices. The civil-law notary decided to file a report with the police after all and also warns her colleagues.

Explanation

This attack affected the confidentiality of a company network and that has serious consequences for the civil-law notary and her clients. The incident could also have an impact on national files because incorrect (manipulated) information can be placed in them. A malicious actor could further exploitation information that may have been manipulated and other persons would also suffer the consequences thereof. In the extreme case, i.e. if the exploitation were to take place at a large scale, it could even result in impairment of the confidence in a professional group and/or national registrations. Everyday information for one organisation could therefore have great value in the wrong hands and should be secured adequately. The weakest link ultimately determines the strength of the entire chain. Organisations can prevent digital incidents or detect them in time by implementing basic measures.

The civil-law notary example show the risks of a smart device, which was a thermostat in this case, which is connected to a company network without separating or segmenting the network from business-critical systems and applications. The administrative account did not require multifactor authentication, which meant that the hackers only needed a password to acquire control. Log information enabled forensic investigators to dissect the attack. Organisations can use log information to detect a digital burglary earlier in order to prevent damage.

Key questions for the reader

1. Do you know which devices on your company network are connected and whether they meet your security standards? Do you supervise newly-connected devices?
2. What measures have you implemented in order to separate mobile devices and smart devices owned by employees and visitors using Wi-Fi from the network traffic of managed devices?
3. Do you know which organisational processes and data could be of particular value to (organised) criminals, state actors or hacktivists?
4. Do you have your own monitoring and detection capacity or did you purchase this as a service? Are you aware of what exactly is being monitored and what types of threat are and are not detected?
5. Are you familiar with of or do you apply an assume breach strategy? In other words: what is your perspective for action if it is assumed that your organisation may be confronted with a cyber incident at some time?
6. Have you ever thought about which company you could engage in the event of a cyber incident at your organisation and if so, have you contacted the company just in case?

Hack by hacktivists during a strike

Description of the events

It is a weekday, but there is no one to be found within the BIV Plastics factory hall. This medium-sized enterprise produces plastics with critical applications for the aerospace industry and refineries among others. However, employee Wim is most proud of the daily delivery of medical packages for hospitals in the region. But not today. They are on strike. Talks have broken down after a considerable time of negotiations concerning a new CLA and the employees subsequently stopped working.

Devon is Wim's son. At home, they discuss the frustrations of the work and the rising inflation. Devon himself is also frustrated with the company where his father works. He joined a group of environmental activists and is afraid that BIV Plastics' production is a danger to people and the environment. If it were up to him the factory would remain closed for longer. Devon has discovered another passion in addition to environmental protection: hacking. Although he is not yet able to develop his own codes, he has already quickly learnt to find and use accessible, of-the-shelf hack tools.

The notion had appeared to Devon previously, but he decides to take action when his father comes home from another day on strike without a breakthrough. He starts to digitally snoop around the plastics factory. Using the special Shodan search engine, he discovers that various BIV Plastics devices are connected to the internet. He even finds several sensors that supervise the production process as operational technology (OT). But because he is not entirely sure what will happen if he starts messing around with the sensors, he continues to search for a system that is more visible to the public.

He finds another target. The software that makes it possible to administer the website and place information on it, i.e. the Content Management System (CMS), proves to be not up to date. Devon manages to crack the access using his tools. He also simply guesses the username and password that grant access to the webhoster's portal (admin, BIV12345). Once inside the CMS, he decides to deface the website or, in other words, daub it digitally. The front page shows the slogan of his group in large font: 'People & PLANET' with a thick line crossing out 'Profit'. The activist group spreads their action very quickly via social media. Devon also changes the passwords for access to the webhoster and that of the e-mail addresses. BIV Plastics manages to take the website offline after 24 hours and regain access to the webhoster. It will take until the end of the strike before the website has been restored to its former condition. Surprised by Devon's easy success, fellow activists manage to repeat the defacement on websites of other companies they consider to be polluting.

Explanation

A website is more than a business card. It is often also a platform for accepting orders and providing services, and it can be hacked in different ways. In this scenario, an actor with an activist motive was able to cause damage using free and easy-to-use attack tools. And on top of this, he did it at a vulnerable moment.

It could have ended differently. An attacker with a different motive and more experience could perhaps also have sabotaged the production line with all resultant consequences, or could have further exploited access to the webhoster. And what if the attack had not come from outside but from within? Would Devon using Wim's work laptop, or an employee from within the company have been able to attack other systems as well?

Key questions for the reader

1. Do you know which systems of your organisation can be approached via the internet?
2. How do you manage which systems the various employees have access to, and are you able to adjust that access adequately in case someone changes positions or an employment contract is terminated? Do you also register the activities of employees on the systems?
3. What checks monitor whether your systems and OT equipment (such as sensors) operate correctly?
4. Does your continuity plan include a communication plan in the event that you do not have access to your official communication channels?
5. Are you aware of your obligations imposed by regulations and insurers in the event that a cyber incident occurs? Do you know how to submit a report to the police?

Annex 1

Rationale behind the creation of the CSAN

The Cybersecurity Assessment Netherlands has been drawn up by the National Coordinator for Counterterrorism and Security (NCTV) and the National Cybersecurity Centre (NCSC). It is defined annually by the NCTV. It gratefully makes use of the information, insights and expertise of government services, organisations in critical processes, science and other parties.

The formulation of the CSAN is divided into three phases:

1. Analysis

The NCTV collects and analyses relevant information about incidents, trends and shifts in the area of the triangle of interest, threat and resilience. The following questions form the basis for the CSAN:

1. What relevant incidents occurred in the Netherlands in the period from 1 March 2022 up to and including February 2023? What type of incidents were they? What caused them and what damage/impact did they cause/have?
2. Which events, developments or insights have an influence on the strategic themes identified in CSAN 2022 and what influence do they have?
3. What changes can be identified that have an influence on interests that may be affected when cyber incidents occur and what could their impact be?
4. What changes can be identified that could have an influence on digital threats affecting national security?
5. What changes can be identified as regards the degree to which the Netherlands is resilient against those digital threats?
6. To what extent do changes occur in the main risks to the national security of the Netherlands?

NCTV analysts started working on these questions and an initial inventory of 'ingredients' for the CSAN was carried out during the analysis phase. In addition, several potential themes were identified for the theme chapters. The results were presented to and discussed with external government partners and colleagues of the NCSC and subsequently supplemented. On the bases of these discussions, it was decided to include a separate theme chapter about operational technology (chapter 4) and about the war against Ukraine (chapter 3).

2. Writing and peer review

The draft chapters were written by separate (teams of) authors after completion of the analysis phase.

The entire text undergoes several peer reviews within the NCTV and the NCSC. Several draft chapters were reviewed in the interim. The NCTV is responsible for the final editing of all the chapters.

Key assessment	NCTV
Chapter 1	NCTV
Chapter 2	NCTV and NCSC
Chapter 3	NCTV
Chapter 4	NCTV
Chapter 5	NCTV, with additions by the police regarding ransomware and 'digitale ecosystemen vormen gelegenheidsstructuur voor cyberaanvallen'
Chapter 6	NCTV
Acknowledgements	NCTV

3. Validation

The CSAN undergoes a comprehensive validation process, in which the draft text is presented to external partners for comments. After processing all the comments, the definitive text is prepared and adopted by the NCTV. Following publication of the CSAN, an extensive internal and external evaluation takes place. The collected feedback is processed in the CSAN procedure of the following year.

Annex 2

Sources and references

1 Since the CSAN 2021 a new conceptual framework is being used, for the creation of which grateful use was made of: J. van den Berg, ‘A basic set of mental models for understanding and dealing with the cybersecurity challenges of today’, Journal of Information Warfare 19:1 (2020). https://repository.tudelft.nl/islandora/object/uuid%3A41a590a2-e11b-4ad3-b5aa-f3e51b2b7313

2 'Grote treinstoring opnieuw veroorzaakt door falend back-upsysteem ProRail’, Security.nl, 02-08-2022, https://www.security.nl/posting/763403/Grote+treinstoring+opnieuw+veroorzaakt+door+falend+back-upsysteem+ProRail

3 ‘Rapport: Europese landen bespioneren burgers maar zijn daar niet open over’, Nu.nl, 08-11-2022, https://www.nu.nl/tech/6234738/rapport-europese-landen-bespioneren-burgers-maar-zijn-daar-niet-open-over.html

4 ‘An Overview of the Increasing Wiper Malware Threat’, Fortinet, 28-04-2022, https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

5 ‘The Year of the Wiper’, Fortinet, 24-01-2023, https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

6 ‘SwiftSlicer: New destructive wiper malware strikes Ukraine’, ESET, 27-01-2023, https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/

7 ‘Fantasy – a new Agrius wiper deployed through a supplychain attack’, ESET, 7-12-2022, https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/

8 ‘LokiLocker ransomware family spotted with built-in wiper’, The Register, 16-03-2022, https://www.theregister.com/2022/03/16/blackberry_lokilocker_ransomware/

9 ‘Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War’, Bloomberg, 07-03-2022, https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine

10 ‘Bug in software van Alstom leidt tot problemen op het spoor’, Executive People, 18-03-2022, https://executive-people.nl/693857/bug-in-software-van-alstom-leidt-tot-problemen-op-het-spoor.html

‘Outage disrupts Polish trains as Ukrainian refugees head west’, Reuters, 17-03-2022, https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/

11 ‘Datalek bij woningcorporaties na ransomware-aanval op ict-dienstverlener’, Security.nl, 06-04-2022, https://www.security.nl/posting/749309/Datalek+bij+woningcorporaties+na+ransomware-aanval+op+ict-dienstverlener

12 ‘Breaking! Black Byte Ransoming 11.000 PDF Scans Of GEBE St Maarten Customers, Internal Powerplant Operations, Technical Scans And Financial BAU records’, St Maarten News, 30-03-2022, https://stmaartennews.org/breaking-black-byte-ransoming-11-000-pdf-scans-of-gebe-st-maarten-customers-internal-powerplant-operations-technical-scans-and-financial-bau-records/

‘GEBE investigating cyberattack, says efforts focused on minimising impact’, The Daily Herald, 31-03-2022, https://www.thedailyherald.sx/islands/gebe-investigating-cyberattack-says-efforts-focused-on-minimising-impact

13 ‘Nederlandse windmolens konden door ransomware-aanval niet proefdraaien’, Security.nl, 17-08-2022, https://www.security.nl/posting/764826/Nederlandse+windmolens+konden+door+ransomware-aanval+niet+proefdraaien

‘Nordex Group impacted by cybersecurity incident’, Nordex Online, 02-04-2022, https://www.nordex-online.com/en/2022/04/nordex-group-impacted-by-cyber-security-incident/

‘Antwoord op vragen van het lid Eerdmans over het hacken van windturbines’, Tweede Kamer, 16-08-2022, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z13483&did=2022D32554

14 ‘ESET onderzoek: Lazarus valt wereldwijd lucht-, ruimtevaart- en defensiebedrijven aan via LinkedIn en WhatsApp’, ESET, 01-06-2022, https://www.eset.com/nl/over/newsroom/persberichten-overzicht/persberichten/lazarus-valt-wereldwijd-aan/

‘Noord-Koreaanse hackers keken mee in systemen van Nederlands defensiebedrijf’, Nu.nl, 01-06-2022, https://www.nu.nl/tech/6204153/noord-koreaanse-hackers-keken-mee-in-systemen-van-nederlands-defensiebedrijf.html#coral_talk_wrapper

‘Noord-Koreaanse hackers vielen Nederlands defensiebedrijf binnen’, Techzine, 01-06-2022, https://www.techzine.nl/nieuws/security/490085/noord-koreaanse-hackers-vielen-nederlands-defensiebedrijf-binnen/.

15 ‘I-SEC attacked by Conti threat actors’, DataBreaches.net, 05-04-2022, https://www.databreaches.net/i-sec-attacked-by-conti-threat-actors/

‘Persoonsgegevens gelekt bij Schiphol-beveiligingsbedrijf I-SEC’, Nu.nl, 03-05-2022, https://www.nu.nl/tech/6198666/persoonsgegevens-gelekt-bij-schiphol-beveiligingsbedrijf-i-sec.html

16 ‘Bestanden van Gelderse gemeenten staan op darkweb na ransomwareaanval’, Tweakers, 21-04-2022, https://tweakers.net/nieuws/195868/bestanden-van-gelderse-gemeenten-staan-op-darkweb-na-ransomwareaanval.html

'Datadiefstal gemeente Buren', Gemeente Buren, 08-07-2022, https://www.buren.nl/nieuws/gegevens-aangeboden-op-het-darkweb/7399/

17 'Datalek gemeente Veenendaal door technische handeling softwareleverancier', Security.nl, 23-06-2022, https://www.security.nl/posting/758076/Datalek+gemeente+Veenendaal+door+technische+handeling+softwareleverancier

'Persbericht: Onderzoek naar datalek raadsinformatiesysteem afgerond', Gemeente Veenendaal, 21-06-2022, https://veenendaal.raadsinformatie.nl/document/11618256/1/PERS2022_33+-+Onderzoek+naar+datalek+raadsinformatiesysteem+afgerond

'Datalek gemeente Veenendaal veroorzaakt door menselijke fout', VPNGids, 23-06-2022, https://www.vpngids.nl/nieuws/datalek-gemeente-veenendaal-veroorzaakt-door-menselijke-fout/

18 'Artis getroffen door ransomware: hackers eisen 1 miljoen losgeld', RTL Nieuws, 28-06-2022, https://www.rtlnieuws.nl/tech/artikel/5317902/artis-dierentuin-hackers

'ARTIS doelwit van cyberaanval', ARTIS, 28-06-2022, https://www.artis.nl/nl/ontdek/nieuws/2022/06/28/ARTIS-doelwit-cyberaanval/

'Artis betaalde hackers geen miljoen euro aan cryptovaluta', Het Parool, 18-07-2022, https://www.parool.nl/amsterdam/artis-betaalde-hackers-geen-miljoen-euro-aan-cryptovaluta~bee5680f/

19 'Ransomware-aanval in Noordenveld: mogelijk gevolgen voor afhandeling bijstandsuitkeringen', RTV Drenthe, 29-07-2022, https://www.rtvdrenthe.nl/nieuws/14848823/ransomware-aanval-in-noordenveld-mogelijk-gevolgen-voor-afhandeling-bijstandsuitkeringen

'Gemeente Noordenveld getroffen door ransomware-aanval', Security.nl, 01-08-2022, https://www.security.nl/posting/763248/Gemeente+Noordenveld+getroffen+door+ransomware-aanval

20 'Grote treinstoring opnieuw veroorzaakt door falend back-upsysteem ProRail', Security.nl, 02-08-2022, https://www.security.nl/posting/763403/Grote+treinstoring+opnieuw+veroorzaakt+door+falend+back-upsysteem+ProRail

'ProRail opnieuw geconfronteerd met falende back-up tijdens ICT-storing', SpoorPro, 01-08-2022, https://www.spoorpro.nl/spoorbouw/2022/08/01/prorail-opnieuw-geconfronteerd-met-falende-back-up-tijdens-ict-storing/?gdpr=deny

21 'Informatiepagina cyberincident augustus 2022, Colosseum Dental, 08-08-2022, https://www.colosseumdental.nl/mededeling-cyberincident

'Meer dan 100 tandartspraktijken dagen dicht door cyberaanval', RTL Nieuws, 05-08-2022, https://www.rtlnieuws.nl/economie/bedrijven/artikel/5325232/meer-dan-100-tandartspraktijken-dicht-door-cyberaanval

22 'Hackers vallen softwareleverancier van vijf Limburgse gemeenten aan', Tweakers, 17-08-2022, https://tweakers.net/nieuws/200002/hackers-vallen-softwareleverancier-van-vijf-limburgse-gemeenten-aan.html

'Vijf Limburgse gemeenten getroffen door hack', Binnenlands Bestuur, 17-08-2022, https://www.binnenlandsbestuur.nl/digitaal/vijf-gemeenten-limburg-getroffen-door-cyberhack

23 'informatie over het herstellen van onze diensten na de cyberaanval op ista.', Ista, 29-07-2022, https://www.ista.com/nl/updates

'Woningcorporaties melden datalek na cyberaanval op energiedienstverlener ista', Security.nl, 04-08-2022, https://www.security.nl/posting/763659/Woningcorporaties+melden+datalek+na+cyberaanval+op+energiedienstverlener+ista

'Bij ista gestolen privédata van 146.000 mensen op internet gepubliceerd', Security.nl, 25-08-2022, https://www.security.nl/posting/765725/Bij+ista+gestolen+priv%C3%A9data+van+146_000+mensen+op+internet+gepubliceerd

'UPDATE: Geen datalek bij ISTA Nederland. Gegevens van gebruikers zijn veilig', Havensteder, 23-08-2022, https://www.havensteder.nl/nieuws/2981/ista-een-leverancier-van-havensteder-is-getroffen-door-een-cyberaanval

24 'Grote storing Maastricht UMC+: afspraken poli's afgezegd', 1Limburg, 08-09-2022, https://www.1limburg.nl/nieuws/1839619/grote-storing-maastricht-umc-afspraken-polis-afgezegd

'Technische oorzaak IT-storing', Maastrict UMC+, 20-09-2022, https://www.mumc.nl/actueel/nieuws/technische-oorzaak-it-storing

25 'DigiD was urenlang beperkt beschikbaar vanwege ddos-aanvallen', Nu.nl, 12-09-2022, https://www.nu.nl/tech/6223663/digid-was-urenlang-beperkt-beschikbaar-vanwege-ddos-aanvallen.html

26 'Incident Statement @ ID-ware', ID-ware, n.d., https://www.id-ware.com/en/about/news/incident-statement.html

'Gegevens van toegangspassen Tweede Kamerleden gelekt door hack', NOS, 07-10-2022, https://nos.nl/artikel/2447439-gegevens-van-toegangspassen-tweede-kamerleden-gelekt-door-hack

'High Tech Campus slachtoffer van hack bij leverancier toegangspassen', Omroep Brabant, 15-10-2022, https://www.omroepbrabant.nl/nieuws/4164616/high-tech-campus-slachtoffer-van-hack-bij-leverancier-toegangspassen

'Adresgegevens duizenden studenten TU Eindhoven liggen op straat na hack', Nu.nl, 20-10-2022, https://www.nu.nl/tech/6231140/adresgegevens-duizenden-studenten-tu-eindhoven-liggen-op-straat-na-hack.html

'Privégegevens personeel Hogeschool Utrecht op darkweb na hack', RTV Utrecht, 20-10-2022, https://www.rtvutrecht.nl/nieuws/3487233/privegegevens-personeel-hogeschool-utrecht-op-darkweb-na-hack

'Data Kamerleden gelekt door hack bij ict-bedrijf: gegevens toegangspassen online', De Volkskrant, 07-10-2022, https://www.volkskrant.nl/nieuws-achtergrond/data-kamerleden-gelekt-door-hack-bij-ict-bedrijf-gegevens-toegangspassen-online~b7051db9/

27 'Nederlands vaccinbedrijf Bilthoven Biologicals getroffen door ransomware', Security.nl, 11-11-2022, https://www.security.nl/posting/774235/Nederlands+vaccinbedrijf+Bilthoven+Biologicals+getroffen+door+ransomware

'Nederlands vaccinbedrijf gehackt, gestolen data op dark web', RTL Nieuws, 11-11-2022, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5345841/vaccinbedrijf-ransomware-bilthoven-biologicals

'Ransomware bij vaccinmaker in Bilthoven, onderzoeksdata gestolen', NOS, 11-11-2022, https://nos.nl/artikel/2452020-ransomware-bij-vaccinmaker-in-bilthoven-onderzoeksdata-gestolen

28 'Landelijke politienummers moeilijk of zelfs niet bereikbaar door storing', Nu.nl, 18-10-2022, https://www.nu.nl/tech/6230635/landelijke-politienummers-moeilijk-of-zelfs-niet-bereikbaar-door-storing.html

'Politienummer moeilijk bereikbaar door landelijke storing: 'Bij tips over Amber Alert kan je 112 bellen'', Noordhollands Dagblad, 18-10-2022, https://www.noordhollandsdagblad.nl/cnt/dmf20221018_48887529

29 ‘Hacker (19) maakt tienduizenden zorgdossiers buit bij digitale inbraak Nedap Groenlo’, De Gelderlander, 25-10-2022, https://www.gelderlander.nl/achterhoek/hacker-19-maakt-tienduizenden-zorgdossiers-buit-bij-digitale-inbraak-nedap-groenlo~ab723a6a/ ‘Zorginstellingen melden datalek na inbraak bij digitaal zorgplatform Carenzorgt’, Security.nl, 02-11-2022, https://www.security.nl/posting/773253/Zorginstellingen+melden+datalek+na+inbraak+bij+digitaal+zorgplatform+Carenzorgt

‘Kwetsbaarheid in Carenzorgt’, Carenzorgt, n.d., https://carenzorgt.freshdesk.com/support/solutions/articles/75000112826-kwetsbaarheid-in-carenzorgt

‘Zorginstellingen melden datalek na diefstal van documenten bij Carenzorgt’, Opgelicht!? – AVROTROS, 03-11-2022, https://opgelicht.avrotros.nl/alerts/artikel/zorginstellingen-melden-datalek-na-hack-bij-carenzorgt/

30 ‘Grote ict-storing Pantar waarschijnlijk door inbraak op systeem’, Security.nl, 04-12-2022, https://www.security.nl/posting/776668/Grote+ict-storing+Pantar+waarschijnlijk+door+inbraak+op+systeem

‘ICT-storing Stichting Panta’, Raad van Toezicht Stichting Pantar Amsterdam, 02-12-2022, https://amsterdam.raadsinformatie.nl/document/12138703/1/2022-12-02_brief_ICT_storing_Pantar_brief_-_RvT_aan_Wth_RGW

‘Vragen en antwoorden – Hack bij Pantar’, Pantar, 22-12-2022, https://pantar.nl/hack/

31 ‘Datalek Caiway en Delta raakt waarschijnlijk tienduizenden klanten’, Security.nl, 06-12-2022, https://www.security.nl/posting/777008/Datalek+Caiway+en+Delta+raakt+waarschijnlijk+tienduizenden+klanten

‘Data theft at DELTA Mobile and Caiway Mobile’, Deltafiber, 06-12-2022, https://www.deltafiber.nl/en/news/data-theft-at-delta-mobile-and-caiway-mobile/

‘Datadiefstal bij DELTA Mobiel’, Delta, n.d., https://www.delta.nl/klantenservice/datadiefstal/

32 ‘Cyberaanval veroorzaakt problemen bij groothandel Makro’, Nu.nl, 08-12-2022, https://www.nu.nl/tech/6241024/cyberaanval-veroorzaakt-problemen-bij-groothandel-makro.html

‘@MakroNederland’, Twitter, 08-12-2022, https://twitter.com/MakroNederland/status/1600781020793634816

33 ‘Leids UMC was ook doelwit van ddos-aanval’, AD, 31-01-2023, https://www.ad.nl/leiden/leids-umc-was-ook-doelwit-van-ddos-aanval~a5b6ae2c

34 ‘Ook Maastricht UMC en instantie Z-CERT doelwit van pro-Russische cyberaanval’, AD, 31-01-2023, https://www.ad.nl/maastricht/ook-maastricht-umc-en-instantie-z-cert-doelwit-van-pro-russische-cyberaanval~a0b1aae3

35 ‘DDoS-aanval op websites UMCG duurt voort, verschillende diensten uit de lucht’, RTV Noord, 28-01-2022, https://www.rtvnoord.nl/nieuws/993500/ddos-aanval-op-websites-umcg-duurt-voort-verschillende-diensten-uit-de-lucht-update

36 ‘Russische DDOS-aanvallers vallen Nederlandse ziekenhuizen aan’, NOS Nieuws, 30-01-2022, https://nos.nl/artikel/2461833-russische-ddos-aanvallers-vallen-nederlandse-ziekenhuizen-aan

37 ‘Weekend met DDoS aanvallen op Nederlandse cyberspace en ESXi kwetsbaarheid’, Emerce, 06-02-2023, https://www.emerce.nl/wire/weekend-ddos-aanvallen-nederlandse-cyberspace-esxi-kwetsbaarheid

‘Your banks are unable to transact. If you do not respect the Quran, we will not respect you. https://regiobank.nl - down @RegioBank

#opholland #holland #bank #cyberattack #botnet #breaking #news #breakingnews #cyber #hack #hacker #hacking #hacked #banking #database #security’, @thtghostkiller, 13-02-2023, https://twitter.com/thtghostkiller/status/1625225884075433984

38 ‘How the French fiber optic cable attacks accentuate critical infrastructure vulnerabilities’, Cyberscoop, 28-04-2022, https://cyberscoop.com/french-fiber-optic-cables-attack-critical-infrastructure/

39 ‘Pegasus spyware targets top Catalan politicians and activists’, Politico, 18-04-2022, https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians-and-activists/

40 ‘Spanish prime minister’s phone ‘targeted with Pegasus spyware’’, The Guardian, 02-05-2022, https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware

41 Costa Rica declares state of emergency over ransomware attack, NBC News, 11-05-2022, https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415

42 ‘Polish officials found to be targeted with Israeli NSO group’s spyware’, Times of Israel, 08-07-2022, https://www.timesofisrael.com/polish-officials-found-to-be-targeted-with-israeli-nso-groups-spyware/

43 ‘Albania shuts down government websites, services due to wide ranging cyberattack’, The Record, 18-07-2022, https://therecord.media/albania-shuts-down-government-websites-services-due-to-wide-ranging-cyberattack/

‘Albania severs diplomatic ties with Iran over cyber-attack’, BBC News, 07-09-2022, https://www.bbc.com/news/world-europe-62821757

44 EU Commission alarmed by new spyware case against Greek socialist leader, Euractiv, 27-07-2022, https://www.euractiv.com/section/politics/news/eu-commission-alarmed-by-new-spyware-case-against-greek-socialist-leader/

45 ‘BlackCat ransomware claims attack on European gas pipeline’, Bleepingcomputer, 01-08-2022, https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

46 ‘Another European nation hit by hackers, Montenegro grapples with ongoing ransomware attack’, Cyberscoop, 02-09-2022, https://cyberscoop.com/montenegro-ransomware-attack/

47 ‘Bosnia and Herzegovina investigating alleged ransomware attack on parliament’, The Record, 19-09-2022, https://therecord.media/bosnia-and-herzegovina-investigating-alleged-ransomware-attack-on-parliament/

48 ‘Major German energy supplier hit by cyberattack’, The Record, 27-10-2022, https://therecord.media/major-german-energy-supplier-hit-by-cyberattack/

49 ‘European Parliament website hit by cyberattack after Russian terrorism vote’, Politico, 23-11-2022, https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/

‘Russische hackers claimen aanval op Europees Parlement’, Computable, 24-11-2022, https://www.computable.nl/artikel/nieuws/overheid/7438668/250449/russische-hackers-claimen-aanval-op-europees-parlement.html

‘European Parliament website hit by DDoS cyberattack from Russia’s Killnet’, TechMonitor, 24-11-2022, https://techmonitor.ai/technology/cybersecurity/european-parliament-cyberattack-ddos-killnet

‘Pro-Russia Killnet Group Takes Down the European Parliament Website’, SpiceWorks, 24-11-2022, https://www.spiceworks.com/it-security/security-general/news/european-parliament-ddos-attack/

50 ‘Rusthuizen schakelen over op pen en papier na massale cyberaan-

val op Antwerpse stadsdiensten’, HLN.be, 06-12-2022, https://www.hln.be/antwerpen/rusthuizen-schakelen-over-op-pen-en-papier-na-massale-cyberaanval-op-antwerpse-stadsdiensten~a24d88fa

‘PLAY ransomware group claims responsibility for Antwerp attack as second Belgian city confirms new incident’, The Record, 12-12-2022, https://therecord.media/play-ransomware-group-claims-responsibility-for-antwerp-attack-as-second-belgian-city-confirms-new-incident/

51 ‘Here’s what cyber pros are watching in the Ukraine conflict’, Washington Post, 24-2-2022, https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/

52 ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’, Wired, 22-8-2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

53 ‘Cyber War and Ukraine’, the Center for Strategic and International Studies, 16-6-2022, https://www.csis.org/analysis/cyber-war-and-ukraine

54 ‘24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis’, AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenisfile:///H:/Downloads/Brochure+24-2+De+Russische+aanval+op+Oekraine+-+een+keerpunt+in+de+geschiedenis+kl.pdf

55 ‘MIVD Jaarverslag 2022’, MIVD, 19-04-2023

56 ‘Evaluating the International Support to Ukrainian Cyber Defense’, Carnegie Endowment for International Peace, 3-11-2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322

57 ‘MIVD Jaarverslag 2022’, MIVD, 19-04-2023

58 ‘MIVD Jaarverslag 2022’, MIVD, 19-04-2023

59 ‘24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis’, AIVD/MIVD, 20-2-2023

60 ‘Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape’, Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

61 ‘Oekraïne blijft doelwit van Russische wiper en ransomware’, Dutch IT-channel, 1-2-2023, https://dutchitchannel.nl/714156/russische-apt-groepen-blijven-oekraine-aanvallen.html

62 ‘Russia hacked an American satellite company one hour before the Ukraine invasion’, MIT Technology Review, 10-5-2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/#:~:text=The%20attack%20on%20Viasat%20showcases%20cyber%27s%20emerging%20role%20in%20modern%20warfare.&text=Just%20an%20hour%20before%20Russian,EU%2C%20and%20UK%20said%20today.

63 ‘Cyberattack against Ukrtelecom on March 28: the details’, State Service of Special Communications and Information Protection of Ukraine, 6-4-2022, https://cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali

64 ‘Mustang Panda Uses the Russian- Ukrainian War to Attack Europe and Asia Pacific Targets’, BlackBerry, 12-6-2022, https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets

65 ‘NCSC-dreigingsanalyse, Q4 2022: oktober – december’, NCSC, 7-2-2023

66 ‘Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape’, Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

67 ‘Analyse van de gelekte interne Conti chat’, Orange Cyberdefense, 3-3-2022, https://www.orangecyberdefense.com/nl/blog/cyberdefense/analyse-van-de-gelekte-interne-conti-chat

68 ‘Russia-based ransomware group Conti issues warning to Kremlin foes’, Reuters, 25-2-2022, https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

69 ‘Dark Covenant 2.0: Cybercrime, the Russian State, and the War against Ukraine’, Recorded Future, 31-1-2023, https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

70 ‘Cybersecuritybeeld Nederland 2022’, NCTV, juni 2022

71 ‘In Cyber, Differentiating Between State Actors, Criminals Is a Blur’, DOD News, 14-5-2021, https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/

72 ‘Hacktivism Is Back and Messier Than Ever’, Wired, 27-12-2022, https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

73 ‘Anonymous: the hacker collective that has declared cyberwar on Russia’, The Guardian, 27-2-2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

74 ‘Digitale oorlog in Oekraïne: nog geen grote aanvallen, wel ‘online pesterijen’, NOS, 4-3-2022, https://nos.nl/nieuwsuur/collectie/13893/artikel/2419749-digitale-oorlog-in-oekraine-nog-geen-grote-aanvallen-wel-online-pesterijen

75 ‘‘Cyberpartisans’ hack Belarusian railway to disrupt Russian buildup’, the Guardian, 25-1-2022, https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

76 ‘Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol’, de Volkskrant, 24-9-2022, https://www.volkskrant.nl/kijkverder/v/2022/een-internationaal-cyberleger-tegen-rusland-met-een-nederlander-in-de-hoofdrol~v580287/?referrer=https%3A%2F%2Fwww.google.nl%2F

77 ‘Hacktivism Is Back and Messier Than Ever’, Wired, 27-12-2022, https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

78 ‘Dark Covenant 2.0: Cybercrime, the Russian State, and the War against Ukraine’, Recorded Future, 31-1-2023, https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

79 ‘Cybersecuritybeeld Nederland 2022’, NCTV, juni 2022

80 ‘Vier cybersecuritylessen uit één jaar oorlog in Oekraïne’, NCSC, 21-2-2023, https://www.ncsc.nl/documenten/publicaties/2023/februari/21/vier-cybersecuritylessen-uit-een-jaar-oorlog-in-oekraine

81 ‘Hoe helpt Microsoft Oekraïne in de oorlog met Rusland? ‘Dit is het eerste dataconflict uit de geschiedenis’’, Knack, 31-10-2022, https://www.knack.be/nieuws/wereld/hoe-helpt-microsoft-oekraine-in-de-oorlog-met-rusland-dit-is-het-eerste-dataconflict-uit-de-geschiedenis/

82 ‘Ukrainian vice prime ministers asks Elon Musk for Starlink satellites as Russia invades’, New York Post, 26-2-2022, https://nypost.com/2022/02/26/ukrainian-vice-prime-minister-asks-elon-musk-for-starlink-satellites-as-russia-invades/

83 ‘Ukraine’s engineers battle to keep the internet running while Russian bombs fall around them’, Forbes, 22-3-2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/

84 ‘Ukraine war: Major internet provider suffers cyber-attack’, BBC, 28-2-2022, https://www.bbc.com/news/60854881

85 ‘MIVD Jaarverslag 2022’, MIVD, 19-04-2023

86 ‘MIVD Jaarverslag 2022’, MIVD, 19-04-2023

87 ‘Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape’, Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

88 ‘24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis’, AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

89 ‘Big tech onder druk om mee te doen tegen desinformatie’, NOS, 28-2-2022, https://nos.nl/collectie/13888/artikel/2419291-big-tech-onder-druk-om-meer-te-doen-tegen-desinformatie-oekraine-oorlog

90 ‘Online platforms beperking in EU toegang tot Russische staatsmedia’, NOS, 1-3-2022, https://nos.nl/collectie/13888/artikel/2419312-online-platforms-beperken-in-eu-toegang-tot-russische-staatsmedia

91 ‘AIVD Jaarverslag 2022’, AIVD, 17-04-2023

92 ‘MIVD Jaarverslag 2022’, 19-04-2023

93 ‘Nederland zet 17 Russische diplomaten uit vanwege spionage’, NOS, 29-3-2022, https://nos.nl/artikel/2423081-nederland-zet-17-russische-diplomaten-uit-vanwege-spionage

94 ‘Polen wijst 45 Russische diplomaten uit, Moskou dreigt met vergelding’, NOS, 24-2-2022, https://nos.nl/collectie/13888/artikel/2422364-polen-wijst-45-russische-diplomaten-uit-moskou-dreigt-met-vergelding

95 ‘AIVD Jaarverslag 2022’, AIVD, 17-04-2023

96 ‘24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis’, AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

97 ‘24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis’, AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

98 ‘Digitale aanvallen oorlog Oekraïne’, NCSC, n.d. https://www.ncsc.nl/onderwerpen/oekraine

99 ‘Cybersecuritybeeld Nederland 2022’, NCTV, juni 2022

100 ‘Rijksbrede Risicoanalyse Nationale Veiligheid’, Analistennetwerk Nationale Veiligheid, 26-09-2022, https://www.nctv.nl/documenten/publicaties/2022/09/26/rijksbrede-risicoanalyse-nationale-veiligheid

101 ‘Voorbereiden op digitale ontwrichting’, WRR, 09-09-2019, https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

102 Zie bijvoorbeeld het scenario cyberaanval ICS - chemische sector in ‘Themarapportage cyberdreigingen’, onderdeel van de ‘Rijksbrede Risicoanalyse Nationale Veiligheid’, Analistennetwerk Nationale Veiligheid, 26-09-2022, https://www.nctv.nl/documenten/publicaties/2022/09/26/themarapportages-cyberdreigingen-2022

103 Robert M. Lee en Tim Conway, ‘The Five ICS Cybersecurity Critical Controls’, SANS Whitepaper, oktober 2022, https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

104 2021 ICS Cybersecurity Year in Review, Dragos, 29-12-2022, https://www.dragos.com/year-in-review/

105 Richard Thomas, Joe Gardiner, Tom Chothia, Manolis Samanis, Awais Rashid en Joshua Perrett. Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures. CPSIOTSEC, 2022

106 ‘The Ultimate Guide to Understanding OT Security’, Verve Industrial, 29-12-2022, https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security/

107 ‘OT:ICEFALL’, Vedere Labs (2022), 29-12-2022, https://www.forescout.com/resources/ot-icefall-report/

108 Ralph Langner, ‘What does “insecure by design” actually mean for OT/ICS security?’, OT base, 03-03-2019, https://www.langner.com/2019/03/what-does-insecure-by-design-actually-mean-for-ot-ics-security/

109 ‘The Convergence of IT and Operational Technology: Cyber Risks to Critical Infrastructure on the Rise’, Microsoft, Cyber Signals, December 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD

110 Mary Gutierrez-May, ‘Transparently Insecure Operational Technology: A Contextual Analysis’, SANS, 06-01-2022, https://www.giac.org/research-papers/transparently-insecure-operational-technology-a-contextual-analysis/

111 ‘Industrial Internet of Things (IIoT)’, Trend Micro, 29-12-2022, https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot

112 Dean Parsons, ‘The State of OT/ICS Cybersecurity in 2022 and Beyond’, SANS, 27-10-2022, https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond/

113 ‘Industroyer2: Industroyer reloaded’, ESET Research, 12-04-2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

114 ‘Sandworm Group (UAC-0082) cyberattack on Ukrainian energy facilities using INDUSTROYER2 and CADDYWIPER MALWARE (CERT-UA#4435)’, CERT-UA, 12-04-2022, https://cert.gov.ua/article/39518

115 Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden en Nathan Brubaker, ‘INDUSTROYER.V2: Old Malware Learns New Tricks’, Mandiant, 25-04-2022, https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks

116 ‘CHERNOVITE’s PIPEDREAM Malware Targeting Industrial Control Systems (ICS)’, Dragos, 13-04-2022, https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

117 Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt en Rob Caldwell, ‘INCONTROLLER: New State-Sponsored Cyberattack Tools Target Multiple Industrial Control Systems’, Mandiant, 13-04-2022, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

118 ‘Dreigingsbeeld Statelijke Actoren 2’, AIVD, MIVD, NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2

119 Marc Rivero, Jornt van der Wiel, Dmitry Galov en Sergey Lozhkin, ‘Luna and Black Basta — new ransomware for Windows, Linux and ESXi’, Securelist, Kaspersky, 20-07-2022, https://securelist.com/luna-black-basta-ransomware/106950/

120 Daniel Kapellmann Zafra, Keith Lunden, Nathan Brubaker en Jeremy Kennelly, ‘Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT’, Mandiant, 24-02-2022, https://www.mandiant.com/resources/blog/ransomware-against-machine-learning-to-disrupt-industrial-production

121 Nathan Brubaker, Daniel Kapellmann Zafra, Keith Lunden, Ken Proska en Corey Hildebrandt, ‘Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families’, Mandiant, 15-07-2022, https://www.mandiant.com/resources/blog/financially-motivated-actors-are-expanding-access-into-ot

122 @malwrhunterteam ‘Among the usual stuffs like passport photos and etc, Clop ransomware gang published these screenshots in the leak page for Thames Water…’, MalwareHunterTeam, 18-08-2022, https://twitter.com/malwrhunterteam/status/1559249802130497538

123 ‘Important Statement’, South Staffs Water, 15-08-2022, https://www.south-staffs-water.co.uk/news/important-statement

124 Dragos, ICS/OT CYBERSECURITY YEAR IN REVIEW 2022, https://www.dragos.com/year-in-review/

125 Vedere Labs, 'The Increasing Threat Posed by Hacktivist Attacks: An Analysis of Targeted Organizations, Devices and TTPs', Forescout, 01-12-2022, https://www.forescout.com/blog/the-increasing-threat-posed-by-hacktivist-attacks-an-analysis-of-targeted-organizations-devices-and-ttps/

126 'Global Hacktivism on the Rise', CYBLE, 25-07-2022, https://blog.cyble.com/2022/07/25/global-hacktivism-on-the-rise/

127 David Krivobokov, 'GhostSec Now Targeting Iranian ICS in Support of Hijab Protests', OTORIO, 06-10-2022, https://www.otorio.com/blog/ghostsec-now-targeting-iranian-ics-in-support-of-hijab-protests/

128 Michael J. Assante en Robert M. Lee, 'The Industrial Control System Cyber Kill Chain', SANS Whitepaper, 05-10-2015, https://www.sans.org/white-papers/36297/

129 Mandiant, 'GRU: Rise of the (Telegram) MinIOns', 23-09-2022, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

130 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

131 ENISA, 'NIS Investments 2022', 23-11-2022, https://www.enisa.europa.eu/publications/nis-investments-2022

132 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

133 Steve McIntosh, 'How to Overcome Vulnerability & Patch Management Challenges in Your OT Environment', Industrial Defender, 28-04-2021, https://www.industrialdefender.com/blog/how-to-overcome-vulnerability-patch-management-challenges-in-ot

134 J. Vos, P. Van den Brink en T. van Schie; TNO 2019 R11304 Succesfactoren voor digitaal veilige Operationele Technologie. TNO, 2019

135 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

136 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

137 NCTV, 'Nederlandse Cybersecuritystrategie 2022-2028', 10-10-2022, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

138 Ministerie van Infrastructuur en Waterstaat, 'Basismaatregelen voor cybersecurity van IACS', 10-10-2022, https://www.ncsc.nl/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs

139 Rijkswaterstaat &, 'Nieuwe richtlijn cybersecurity: veilig én werkbaar', Rijkswaterstaat, https://www.magazinesrijkswaterstaat.nl/zakelijkeninnovatie/2022/01/cybersecurity

140 Digital Trust Center, 'Doe de Security Check Procesautomatisering', https://www.digitaltrustcenter.nl/tools/doe-de-security-check-procesautomatisering

141 Europese Commissie, 'Cyber Resilience Act', 15-09-2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

142 Ralph Moonen, Sjoerd Peerlkamp, Bram Blauwendraad, 'Onderzoeksrapport Competenties IACS Security Teams', Secura, 18-11-2021, https://www.ncsc.nl/onderzoek/documenten/rapporten/2021/november/19/onderzoeksrapport-competenties-iacs-security-teams

143 Ralph Moonen, Sjoerd Peerlkamp, Bram Blauwendraad, 'Onderzoeksrapport Competenties IACS Security Teams', Secura, 18-11-2021, https://www.ncsc.nl/onderzoek/documenten/rapporten/2021/november/19/onderzoeksrapport-competenties-iacs-security-teams

144 ENISA, 'NIS Investments 2022', 23-11-2022, https://www.enisa.europa.eu/publications/nis-investments-2022

145 Cybersecurity Raad, 'Adviesrapport Integrale Aanpak Cyberweerbaarheid', 06-04-2021, https://www.rijksoverheid.nl/documenten/rapporten/2021/04/06/tk-bijlage-csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

146 NCTV, 'Nederlandse Cybersecuritystrategie 2022-2028', 10-10-2022, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

147 'Europees akkoord over vernieuwing basis digitale economie', Rijksoverheid.nl,23-04-2022, https://www.rijksoverheid.nl/actueel/nieuws/2022/04/22/europees-akkoord-over-vernieuwing-basis-digitale-economie.

148 'Beoordeling Verordening Cyber Resilience Act (CRA). Fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC)', Rijksoverheid.nl, 21-10-2022, https://open.overheid.nl/repository/ronl-3f800b4a35a8c2684d7337c14231b1e7441abfa8/1/pdf/fiche-1-verordening-cyber-resilience-act.pdf.

149 'Actieplan Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022.

150 'Europees Parlement publiceert wet die bedrijfsleven strenge securityeisen oplegt', Tweakers.nl, 27-12-2022, Europees Parlement publiceert wet die bedrijfsleven strenge securityeisen oplegt - IT Pro - Nieuws – Tweakers; 'Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022; 'Actieplan Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022.

151 Voor dat laatste: 'Onveilige 'slimme' apparaten straks van de markt geweerd, maar risico's blijven', NOS.nl, 23-10-2022,https://nos.nl/artikel/2449517-onveilige-slimme-apparaten-straks-van-de-markt-geweerd-maar-risico-s-blijven.

152 'Meer mogelijkheden NCSC om dreigings- en incidentinformatie te delen', NCSC, 01-12-2022, https://www.ncsc.nl/actueel/nieuws/2022/december/01/mogelijkheden-voor-het-delen-van-dreigings--en-incidentinformatie; 'Nationale cybersecurity organisaties gaan krachten bundelen', 07-09-2022, https://www.ncsc.nl/actueel/nieuws/2022/september/7/nationale-cybersecurity-organisaties-gaan-krachten-bundelen.

153 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

154 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

155 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022; ' Themarapportage Cyberdreigingen van het Analistennetwerk Nationale Veiligheid, Analistennetwerk Nationale Veiligheid, juli 2022.

156 'ChatGPT and large language models: what's the risk?', NCSC, 14-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

157 'ChatGPT and large language models: what's the risk?', NCSC, 14-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

158 'AP: centrale database paspoortgegevens groot risico', Autoriteit Persoonsgegevens, 30-01-2023,https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-centrale-database-paspoortgegevens-groot-risico.

159 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, p. 19, 33, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

160 'Jaarverslag AIVD 2022', AIVD, 17-04-2023, https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022.

161 'Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Openbaar jaarverslag 2022', Ministerie van Defensie, 19-04-2023, file:///H:/Downloads/openbaar-jaarverslag-mivd-2022.pdf.

162 'Jaarverslag AIVD 2022', AIVD, 17-04-2023, https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022.

163 'Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Openbaar jaarverslag 2022', Ministerie van Defensie, 19-04-2023, file:///H:/Downloads/openbaar-jaarverslag-mivd-2022.pdf.

164 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

165 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

166 Information provided by the High-Tech Crime Team.

167 'Conti ransomware's internal chats leaked after siding with Russia', 27-02-2022, https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/; 'Checkpoint, Leaks of conti ransomware group paint picture of a surprisingly normal tech start up sort of', 10-03-2022, https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/.

168 'Russia-Linked Ransomware Groups Are Changing Tactics to Dodge Crackdowns', The Wall Street Journal, 2-6-2022, https://www.wsj.com/articles/russia-linked-ransomware-groups-are-changing-tactics-to-dodge-crackdowns-11654178400

169 'Impact en schade cybercrime onverminderd groot', politie.nl, 19-1-2023, https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html.

170 Information provided by the High-Tech Crime Team.

171 'Impact en schade cybercrime onverminderd groot', politie.nl, 19-1-2023, https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html.

172 'Hackers opgepakt voor stelen miljoenen persoonsgegevens', NOS.nl,,23-02-2023, https://nos.nl/artikel/2464987-hackers-opgepakt-voor-stelen-miljoenen-persoonsgegevens.

173 'Ransomware Hackers Will Still Target Smaller Critical Infrastructure, CISA Director Warns''', Nextgov.com, 26-7-2022, https://www.nextgov.com/cybersecurity/2022/07/ransomware-hackers-will-still-target-smaller-critical-infrastructure-cisa-director-warns/374953/.

174 'Cyber-attack strikes German fuel supplies', BBC, 1-2-2022, https://www.bbc.com/news/technology-60215252

175 'BlackCat ransomware claims attack on Italian energy agency', Bleepingcomuter, 2-9-2022, https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/

176 'Ransomwaregroep steelt gevoelige data van politie in het Belgische Zwijndrecht', Security.nl, 25-11-2022, https://www.security.nl/posting/775732/Ransomwaregroep+steelt+gevoelige+data+van+politie+in+het+Belgische+Zwijndrecht

177 'Politie waarschuwt hostingsector voor hosting resellers', Politie, 12-10-2022, https://www.politie.nl/nieuws/2022/oktober/12/11-politie-waarschuwt-hostingsector-voor-hosting-resellers.html.

178 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

179 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668.

180 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/; 'Lloyd's stopt volgend jaar dekking voor catastrofale statelijke cyberaanvallen', Security.nl, 22-08-2022, https://www.security.nl/posting/765265/Lloyd%27s+stopt+volgend+jaar+dekking+voor+catastrofale+statelijke+cyberaanvallen; 'Verzekeraars in een veranderende wereld. Kansen en risico's in tijden van klimaatverandering, digitalisering en inflatie', De Nederlandsche Bank, 16-11-2022,https://www.dnb.nl/media/elrpseou/dnb-verzekeraars-in-een-veranderende-wereld.pdf.

181 Verzekeraar moet 1,4 miljard dollar schade door NotPetya bij Merck vergoeden, security.nl, 4-5-20223, https://www.security.nl/posting/795246/Verzekeraar+moet+1%2C4+miljard+dollar+schade+door+NotPetya+bij+Merck+vergoeden.

182 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/.

183 'Meer aandacht nodig voor silent cyber risico op traditionele verzekeringen', Verbond van verzekeraars, 17-6-2022, https://www.verzekeraars.nl/publicaties/actueel/meer-aandacht-nodig-voor-silent-cyber-risico-op-traditionele-verzekeringen;

'EIOPA publishes supervisory statements on exclusions related to systemic events and the management of non-affirmative cyber exposures', European Insurance and Occupational Pensons authority, 22-09-2022, https://www.eiopa.europa.eu/eiopa-publishes-supervisory-statements-exclusions-related-systemic-events-and-management-non-2022-09-22_en;

'Supervisory statement on the management of non-affirmative cyber exposures', European Insurance and Occupational Pensons authority, 22-09-2022, https://www.eiopa.europa.eu/publications/supervisory-statement-management-non-affirmative-cyber-exposures_en.

184 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/.

185 ''Negen op de tien bedrijven willen over op netwerk-as-a-service'', TECHZINE, 20-10-2022, https://www.techzine.nl/nieuws/infrastructure/505860/negen-op-de-tien-bedrijven-willen-over-op-netwerk-as-a-service/; 'Network-as-a-service: opkomst van soepel netwerk', Computable.nl, 20-7-2022, https://www.computable.nl/artikel/blogs/management/7361407/5260614/network-as-a-service-opkomst-van-soepel-netwerk.html.

186 'Toezichthouders publiceren samenhangend beeld cybersecurity vitale processen', Inspectie Justitie en Veiligheid,06-07-2022, https://www.inspectie-jenv.nl/actueel/nieuws/2022/07/06/toezichthouders-publiceren-samenhangend-beeld-cybersecurity-vitale-processen;

'Samenhangend inspectiebeeld cybersecurityvitale processen 2021-2022', Agentschap Telecom, juni 2022.

187 'Nebu moet aan Blauw informatie verstrekken over datalekken', de Rechtspraak, 06-04-2023, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Rotterdam/Nieuws/Paginas/Nebu-moet-aan-Blauw-informatie-verstrekken-over-datalekken.aspx ;'Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen', NOS.nl, 30-03-2023,https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen.

188 Voor dat laatste: 'We zagen het lek, maar mochten niets zeggen',De Volkskrant, 14-01-2023.

189 'Nebu moet aan Blauw informatie verstrekken over datalekken', de Rechtspraak, 06-04-2023, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Rotterdam/Nieuws/Paginas/Nebu-moet-aan-Blauw-informatie-verstrekken-over-datalekken.aspx ;'Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen', NOS.nl, 30-03-2023,https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen.

190 'Landelijk Crisisplan Digitaal', NCTV, december 2022,https://open.overheid.nl/documenten/ronl-43856896b0650c8210331268of9c-830c09b5f485/pdf.

191 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

192 'Risicorapportage cyberveiligheid economie 2019', Centraal Planbureau, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

193 'Toezichthouders publiceren samenhangend beeld cybersecurity vitale processen', Inspectie Justitie en Veiligheid,06-07-2022, https://www.inspectie-jenv.nl/actueel/nieuws/2022/07/06/toezichthouders-publiceren-samenhangend-beeld-cybersecurity-vitale-processen;'Samenhangend inspectiebeeld cybersecurityvitale processen 2021-2022', Agentschap Telecom, juni 2022.

194 'Microsoft Digital Defense Report 2022', Microsoft, 2022, p. 108, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

195 Based on a conversation with professor Bibi van de Berg on 11 January 2023.

196 'Een digitaal veilige gemeente begint niet bij de burgemeester', Nederlands Genootschap van Burgemeesters,3-1-2023,https://www.burgemeesters.nl/actueel/nieuws/een-digitaal-veilige-gemeente-begint-niet-bij-de-burgemeester/.

Publication details

The Cybersecurity Assessment Netherlands 2023 (CSAN 2023) provides insight into the digital threat, the interests that may be affected by this threat, digital resilience and finally digital risks. CSAN 2023 is also intended to provide insight into the possible changes to the strategic themes that were elaborated in CSAN 2022. These themes formed a substantive basis for the Dutch Cybersecurity Strategy 2022-2028. This CSAN in turn forms a substantive basis for the evaluation of the action plan that is derived from this strategy. It focuses on national security.

The CSAN was drawn up by the National Coordinator for Counterterrorism and Security (NCTV). It involved close cooperation with the National Cybersecurity Centre (NCSC). The CSAN is adopted annually by the NCTV.

The NCTV together with partners from the security domain contributes to a safe and stable Netherlands by recognising threats and strengthening the resilience and protection of national security interests. The purpose is to prevent and limit social disruption. Ever since the formation of the NCTV, there has been one organisation within the Central Government responsible for counterterrorism, cybersecurity, national security and crisis control.

The NCSC is the central information hub and expertise centre for cybersecurity in the Netherlands. The NCSC contributes to increasing the digital resilience of Dutch society, specifically the digital resilience of the Central Government and vital providers.

Publication
National Coordinator for Security
and Counterterrorism (NCTV)
PO Box 20301, 2500 EH The Hague
Turfmarkt 147, 2511 DP The Hague,
The Netherlands
+31 (0)70 751 5050

More information
www.nctv.nl csbn
@nctv.minjenv.nl
@nctv_nl

July 2023