National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

The Critical National Infrastructure Threat Landscape

Understanding the accumulation of increasing and changing threats



Cover photo: *The Oosterschelde storm surge barrier (Oosterscheldekering) protects the Netherlands during high tides. System failures can have serious consequences.*

Contents

Summary 4

1. Introduction 7

2. Conceptual model for threats, national security interests and resilience of critical infrastructure 10

3. Deliberate threats to critical infrastructure 15

3.1 State actors pose a growing threat to critical infrastructure 15

3.1.1 The sabotage of critical infrastructure by state actors 15

3.1.2 Pre-positioning of critical infrastructure by state actors 17

3.1.3 Cyberattacks by state actors and hacktivists 18

3.1.4 Disinformation 19

3.1.5 Economic pressure and strategic dependencies 19

3.2 Terrorism and violent extremism: a potential threat to critical infrastructure 22

3.3 Activists also target critical infrastructure 23

3.4 Criminal activity: a potential threat to critical infrastructure 24

4. Natural threats to critical infrastructure 27

4.1 Climate change poses a growing threat to critical infrastructure 27

4.1.1 Extreme weather as a consequence of climate change 27

4.1.2 Sea level rise due to climate change 29

4.2 Earthquakes 29

4.3 Threat to critical infrastructure posed by space weather 29

4.4 Threat to critical infrastructure posed by infectious diseases 30

5. Threats arising from the failure of critical processes themselves 32

5.1 Human and system failures 32

5.2 Chain effects 33

6. Political, economic, social and technological factors 36

6.1 Increasing dependency on digital systems 36

6.2 Technological developments 37

6.3 Energy transition 37

6.4 Shortages on the labour market 38

6.5 Economic developments 38

7. Conclusion 40

Sources 41

Summary

The Netherlands' critical infrastructure faces an accumulation of diverse, increasing and changing threats. These threats, which include geopolitical tensions, climate change and human and system failures, can lead to the disruption or failure of critical processes which, in turn, may pose a threat to the continuity of these processes and therefore to national security.

This first ever threat landscape report provides an overview of the main threats to critical infrastructure and an insight into recent developments in relation to those threats. It is intended to provide government departments and critical providers with a conceptual model that can, in the context of specific critical processes, help them gain a better understanding of the threats, the level of resilience, the security interests affected in the event of disruption or failure and the resulting risks to national security. This threat landscape report can therefore be used by government departments and critical providers as a starting point for making risk and resilience analyses for the various critical processes that will be performed as part of the critical cycle and for the purpose of the Critical Entities Resilience Act (*Wet weerbaarheid kritieke entiteiten*, Wwke).

Conceptual model for threats, national security interests and resilience of critical infrastructure

- A proper assessment of the risks to critical processes, and therefore to national security, requires insight into three aspects, namely the threats faced by a critical process, the resilience of critical processes and the extent to which national security interests are affected. Risks to national security exist when a critical process is faced by certain threats, is insufficiently resilient to those threats and when disruption to or failure of a critical process results in one or more national security interests being compromised.
- A threat is the likelihood of an intentional or unintentional event occurring that could lead to the disruption or failure of critical processes or affect their integrity and confidential nature, with one or more national security interests being compromised. This threat landscape report distinguishes three types of threats to critical infrastructure, namely deliberate threats, natural threats and threats arising from the failure of critical processes themselves.
- The six national security interests are territorial, physical, economic and environmental security, social and political stability and the international rule of law and stability. Although the continuity of critical processes is an element of economic security, the disruption or failure of a critical process can impact all national security interests.
- Resilience is society's ability to be prepared for, resist, absorb and/or rebalance social (and ecological) disruption. The resilience of critical processes is determined by the policies of critical providers, government policies and the strengths and vulnerabilities of the Netherlands and its critical infrastructure.

Deliberate threats to critical infrastructure

- Critical processes may face deliberate threats from, among others, state actors, terrorism and violent extremism, activism and criminal activities which may lead to disruption or failure. Such threats can also put pressure on the integrity and confidentiality of critical processes, for instance in the case of espionage and pre-positioning for sabotage.
  - **State actors** also pose an increasing threat to critical infrastructure. Wars, geopolitical tensions and growing competition between major powers have made the world around the Netherlands and the European Union more unstable. Russia and China, in particular, pose a threat to Dutch critical infrastructure in various ways. This threat is apparent in, among other things, an increase in the use of hybrid tools, such as sabotage, espionage and pre-positioning, cyberattacks, disinformation, economic pressure and the abuse of strategic dependencies.
  - Critical infrastructure can be an attractive target for **sabotage** by state actors. It may be sabotaged not only to cause social disruption, but also to put pressure on countries, undermine the autonomy of other countries, or test how countries and NATO respond to acts of sabotage. There have been no recent examples in the Netherlands of successful physical sabotage of critical infrastructure by state actors. However, several incidents at European level show that critical infrastructure is vulnerable to hybrid attacks and that actors are also actually prepared to resort to sabotage. For example, Western countries hold Russia responsible for carrying out, or attempting to carry out, attacks and sabotage in several places in Europe in recent years. In some cases, sub-processes of critical sectors were also targeted and there have also been several incidents involving underwater infrastructure in European waters in recent years. In addition, aviation and shipping have been affected recently by a significant increase in the jamming and spoofing of GPS signals.
  - State actors may also carry out acts to prepare for sabotage, or may attempt to acquire a position in other countries' critical

infrastructure without (directly) engaging in sabotage. Sometimes the purpose of **espionage and pre-positioning** is still to have the capability to sabotage critical infrastructure at a later date, to put pressure on other countries, or to undermine the autonomy of certain countries. Russia, for example, is identifying critical maritime infrastructure in the Dutch part of the North Sea and is undertaking activities that are conducive to espionage and preparatory acts of disruption and sabotage.

- State actors also use **cyberattacks** to achieve their political, military and/or economic goals. There have been various examples in Europe and the US which demonstrate how China, Russia and Iran and others are able to carry out cyberattacks on Western governments and critical providers. Although cyberattacks on critical infrastructure in the Netherlands have not had a disruptive impact on national security to date, they are a daily occurrence. Among other things, state actors use them to gain access to critical processes so that they can, for example, disrupt them at a later date. They may also use cyberattacks to carry out espionage and for financial gain. In practice, there is a mix of state actors and hacktivists that engage in cyberattacks for ideological reasons.
- While little is known about the impact of **disinformation** on the functioning of critical infrastructure, it is still a hybrid threat that can affect critical providers and processes.
- In times of increasing competition between superpowers, state actors are attempting to use **economic pressure and strategic dependencies** to exert influence. They do so, for example, by means of trade-restricting measures, or by abusing the presence of foreign companies in Dutch critical infrastructure or strategic dependencies. Strategic dependencies can also pose a threat to the continuity of critical processes when supplies are interrupted by conflict elsewhere in the world, or because the dependency limits the Netherlands' open strategic autonomy. Strategic dependencies not only exist with respect to countries, but also one or a number of (tech) companies.

- **Terrorists and violent extremists** can also pose a threat to critical infrastructure. There have been no disruptive terrorist or extremist attacks on critical infrastructure in the Netherlands. However, accelerationist publications and foreign examples do show that critical processes can be targeted by terrorists and violent extremists. What is more, critical providers may have to deal with employees with extremist views, such as sovereigntists and right-wing extremists.
- Various protests and **activist campaigns** in the Netherlands and Europe in recent years have shown that critical sectors can be targeted or affected by activists and demonstrators. Several activities in recent years have caused short-term disruption to critical infrastructure such as airports, road infrastructure and a system of locks. National security interests were not compromised in the process.
- Critical infrastructure can also be threatened by **criminal activity**. These often take the form of cyberattacks by criminals, but may also involve subversive crime or physical acts. The actions of cybercriminals are motivated by financial gain and are not (primarily) intended to disrupt society. Although criminal cyberattacks have not caused social disruption in the Netherlands in recent years, several incidents do show how critical sectors can be affected by them.

Natural threats to critical infrastructure

- Critical processes may also be affected by a variety of natural threats. One increasing threat to critical infrastructure is, in particular, the impact of **climate change**, which is accelerating and becoming more severe than previously thought.
- Climate change will substantially increase the water-related challenges facing the Netherlands. Shortages of freshwater will increase during the summer, there will be more flooding due to rainstorms and the effects of that flooding will become more severe. Flooding can be disruptive when critical networks cease to function. In recent years, extreme precipitation in several European countries led to, among other things, power cuts, public transport shutdowns and airport closures. Climate change also causes both extreme heat and drought in the summer. Prolonged drought can put pressure on critical processes such as drinking water supply and inland shipping. Wildfires are also becoming more prevalent and they will more frequently result in damage and the failure of critical infrastructure.
- Sea levels around the world are rising more quickly as a consequence of accelerating climate change. The rise in sea levels in the Netherlands will mainly affect water safety and the availability of freshwater.
- There are no known recent incidents involving the disruption or failure of critical processes due to an earthquake in the Netherlands.
- Some critical processes use advanced technologies that may be vulnerable to **space weather**, such as solar flares, coronal mass ejections and proton storms. Space weather can, for example, temporarily disrupt communications and navigation or damage satellites.

Threats arising from the failure of critical processes themselves

- National security can also be compromised when critical processes fail due to human error, system failure or chain effects.
- **Human failure** involves failure or disruption of a critical process due to inadvertent human error. **System failure** is the result of a technical fault in the system itself. Several examples, such as the outages that affected CrowdStrike and the Netherlands Armed Forces Integrated Network (NAFIN), show that a seemingly minor technical or human error can have major consequences for critical processes and, in extreme cases, can even pose a threat to national security.
- The interdependencies within critical national infrastructure mean that a disruption to a single critical process can result in

chain reactions that impact other critical processes. The complexity of systems, increasing dependencies between systems and processes and the many mutual and hidden dependencies make it difficult to estimate the chain effects of a disruption to critical processes properly. Critical processes are also connected to all kinds of non-critical processes. Consequently, disruptions to these non-critical processes can also have major chain effects on critical ones.

Political, economic, social and technological factors

- Various political, economic, social and technological factors influence the critical infrastructure itself, as well as the threats to it, and its resilience.
- Key developments include the increasing dependency of critical processes on complex digital systems. Technological developments, such as artificial intelligence and space and quantum technology, are also influencing the security environment of critical processes. The energy transition is also having an effect on critical infrastructure and shortages on the labour market mean that critical providers cannot recruit sufficient staff and that makes them less resilient to threats. Finally, global economic developments can also affect critical processes.

1. Introduction

Dutch society is highly dependent on critical processes such as electricity, Internet access, drinking water and payment transactions. These processes are critical because disruption or failure can have major consequences for the functioning of the economy and society in the Netherlands and in Europe as a whole and that, in turn, may pose a threat to national security.[1]

Critical infrastructure faces an accumulation of diverse and increasing threats. Geopolitical tensions are an increasing threat to our critical infrastructure. Wars and competition between superpowers such as Russia and China mean the Netherlands is a target of hybrid attacks. By this we mean the deployment of a mix of civilian and military instruments to achieve certain strategic objectives, without resorting to armed conflict. Hybrid instruments are deployed by both state actors and non-state actors that collaborate with a state.[2] Such attacks can take the form of, for example, physical and digital espionage and sabotage, disinformation and economic destabilisation. Geopolitical developments could, for instance, lead to disruptions in supply chains, which could have a major impact on critical infrastructure.

The effects of climate change are also a growing threat to critical infrastructure, with global warming increasing the likelihood of weather events such as extreme heat, drought and precipitation. Such extreme weather events can then lead to disruptions or failures of critical processes such as energy supply, water management and transport. Although the exact consequences of climate change are difficult to predict, it is clear that the combination of different climate trends poses an increasing threat to sometimes vulnerable critical processes.

Several recent incidents, such as the CrowdStrike outage in July 2024[1], show that human error, system failure and chain effects can also disrupt critical processes. Finally, various political, economic, social and technological factors influence the threats to, and resilience of, critical infrastructure. For instance, increasing dependency on digital systems, shortages on the labour market and fragmentation of the global economy make critical infrastructure less resilient to threats, while technological developments may reinforce existing threats.

Critical processes, infrastructure and providers

The central government's 'Policy Approach to Critical Infrastructure' (*Aanpak Vitaal*) refers to protecting critical processes. Examples include 'control and management of water quantity', 'Internet and data services' or 'over-the-counter payment transactions'. A critical process is one whose failure, disruption or manipulation could lead to such serious effects that it could damage national security and therefore cause social disruption. It is up to each government department to assess which processes are critical within their policy domain. The Critical Entities Resilience Act talks about ensuring the continuity of essential services within the European Union. An essential service is one that is crucially important for the maintenance of critical social functions, economic activities, public health and safety or the environment. These essential services can be seen and designated as critical processes which together constitute the critical infrastructure of the Netherlands.[3]

One or more organisations within a critical process, such as private companies, public organisations, autonomous administrative authorities and parts of the central government are important for the continuity and resilience of the process. These organisations are referred to as critical providers. An overview of all critical processes, a detailed explanation of the central government's Approach to Critical Infrastructure and the definitions used in it can be found on the website of the National Coordinator for Counterterrorism and Security (Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCTV).

Purpose and scope of the threat landscape report

This first critical infrastructure threat landscape report provides an overview of the main threats to critical infrastructure and insight into recent developments regarding those threats. It provides a basis for testing in the coming years whether events fit within, or differ from, the threats described in this threat landscape report. This threat landscape report can therefore be seen as a reference point.

In addition to understanding threats, an understanding of resilience and the extent to which national security interests are affected is needed in order to obtain a proper picture of the risks to critical processes (see chapter 2 for an explanation of these interests). This threat landscape report only briefly discusses

1 This was an incident whereby a faulty update of CrowdStrike's software led to outages and disruption of critical processes in several countries. See also Paragraph 5.1.

resilience and national security concerns. The broad scope of critical infrastructure means only limited insight into these aspects can be given, based on public sources.

It is intended to provide government departments and critical providers with a conceptual model that can, in the context of specific critical processes, help them gain a better understanding of the threats, the level of resilience, the security interests affected in the event of disruption or failure and the resulting risks to national security.

This threat landscape report can therefore be used by government departments and critical providers as a point of departure for making risk and resilience analyses for the various critical processes involved in the critical cycle and for the purpose of the Critical Entities Resilience Act. The critical infrastructure consists of a large number of diverse critical processes and providers which, in turn, face a wide range of (potential) threats. The threats described in this threat landscape report are relevant to most critical processes. However, it is impossible to provide a detailed comprehensive overview here of all conceivable threats to all critical processes and providers because the threats that all individual critical processes and providers may face are too wide-ranging, too diverse and sometimes too specific to one critical process.

This threat landscape report is based solely on public sources and aligns as much as possible with existing threat products, such as the State Actors Threat Assessment (*Dreigingsbeeld Statelijke Actoren*), the National Cybersecurity Assessment (*Cybersecuritybeeld Nederland*), the Terrorist Threat Assessment for the Netherlands (*Dreigingsbeeld Terrorisme Nederland*), the National Risk Assessment of the Kingdom of the Netherlands (*Rijksbrede Risicoanalyse Nationale Veiligheid*), the National Security Trend Analysis 2024 (*Trendanalyse Nationale Veiligheid 2024*), the Military and Hybrid Threats Assessment (*Dreigingsbeeld militaire en hybride dreigingen*), the annual reports of the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*, AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen en Veiligheidsdienst*, MIVD) and the Delta Scenarios (Deltascenario's). Based on existing insights, the findings of this threat landscape report are translated explicitly to the critical infrastructure wherever possible.

Document structure

This threat landscape report begins in Chapter 2 with an explanation of the triad of threats, national security interests and the resilience of critical infrastructure. Chapter 3 provides an overview of the main deliberate threats to critical infrastructure and addresses threats from state actors, terrorism, activism and criminal activities. Chapter 4 deals with natural threats to critical infrastructure, including the effects of climate change, space weather, infectious diseases and earthquakes. Chapter 5 deals with the failure of critical processes themselves and the chain effects that can arise from this. Chapter 6 describes the main political, economic, social and technological factors which affect threats, resilience and the critical infrastructure itself.



Numerous dams, like this one at Borgharen, which is able to process large quantities of water when water levels rise in the Maas river, protect towns and cities in the Netherlands during periods of high water.

2. Conceptual model for threats, national security interests and resilience of critical infrastructure

A proper assessment of the risks to critical processes, and therefore to national security, requires insight into three aspects, namely the threats facing a critical process, the resilience of critical processes and the extent to which national security interests are affected. Risks to national security exist when a critical process is faced by certain threats, is insufficiently resilient to those threats and when disruption to or failure of a critical process results in one or more national security interests being compromised. These risks may also exist without causing actual incidents, for example because the critical infrastructure is highly resilient to a particular threat.

Rising sea levels, for example, would pose a major threat of large-scale flooding if no resilience-enhancing measures were taken. After all, the Netherlands is 26% below sea level and about 60% of the country is prone to flooding.[4] Any large-scale flood would be a risk to various national security interests. However, thanks to dyke reinforcements, storm surge barriers, sand replenishment and pumps to ensure water safety, the Netherlands is resilient to (probably) a 3 metre rise in sea levels and the risk of any resulting flooding is therefore minor.[5]

The triad of threats, interests that need protecting and resilience are the point of departure for analyses relating to national security (see Figure 1).

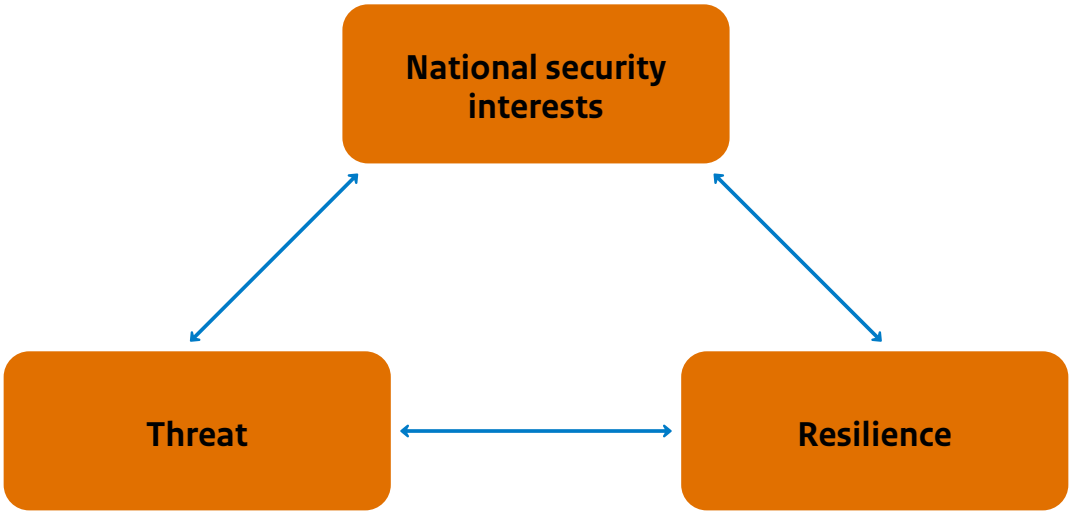


Figure 1: The general triad of threat, national security interests and resilience.

The general 'triad' has been developed in more detail for this threat landscape report on critical infrastructure by defining threats and resilience more specifically and by adding risks as well as political, economic, social and technological factors (see Figure 2).

Threats

A threat is the likelihood of an intentional or unintentional event occurring that could lead to the disruption or failure of critical processes or affect their integrity and confidential nature, with one or more national security interests being compromised.[2] In line with the National Risk Assessment of the Kingdom of the Netherlands (*Rijksbrede Risicoanalyse Nationale Veiligheid*), this threat landscape report distinguishes between three types of threats to critical infrastructure, namely deliberate threats, natural threats and threats arising from the failure of critical processes themselves.[6]

Critical infrastructure is an attractive target for malicious parties, such as state actors. This is pnd outages, or the compromising of the integrity and confidentiality of critical processes.[7] This threat landscape report contains several examples of how critical infrastructure can be vulnerable. Sometimes it takes very little to disrupt critical processes such as energy, telecommunications, the transport sector and the supply of drinking water.[8] Natural phenomena, such as extreme weather and natural disasters, can also disrupt critical processes.[9] Climate change means extreme weather events are becoming more frequent and critical infrastructure is increasingly likely to be disrupted by natural causes.[10] Finally, human or system failures can also lead to the disruption or failure of critical infrastructure.[11]

As critical processes face an accumulation of diverse threats, multiple threats may occur simultaneously, thereby increasing the risk of the disruption or failure of critical processes. For example, a single-incident cyberattack can generally be mitigated. This will be more difficult, however, when an attack is combined with another event. This would apply, for example, in the event of an attack on rail transport operators during major track maintenance, or an attack on water authorities during a major storm.[12]

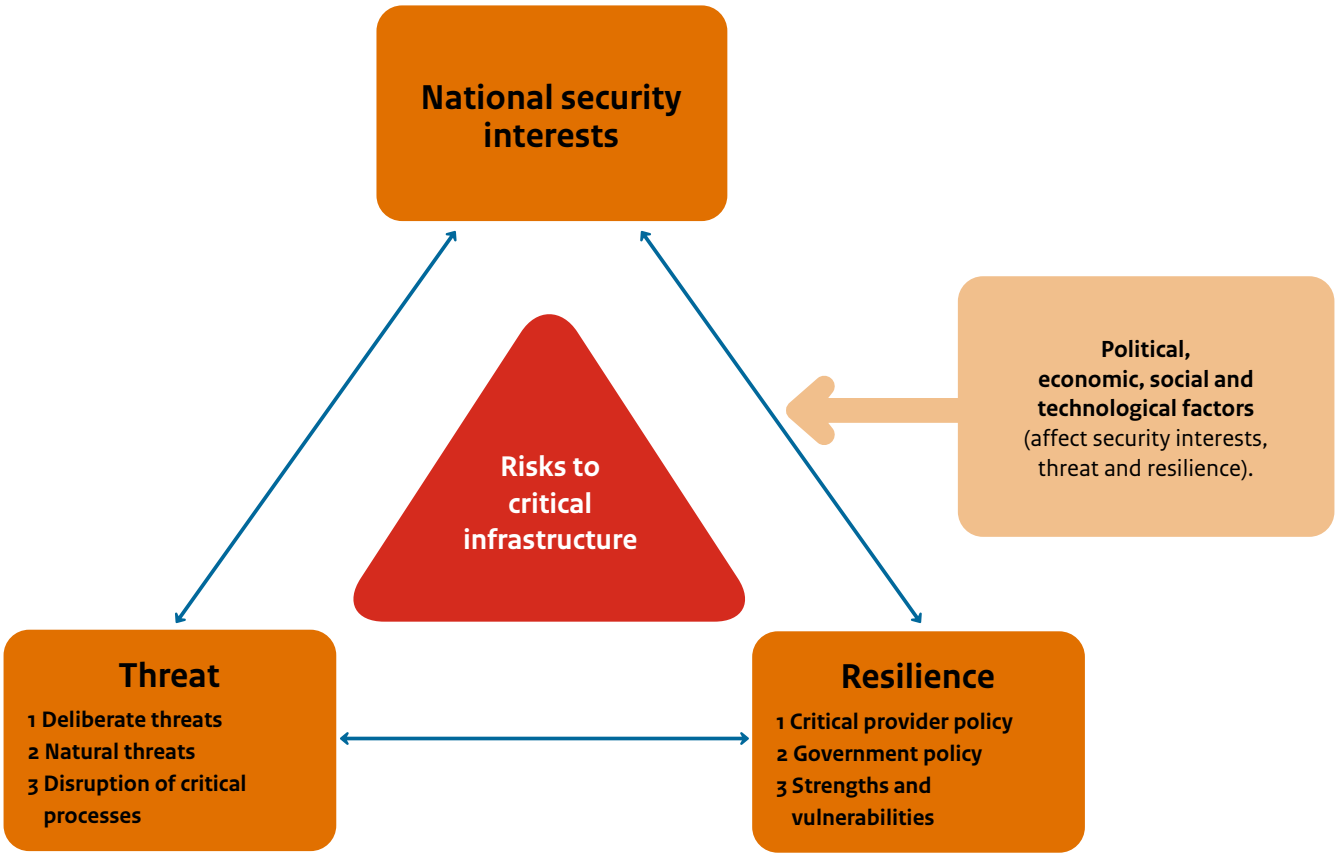


Figure 2: The triad of threat, national security interests and resilience of the critical infrastructure.

2 Slightly different definitions for threats are sometimes used in various other studies and analyses. This is the definition used in this threat landscape report, specifically for critical infrastructure.

A disruption of a critical process can be 'self-contained', in which case it does not affect other critical processes. Since a key feature of critical infrastructure is that critical processes are interdependent, chain effects (also known as cascading effects) may also occur, causing multiple processes to be affected.[13] In the event of a flood, for example, power outages could impact parts of the Internet or the functioning of hospitals.[14]

National security interests

Critical processes and providers have to deal with numerous threats. However, a threat to national security only exists when one or more national security interests are affected. The six national security interests are:

1. *Territorial security*: This includes the integrity of Dutch territory, the integrity of digital space (IT networks and information systems) and the integrity of allied territory.
2. *Physical security*: This covers the undisturbed functioning of individuals, which may be compromised, for example, by accidents, attacks, diseases or a lack of basic necessities.
3. *Economic security*: This covers the undisturbed functioning of the Netherlands as an effective and efficient economy and includes ensuring the continuity of critical processes, mitigating risky strategic dependencies and preventing the unwanted transfer of knowledge and technology.
4. *Ecological security*: This includes the unimpeded continued existence of the natural living environment in and around the Netherlands. This can be compromised when nature and the environment are affected over a long period of time.
5. *Social and political stability*: This covers the continued and unimpeded existence of a social climate in which individuals are free to go about their lives and groups are able to coexist within, and in accordance with, the democratic rule of law of the Netherlands and its shared values.
6. *International rule of law and stability*: This covers the proper functioning of the international system of standards and agreements aimed at promoting international peace and security.[15]

A detailed explanation of national security interests can be found in the National Risk Assessment Guidelines (*Leidraad Risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid*).

Although the continuity of critical processes is an element of economic security, the disruption or failure of a critical process can impact all national security interests.[16] For example, a major and prolonged outage in the power supply and/or digital infrastructure could not only affect economic security, but also lead to social unrest. Physical security may also be compromised if, for example, hospitals are no longer able to provide essential care.

Resilience

Various definitions of resilience exist. Research organisation RAND examined the different ways in which the concept of resilience is used and interpreted in Dutch national security policy documents. Based on this, it drew up a working definition of resilience in the context of national security. It reads: *'society's ability to be prepared for, resist, absorb and/or achieve a new state of equilibrium after a disruption'*.[17] While disruptions to, or the failure of, critical processes whereby one or more national security interests are compromised will often lead to social disruption, in the context of critical infrastructure it is also possible for ecological disruption to occur, without major effects on society. This may be the case, for example, when a failure or disruption of a critical process causes large-scale and long-term damage to nature or the environment, without affecting people (on a large scale).

The RAND definition is largely in line with the definition of resilience in the Critical Entities Resilience Act[3], which defines resilience as *the ability of a critical entity to prevent, mitigate and manage an incident, and to protect and resist, respond to or, adapt to and recover from an incident.18*

In this threat landscape report we assume that the resilience of critical processes and the critical infrastructure as a whole is determined by three aspects:

1. *The set of policy instruments of critical providers* aimed at preventing and mitigating threats. The majority of critical processes are in the hands of private parties. They are primarily responsible for the continuity and resilience of critical processes and take appropriate measures to protect them from threats. The resilience of critical processes is partly determined by the extent to which critical providers are prepared for, can withstand, absorb and/or rebalance disruption. These include cybersecurity measures to resist digital attacks, staff screening to prevent insider threats or adapting infrastructure and equipment to changing climate conditions.
2. *The government's set of policy instruments.* Government departments draw up frameworks for the sectors under their responsibility. This covers things like sectoral policies, legislation and regulations. The National Coordinator for Counterterrorism and Security (*Nationaal Coördinator Terrorismebestrijding en Veiligheid*, NCTV) fulfils a coordinating role when it comes to protecting critical infrastructure. This involves the cross-sectoral approach such as drafting general policies, legislation and regulations and developing resilience-enhancing tools such as the Critical Cycle. The resilience of critical processes is partly determined by the extent to which public policies prepare critical providers and society to withstand, absorb and/or rebalance the effects of disruption. A detailed explanation of all government organisations involved and their roles and responsibilities can be found on the website of the NCTV.

3 The Wwke is the national legislation which implements the European Critical Entities Resilience (CER) Directive and focuses on protecting critical entities from all natural and man-made risks.

3. *Strengths and vulnerabilities* of the Netherlands and its critical infrastructure. This covers issues such as geographical, spatial, social and economic characteristics that affect the extent to which critical processes are susceptible to threats. For example, the Netherlands has a small and open economy which is orientated towards international trade. As a result the economy is vulnerable to international (economic) developments that could, for instance, affect the financial position or supply chains of critical providers.[19] In addition, the Netherlands' geographical location as a gateway to Europe and its role as a logistics hub within NATO makes its critical infrastructure vulnerable to hybrid attacks.[20] On top of that, the fact that the Netherlands is a low-lying and also densely populated river delta, where the major European rivers of the Rhine, Meuse and Scheldt flow into the sea, makes the country and elements of its critical infrastructure vulnerable to flooding (if no resilience-enhancing measures are taken).[21]

A proper understanding of the resilience of individual critical processes and the critical infrastructure as a whole therefore requires insight into the effectiveness of the set of policy instruments used by critical providers and the government, and the strengths and weaknesses that affect the critical infrastructure's susceptibility to threats. Because it is too extensive and complex to formulate this for the entire critical infrastructure and because it will also be part of the resilience analyses that the government departments are going to conduct as part of the Critical Cycle, this falls outside the scope of this threat landscape report.

Political, economic, social and technological factors

The critical infrastructure itself, its resilience and the threats facing critical processes are additionally influenced by various political, economic, social and technological (PEST) factors. These factors can amplify or diminish threats, or make critical infrastructure more susceptible or indeed more resilient to the threats. Examples include technological developments such as AI that amplify existing threats, or shortages on the labour market that make critical providers less resilient due to shortages of technical staff.



The North Sea is home to critical infrastructures such as Internet cables and gas pipelines. The Coast Guard monitors suspicious activity at sea so that sabotage can be detected as soon as possible.

3. Deliberate threats to critical infrastructure

Critical processes may also be affected by a variety of deliberate threats. The discussion below focuses on threats from state actors, terrorism and violent extremism, activism and criminal activities. In particular, hybrid attacks by state actors or their proxies pose a growing threat to critical processes which may not only lead to disruption or outages, but may also compromise the integrity and confidentiality of critical processes. This applies, for example, in the case of espionage and pre-positioning for sabotage.

In some instances malicious actors deliberately target a specific part of the critical infrastructure. However, actors such as states and criminals also regularly act on an opportunistic basis. This means they look at how best to achieve their goals and focus their activities, such as cyberattacks, on a wide range of systems and (critical) infrastructure that the attackers themselves have no specific knowledge of. Critical processes can fall victim to these activities in such an instance especially when they have a low level of resistance.

3.1 State actors pose a growing threat to critical infrastructure

Wars, geopolitical tensions and growing competition between major powers have made the world surrounding the Netherlands and the European Union more unstable and this has led to a rapid deterioration in the European security situation.[22] Russia and China, in particular, pose a threat to Dutch critical infrastructure in various ways.[23]

Russia is seeking confrontation with the West and is using a wide arsenal of means to harm Western countries and improve its own position.[24] One way it is doing this is through physical and digital sabotage, gathering information about our critical infrastructure and spreading disinformation.[25] China also aspires to playing a leading role in the world and, in the process, is challenging the existing world order. It is using a variety of means to increase its influence, including espionage, economic investment, technological development and changing international institutions to its own advantage. Chinese ambitions have implications for the Netherlands, such as economic dependency and advanced cyberattacks.[26] Russia and China are also cooperating economically, politically and militarily. For example, China is directly and indirectly contributing to sustaining Russia's war effort in Ukraine.[27]

The increasingly fierce competition between superpowers is evident in, among other things, an increase in the use of hybrid instruments.[28] This keeps them below the threshold of armed conflict, but still enables them potentially to harm Dutch critical infrastructure and national security.[29]

This section describes the following hybrid threats by state actors to critical infrastructure: sabotage, espionage and pre-positioning, cyberattacks, disinformation, economic pressure and abuse of strategic dependencies.

A military conflict is usually preceded by such hybrid threats.[30] For the first time in a long while, the collective defence clause in the NATO treaty (Article 5) means there is a real possibility of the Netherlands becoming directly involved in a large-scale armed conflict. That conflict does not have to take place in the Netherlands but Dutch critical infrastructure could also become a target if the Netherlands becomes involved in an armed conflict in another NATO member state, or if that armed conflict takes place near the Netherlands.[31] Russia's actions in, and aggression towards, Ukraine pose the biggest threat in this regard. This is because Russia's armed forces are being reformed in a way that is aimed at a future conflict with NATO and Russia is continuing to escalate the situation between the two. This dynamic means there is a risk of an unwanted escalation.[32]

3.1.1 The sabotage of critical infrastructure by state actors

Critical infrastructure can be an attractive target for sabotage by state actors.[33] The Netherlands is a digital and physical hub and gateway to Europe. Partly because of this, Dutch critical infrastructure is, in principle, an interesting target for sabotage, with the aim being, for example, to disrupt logistic support to

Ukraine or the supply of military troops to Eastern Europe.[34] Dutch critical infrastructure may be sabotaged not only to cause social disruption, but also to put pressure on countries, undermine the autonomy of other countries, or test how countries and NATO respond to acts of sabotage.

There have been no recent examples in the Netherlands of successful physical sabotage of critical infrastructure that can be unambiguously linked to state actors.[35] However, several European incidents show that critical infrastructure is vulnerable to hybrid attacks and that actors are also actually prepared to resort to sabotage. In addition, the sabotage of European allies' critical infrastructure can also have an impact on Dutch national security due to chain dependencies.[36]

Three developments are highlighted below that provide insight into the current threat of sabotage of critical infrastructure by state actors:

1. The increase in Russian acts of sabotage in Europe.
2. Recent acts of sabotage which targeted underwater infrastructure.
3. The increase in deliberate jamming of GNSS signals.

Increase in Russian acts of sabotage in Europe

Western countries hold Russia responsible for carrying out, or attempting to carry out, attacks and sabotage in several places in Europe in recent years. In some cases, sub-processes of critical sectors were also targeted. Sometimes the country uses proxies to disguise its own involvement.[37] Leiden University research shows a sharp increase in 2024 of Russian acts of sabotage which targeted European countries.[38] According to the Strategic Monitor 2025 by The Hague Centre for Strategic Studies (HCSS), the number of Russian hybrid attacks on Europe more than doubled in 2024 compared to the previous year[4].[39] These acts of sabotage have multiple purposes. On the one hand, the aim is to delay Western supplies to Ukraine while, on the other, it is to sow division and instil fear in the West. In addition, acts of sabotage allow Russia to test where the West draws its red lines when it comes to Russian aggression on its own territory.

In April 2024, for example, two German-Russian nationals, who were planning to attack military and industrial infrastructure on behalf of Russia using explosives and arson, were arrested in Germany.[40] According to the German federal prosecutor, one of them wanted to attack, among other things, railways used to transport military supplies.[41] That same month, two men were charged in the UK for setting fire to a warehouse containing relief supplies for Ukraine. British prosecutors have accused them of working for the Russian government.[42] In 2024 there were several incidents involving parcels containing explosives at air cargo transfer points in Poland, Germany and the UK. According to various Western intelligence agencies, the Russian military intelligence service (GRU) was behind them.[43]

In any event, at least one person was also targeted by Russian actions. In July 2024 it was revealed that US intelligence agencies had uncovered Russian plans to assassinate the CEO of German arms manufacturer Rheinmetall.[44]

Russia has tried to disrupt the signalling systems of Czech railways several times in the Czech Republic.[45] In the Netherlands too, the sabotage of physical infrastructure such as ports and railways is a real threat. The ports of Rotterdam, Vlissingen and Eemshaven are used to move military personnel and equipment for NATO's so-called 'Host Nation Support'.[46] Military equipment loaded at those ports is then sent into Europe by rail and road. This alone makes the Netherlands a possible military-logistics target. If NATO goes to war on Europe's eastern flank this risk will only increase.[47]

Recent acts of sabotage targeting underwater infrastructure

Several incidents involving underwater infrastructure in European waters have occurred in recent years. The significant increase in the amount of underwater infrastructure and the growing dependency on it has made it a more attractive target for malicious actors.[48] Internet cables, for example, enable global connectivity and the network in Europe is essential for financial transactions.[49] However, because much of this infrastructure lies on the seabed outside territorial waters, it is difficult to protect and monitor. The fact that it can be approached covertly makes underwater infrastructure an attractive target for hybrid conflict. Malicious actors can cause substantial damage by disrupting it, without any great risk to themselves. Sometimes it is difficult to establish who the perpetrators are and determine whether what happened was indeed a case of deliberate sabotage.[50] This is because failures in underwater cables can also be inadvertently caused by fishing, ships' anchors or ground movements.[51]

The most important recent examples of incidents involving undersea communication cables, power links and pipelines involving or potentially involving sabotage are listed below. In January 2022, one of the two fibre-optic cables between Norway and the Svalbard archipelago was destroyed, limiting communications with the mainland.[52] In September 2022, three Nord Stream 1 and 2 pipelines (each consisting of two identical pipelines) were blown up at the bottom of the Baltic Sea. These pipelines supplied Europe with Russian gas. Three Ukrainian nationals are suspected in this act of sabotage.[53] In October 2022, several French and Scottish cables were simultaneously severed, thereby cutting off the Shetland Islands from the outside world and rendering three key French communication lines unusable.[54] In October 2023, a gas pipeline and a communications cable between Finland and Estonia were damaged.[55] According to Finland, this damage was deliberate and investigations by the Finnish authorities found that it was probably the result of a Chinese container ship dragging its anchor for more than 180 kilometres off

4 The HCSS report identified 24 examples of Russian hybrid activities for 2023 and 55 for 2024.

the Baltic seabed. It took six months to repair the damage. Thanks to new LNG infrastructure which was accelerated after 2022, Finland still had sufficient supplies of gas.[56] At the beginning of 2024, four major undersea Internet cables were destroyed in the Red Sea, possibly by Houthi militias.[57] In November 2024, two underwater cables were damaged in the Baltic Sea, probably by the Yi Peng 3 merchant ship. One cable runs between Sweden and Lithuania and the other between Germany and Finland.[58] In December 2024, the Estlink 2 power link and several data cables between Finland and Estonia failed. According to Finland, this was due to a Russian sabotage operation with the Eagle S, an oil tanker which Russia allegedly used for espionage and acts of sabotage.[59]

One example from January 2025 shows how undersea cables can also be unintentionally disrupted. During that month a fibre-optic cable at the bottom of the Baltic Sea between Sweden and Latvia was broken. Initially, Swedish police suspected that this was due to sabotage by the Russian shadow fleet. Further investigation revealed that there was no intent, but that a ship called the Vezhen had lowered its anchors due to heavy winds and then unintentionally pulled the cable until it broke.[60]

The increase in deliberate jamming of GNSS signals

Disrupting global navigation satellite system (GNSS) signals is another form of hybrid attack that poses a threat to critical infrastructure. There are four major GNSS systems used worldwide for time and positioning. The American GPS is the best known of these, alongside the European Galileo, Russian GLONASS and Chinese Beidou systems. Many critical processes, such as aviation, energy supplies and digital payments, rely on GNSS for their timing and positioning capabilities.[61] Aviation and shipping have been affected recently by a significant increase in primarily the jamming and spoofing of GPS signals.

GPS jamming involves the signal being completely disrupted, while spoofing means that the signal is deliberately overridden by another fake signal. [62] That is done by using a more powerful signal on the same frequency as the GPS signal.[63] Because they are transmitted from space, GNSS signals are not as strong and a small transmitter is all malicious actors need to significantly disrupt such a signal.[64]

Both the Dutch Civil Aviation Incident Analysis Department and the European Union Aviation Safety Agency (EASA) have reported more incidents of interference with aircraft GPS signals since 2023.[65] This interference occurs mainly over Eastern Europe and the Middle East.[66] There were about 600 reports of jamming and spoofing in 2023. Approximately 150 of these reports involved spoofing, while there were no reports of spoofing at all in the years 2018 to 2022.[67] The Aviation Occurrence Analysis Bureau received 1,318 reports about spoofing alone in 2024.[68]

When GPS signals are disrupted, aircraft have to fall back on other independent navigation systems.[69] Sometimes pilots who are, for example, flying from the direction of Russia have to ask for help from the control tower to determine their location because their GNSS navigation has not yet been rectified.[70] Shipping is also being affected by GNSS interference.[71] The Finnish Coast Guard, for example, reported in late 2024 that satellite navigation in the Baltic Sea has been increasingly disrupted since April that year, causing ships to get lost at sea. In a number of cases the Finnish coastguard had to intervene to prevent ships from getting too close to islands or shallow waters.[72]

GPS spoofing is an effective tool against, for example, drones, precision weapons systems and missile systems. A lot of incidents of GPS spoofing affecting civilian aircraft therefore take place (at the periphery of) conflict zones.[73] The GPSJAM website plots GPS interference on a daily basis. Its maps show that this interference is concentrated around the Baltic States, the Baltic Sea, Ukraine and the Middle East.[74] Besides localised jamming and spoofing, GNSS systems can also fail on a much larger scale. Several state actors possess anti-satellite or counterspace weapons and cyberweapons that they use to target satellite systems. Russia, China, Iran and North Korea have, for example, conducted operations against GPS in the past.[75]

The impact of large-scale and protracted GNSS system failures on critical infrastructure can be significant, as many critical processes depend on GNSS for precise determination of location and time. Accurate timing and positioning is, for example, essential for navigating (autonomous) road traffic, monitoring drinking water supplies, synchronising energy supplies, digital payment transactions and the proper operation of modern networks such as 5G.[76] However, the precise dependencies of critical processes on GNSS and the potential impact of a disruption are not entirely clear.[77]

3.1.2 Pre-positioning of critical infrastructure by state actors

State actors may also carry out acts to prepare for sabotage, or may attempt to acquire a position in other countries' critical infrastructure without (directly) engaging in sabotage. Sometimes the purpose of espionage and pre-positioning is to retain the capability to sabotage critical infrastructure at a later date. However, state actors can also use pre-positioning as a means of putting pressure on other countries and compromising their autonomy. Espionage may be an end in itself or precede pre-positioning or sabotage to gain a better picture of critical infrastructure and its vulnerabilities in advance. Given the complexity and interconnectedness of our critical infrastructure, it can be difficult to establish whether a state actor or its affiliated proxies are present in certain systems.[78]

Critical infrastructure in the North Sea is, for example, vulnerable to espionage and sabotage. On the bottom of the North Sea lie thousands of kilometres of data cables that are important for the Netherlands' connectivity. The North Sea is also home to

important gas pipelines and electricity cables used to supply energy and the North Sea itself and offshore wind farms are becoming increasingly important for the Netherlands' national energy needs and its energy transition.[79] In the coming years, the North Sea's critical infrastructure will be greatly expanded and this will increase our dependency on it.[80] In its 2023 annual report the MIVD described Russia's mapping of critical maritime infrastructure in the Dutch part of the North Sea, such as Internet cables, gas pipelines and wind farms, as well as activities which indicate espionage and preparatory acts of disruption and sabotage.[81]

3.1.3 Cyberattacks by state actors and hacktivists

State actors also use cyberattacks to achieve their political, military and/or economic goals. State cyberattacks are not isolated incidents but part of a broader toolkit. Several such attacks can be carried out at the same time or an attack may be combined with other, non-digital, resources from that toolkit.[82] Cyberattacks are attractive to perpetrators because they can be difficult to trace back to them and they can be carried out relatively cheaply compared to the damage they can cause.[83] For an overview of different types of cyberattacks, see the National Cybersecurity Assessment 2024 (*Cybersecuritybeeld Nederland 2024*).

Different cyberattacks have different intended outcomes. One of the reasons state actors may use them is to gain and maintain access to critical processes. They can then misuse that access at a later point in time, for example in the event of a conflict, to disrupt critical processes such as energy supplies or telecom networks.[84] In addition, state actors can also use cyberattacks against critical processes for espionage purposes, with the motivation being, for example, to gain access to the large amounts of data used within a particular sector. One example of this is state actors trying to steal data in the (European) travel and aviation sector in order to identify, track or follow individuals who are of interest to them.[85] Finally, cyberattacks on critical infrastructure can also be motivated by financial gain.[86]

Cyberattacks on critical infrastructure have not had a disruptive impact on national security in the Netherlands to date.[87] Nevertheless, sophisticated cyberattacks on Dutch critical infrastructure are commonplace.[88] The conclusion in the National Cybersecurity Assessment 2024 was that cyberattacks by state actors seem to be the new normal. Among others, Russia and China are intensifying their cyber activities and broadening their capabilities to include non-state actors. The Netherlands has also experienced the effects of cyberattacks which then spread throughout the digital ecosystem.[89] The National Cybersecurity Assessment also confirmed that these actors are increasingly attacking edge devices, such as firewalls, VPN servers and routers. Malicious parties use such systems on the periphery of a network as an access point to the underlying network and try, among other things, to insert a backdoor to maintain access.[90]

In addition to state actors, hacktivist cyberattacks have received a lot of attention in recent years. Hacktivists carry out cyberattacks for ideological reasons. Geopolitical tensions, conflicts and socially controversial topics can also give rise to hacktivism. For instance, while the war against Ukraine has been a trigger, the conflict between Israel and Hamas has also led to an increase in cyberattacks. Since the end of 2023, shortly after the outbreak of the conflict between Israel and Hamas, Microsoft noted an increase in the number of reports of attacks against Israeli-made operational technology (OT) systems. The decision to target these systems was probably based on a desire to highlight the use of such equipment, rather than any animosity towards the affected organisations themselves. One such cyberattack on a local drinking water supply which uses Israeli-made digital equipment left residents of an Irish village without water for two days in November 2023.[91]

In practice, state actors and hacktivists make up a mixed group.[92] In recent years, for example, 'hacktivist' collectives have been carrying out more and more Russian digital espionage, sabotage and influence activities. Sometimes these were so-called cover operations and sometimes they were actual hacktivist groups acting as an extension of the Russian state.[93]

Examples of cyberoperations by state actors and hacktivists

There have been various examples in Europe and the US which demonstrate how state actors like China, Russia and Iran are able to carry out cyberattacks on Western governments and critical providers.

Cyberattacks by Chinese actors

China has been using its cyber programmes for years to pre-position for possible sabotage and to perform actual sabotage, (economic and political) espionage and influencing operations which have targeted various Western countries.[94] The pace of cyberoperations on Western targets remains high and Chinese intelligence services are continually ramping up activities to attack Western targets.[95]

At the beginning of 2024, the MIVD reported the presence of malware called COATHANGER on a stand-alone Ministry of Defence computer network, which had fewer than 50 users. This malware came from a Chinese state actor. The discovered malware had installed a 'backdoor' by exploiting a known vulnerability in FortiGate devices. China uses this type of malware to spy on computer networks.[96] Because the malware had gained access to an isolated research network, the damage was limited. [97]

In 2023, the United States and Microsoft announced that hackers from China-linked Volt Typhoon had infiltrated America's critical infrastructure. The hackers in question had reportedly been active since mid 2021 and were preparing for digital sabotage.[98] According to US officials, China's aim is thought to be the exploitation of

access gained to US critical infrastructure in the event of war or conflict.[99]

In September 2024, it was revealed that another Chinese hacker group, known as Salt Typhoon, had been carrying out an extensive cyberespionage campaign against telecom providers for over two years. Its victims included at least eight US telecom providers and dozens of other countries. Although the hackers had wide access at the telecom organisations, they would have been mainly interested in prominent individuals. However, in order to get to those individuals, metadata of phone calls and text messages would have been stolen from a large number of Americans citizens.[100] According to reports in The Wall Street Journal, this hacker group had also gained access to US investigative agencies' wiretap systems.[101]

Cyberattacks by Russian actors

Several examples of cyberattacks by Russian state actors and pro-Russian hacktivists have also been made public in recent years. In September 2024, for example, the MIVD and its international partners, warned of Russian cyberoperations by GRU unit 29155. The focus of these Russian military secret service hackers includes gaining an insight into and disrupting Western aid to Ukraine. Their cyberoperations may also be aimed at supporting physical sabotage, with which this unit has long been associated. Their operations primarily target Western governments and critical infrastructure. It is a unit that the Netherlands must keep its eye on, partly because of its role as a major transit country. In other Western countries, the GRU unit did indeed engage in cyberoperations which targeted logistics sectors that provide, or have a role in providing, aid to Ukraine.[102]

In February 2022, just an hour before the Russian invasion of Ukraine, a large-scale cyberattack was carried out on US satellite company Viasat. The erasure of large quantities of data using wiper malware temporarily disrupted both communications on the Ukrainian side and satellite communications in several European countries.[103] In April 2024 in the Netherlands, the broadcast of children's channel BabyTV was also interrupted by a short transmission of some Russian propaganda. This signal hijacking, whereby a strong signal is sent to the satellite from an alternative station, was not aimed at BabyTV, but was collateral damage from a broader attack which was intended to disrupt broadcasts by Ukrainian TV stations.[104] These attacks were not isolated, but were part of a large-scale Russian cybercampaign as part of the war against Ukraine. A study by the Center for Security Studies identified 124 cyberoperations against the space sector during the war in Ukraine. These were all focused on space systems and companies on Earth and not on systems in space and most of them were Distributed Denial of Service (DDoS) attacks. The study additionally identified 35 actors, including hacktivists and state actors on both sides of the conflict, who carried out these cyberattacks.[105]

In June 2023, websites of Dutch ports were temporarily down due to DDoS attacks by a pro-Russian hacktivist group.[106] In August 2023, the websites of several Dutch airports were the target of DDoS attacks by pro-Russian hacktivists, but they only caused the website of Groningen Airport Eelde to go down temporarily.[107] In July 2024, hackers from hacktivist group the Cyber Army of Russia Reborn (CARR) were convicted in the US for cyberattacks on critical infrastructure, such as water infrastructure and energy companies.[108]

Cyberattacks by Iranian actors

Iran has proven it can also pose a digital threat to government organisations and critical providers through its attacks on Albania. These attacks must be seen in the specific geopolitical context of both countries. Tensions have been high between Iran and Albania for some time now. The examples are proof that Iran has relevant cyber capabilities and is willing to deploy them for its own geopolitical interests.

In 2022, Albania's government networks were the target of a cyberattack for which Albania and the US hold Iran responsible.[109] The attack took down several Albanian government websites and digital services and, according to the Albanian prime minister, could have brought down the entire country.[110] At the end of 2023, the Albanian parliament and telecom company One Albania became targets of cyberattacks. The exact scope and extent of the attacks are unknown. An Iran-linked hacker group called Homeland Justice claimed responsibility for the attacks through its Telegram channel. It also claimed to have hacked a second telecom company and the national airline, Air Albania.[111]

3.1.4 Disinformation

Disinformation is also a hybrid threat that can affect critical providers and processes. Disinformation is the deliberate spreading of misleading information, for example to influence opinions, make money or cause damage to Dutch society.[112] State actors spread disinformation, for example, during the COVID-19 pandemic, in relation to the war in Ukraine and in recent elections.[113] Although little is known about the actual impact of disinformation on the functioning of critical processes, critical providers have expressed concerns about the potential consequences, especially for their employees. At the end of 2024 the Dutch Central Bank warned in its report 'Resilience in turbulent times - Geopolitical risks and financial institutions', that financial institutions could also be confronted with the problem of disinformation, for example if malicious actors were to spread fake news about the financial position of banks in order to cause social disruption.[114]

3.1.5 Economic pressure and strategic dependencies

In times of increasing competition between superpowers, state actors are attempting to use economic dependencies to exert influence.[115] They do so, for example, by means of trade-restricting measures, or by abusing the presence of foreign companies in

Dutch critical infrastructure or strategic dependencies. These types of economic pressures can also affect the integrity and availability of critical processes, for instance when it is no longer possible to import essential raw materials, services and products. There is also a risk of no alternatives existing for some essential components (in the long run) from countries without opposing (geopolitical) interests.

State actors do not always need to adopt a deliberate strategy in order to become part of the Dutch critical infrastructure or to create strategic dependencies and take advantage of these. There may, for example, be an economic agreement which simultaneously enables foreign companies to gain a position in the critical infrastructure or supply chains of critical providers, which state actors can abuse (at a later date). This means, for example, that the presence of Chinese companies in the supply chains of critical processes can represent or become a threat to those processes. As a result, critical providers may, for example, become a target of opportunity of Chinese economic pressure, including abuse of strategic dependencies.

Economic pressure from China

Chinese companies are increasingly present in the European market, for example in the ecosystem of various critical sectors, such as ports and physical infrastructure, energy and telecoms. In times of increasing geopolitical tension China can use these companies to put pressure on Europe and the Netherlands for political and strategic purposes.[116]

Research by the European Parliamentary Research Service has revealed that China very regularly exerts economic pressure on other countries and companies for political purposes. China also exerts such economic pressure on the European Union. By putting pressure on prominent companies or sectors, Beijing attempts to deter others from crossing certain lines. Those red lines concern not only issues of sovereignty and national security, but also China's international image and the treatment of Chinese companies abroad.[117]

China often uses a combination of methods to exert economic pressure. Governments mainly face trade restrictions in the form of limitations on imports and (to a lesser extent) exports. Concrete measures used by China include raising customs tariffs, selectively applying domestic and international regulations, targeted customs controls, denying licences, or imposing unofficial embargoes. In addition, China passed a new export control law in 2020 that allows it to control exports of goods, technologies and services to protect its (vaguely defined) national security and interests.[118]

Researchers from the Merics think tank identified 123 instances of economic pressure being exerted by China between 2010 and 2022, with a marked increase in the last four years. According to the researchers, this is probably just the tip of the iceberg, as China often does not make the measures public, sometimes appears to make them deliberately difficult to detect, and companies themselves are also reluctant to report them for fear of reprisals from Chinese authorities and Chinese consumers. Companies in the consumer and agricultural goods, commodities and services sectors are the most frequent targets of Chinese economic pressure.[119] The best-known example of economic pressure from China is the import restrictions it imposed on Lithuania following the opening of a '*Taiwanese representative office*' in Vilnius in November 2021. China cut Lithuanian imports by almost 90%.[120]

More recent research from the International Institute for Strategic Studies shows that, since 2024, China has been shifting its strategy of exerting economic pressure from informal trade bans and symbolic changes in laws and regulations to the active imposition of formal export controls. For the time being, these export controls seem to be focused primarily on the United States, with China replicating US export controls which have been imposed on Chinese technology companies. It now increasingly states openly what these measures are a response to and imposes its countermeasures very quickly.[121]

In addition, China offers goods on the European market at prices with which Dutch companies cannot compete. As a result, Dutch and European companies may be out-competed in the market and existing strategic dependencies on China may increase, or new ones may come into being. Among other things, the country is an indispensable player in the energy transition. For instance, China is deliberately pursuing policies to maintain a monopoly on solar panels.[122] The same approach is playing out in the chemical industry. Dutch companies that produce fibres for defence equipment, such as bullet-proof vests, cannot compete with the prices offered by Chinese companies. These Chinese companies receive state support and can therefore offer their products at very low prices. The Royal Association of the Dutch Chemical Industry (*Koninklijke Vereniging van de Nederlandse Chemische Industrie*, VNCI) therefore warned at the end of 2024 that Europe should be aware that it might lose its basic chemical industry.[123]

US economic pressure

The US is increasingly likely to urge the Netherlands and the European Union to take restrictive action towards countries such as China and Russia.[124] The US applies export controls to China to curb, among other things, Chinese technological innovation and military modernisation.[125] A continuation of the current trade dispute with China is to be expected under the new Trump administration. This is something that Europe can scarcely ignore because it is heavily dependent on the US. The result could be economic retaliation by countries like China, such as the closing of markets to European companies and banning the export of critical raw materials and strategic goods and services to the Netherlands and the EU. If this leads to shortages in the Netherlands, the functioning of critical processes could come under pressure.[126]

Strategic dependency

The strategic dependencies[5] of certain commodities, goods and services can threaten the continuity of critical processes. This may be because state actors deliberately abuse these dependencies. Even when this is not the case, an over-reliance on certain goods and services can pose a threat to critical processes, for example when supply is interrupted by conflict elsewhere in the world, or dependency limits the Netherlands' open strategic autonomy. Strategic dependencies may exist not only with respect to countries, but also to one or a number of (tech) companies.

With regard to China in particular, there are strategic dependencies that may be risky for the continuity of critical processes. Such dependencies also exist with regard to Russia, but they are much smaller than those relating to China. As a result the damage in the event of an extreme and sudden disengagement from China would be considerably greater.[127] Dependencies which may affect critical processes also exist in relation to, among others, Taiwan and the US. A number of strategic dependencies on China, Russia, Taiwan and the United States are discussed below by way of an illustration. This is, however, not an exhaustive overview of all conceivable strategic dependencies for the Netherlands' entire critical infrastructure.

Strategic dependencies in relation to commodities

The Netherlands and the EU are heavily dependent on China for critical raw materials.[128] Without critical raw materials mined or refined by China, many critical processes would lack essential end products needed to keep functioning. Increasing tension between China on the one hand and the US and EU on the other could put pressure on the security of supply of critical raw materials.[129]

Research by The Hague Centre for Strategic Studies (HCSS) on the risks of dependency on Chinese raw materials for critical sectors shows that these critical raw materials are needed in numerous devices. Examples include wind turbines, helicopters, fighter jets, security cameras, drones and mobile technology ranging from smartphones and computers to ICT applications for online payments. Drones, for example, contain the raw materials silicon, cobalt, gallium and germanium, which are predominantly mined or processed by China.[130] Such critical raw materials are crucial for the functioning of critical processes, for example in the defence and security domain, sustainable energy system, sustainable mobility and ICT.[131]

Wind turbines and solar panels, which make up an increasing share of Dutch and European energy production, also use critical raw materials. Wind turbines require rare earth metals, cobalt and permanent magnets, almost all of which are produced in China. The production of solar panels depends on silicon, germanium and gallium.[132]

Strategic dependencies on China also exist in the healthcare sector, for example in the field of antibiotics and raw materials for the pharmaceutical industry.[133] In addition, most modern medical procedures rely on devices which are rich in the aforementioned critical raw materials, such as respirators, pacemakers, MRI scanners, X-rays and ultrasound machines.[134]

According to an NOS publication the Netherlands depends on Russia for nuclear medicine production. Radioactive substances are increasingly being used for medical research and to treat various types of cancer. This requires processed raw materials that are made almost exclusively in Russia.[135]

Strategic dependencies in relation to semiconductors

The research by HCSS also outlines the dependency of the Dutch critical infrastructure on semiconductors from Taiwan. Their supply could be cut off or restricted in the event of a Chinese blockade and/or invasion. Various critical processes are to a lesser or greater degree dependent on Taiwanese semiconductors[6]. In the medical sector, Taiwan plays an important role in supplying chips for medical devices, such as respiratory support systems, diagnostic devices and pacemakers. In the defence and security domain, advanced Taiwanese chips play an important role in military and police equipment. They are also needed for new technologies, such as AI and drones, which are going to be used on an increasingly large scale. Taiwanese chips are also used in the energy sector, in the automotive industry and numerous ICT applications.[136]

Strategic dependencies in relation to digital infrastructure

Strategic digital infrastructure dependencies also play a role within critical processes. Digital infrastructure is an essential element of the business processes of critical sectors such as energy, telecoms, finance and road and rail management. However, the Dutch digital infrastructure is largely managed and developed by large tech companies from non-European countries.[137] As data and digital services are moved to other countries and digital innovation increasingly takes place outside the EU, strategic dependencies on other countries, especially the US and China, in the digital domain are increasing. These dependencies imply risks, for example, when state actors gain access to sensitive information and critical processes through digital technology and services. They also limit

5 A dependency is strategic when a product or service is crucial in order to safeguard the public interests of the Netherlands and/or the EU, or when the dependency poses a risk to the continuity of critical processes or third-party access to sensitive information. A strategic dependency can be risky when there is a high risk of supply disruption. This depends on market concentration and the possibility of substitution, the nature of relations with the country we depend on and the degree of interdependency.

6 Taiwan Semiconductor Manufacturing Corporation (TSMC) in particular plays a key role in the semiconductor supply chain. TSMC produces 92% of the world's most advanced logic chips, referred to as cutting-edge chips (i.e. <10 nanometres). Taiwanese companies, including TSMC and United Microelectronics Corporation (UMC), also produce a significant proportion of less advanced chips, or 'trailing-edge' and 'mature' chips (i.e. ≥10nm). In total, Taiwan accounts for more than 20% of global semiconductor production, more than any other country in the world.

the Netherlands' digital strategic autonomy and may jeopardise Dutch public values and public interests.[138]

Dependencies on America exist in the area of cloud services, for example. A small number of American companies, Amazon Web Services, Microsoft Azure, and Google, dominate 70-80 percent of the European cloud services market.[139] In addition, the power of the largest cloud companies is growing because, once chosen, companies find it difficult to switch providers due to technical, organisational and financial barriers. Even when using European or Dutch providers, there is still a chance that they too use the services of these major cloud providers.[140] Much of the data of Dutch banks, for example, is being stored in the clouds of these US tech companies.[141] This strategic dependency has implications for Dutch digital open strategic autonomy. For example, the dependency on US companies means that US legislation also applies to varying degrees to Dutch organisations. In addition, the Netherlands only has limited authority when it comes to monitoring these companies. There is also the risk of a single point of failure and a failure or cyberattack on one of the three largest providers could have global repercussions.[142]

In the development of AI applications, large US and Chinese private tech companies have so far had the upper hand and the European market is lagging behind. Europe is therefore largely dependent on the big tech companies when it comes to obtaining the latest AI-related software and services, such as image recognition models and AI management tools. As the digitisation of processes and reliance on AI technology for basic services increase, with the software and services of tech giants being the only solution, so does the dependency on those same companies. After all, the accessibility and reliability of the software depends largely on the provider. Moreover, big tech companies are also getting involved in discussions with governments on the extent to which democratic freedoms should be taken into account.[143]

Europe also has a weak position in the field of applications and services, particularly with respect to the US and, in some areas, China. This applies, for example, to social media, office software and cybersecurity.[144] Once again, this may pose a threat to national security in some instances, for example when state actors, such as China, use applications and services for the purposes of state interference, economic espionage and the sabotage of critical processes.[145]

3.2 Terrorism and violent extremism: a potential threat to critical infrastructure

Terrorists and violent extremists can pose a threat to critical infrastructure. There have been no disruptive terrorist or extremist attacks on critical infrastructure in the Netherlands. However, accelerationist[7] publications and foreign examples do show that critical processes can be targeted by terrorists and violent extremists. What is more, critical providers may have to deal with employees with extremist views, such as sovereigntists and right-wing extremists.

The terrorist threat to the Netherlands and its critical infrastructure

There is a real chance of a terrorist attack taking place in the Netherlands. As stated in the Terrorist Threat Assessment for the Netherlands, the threat from jihadism and other radical Islamist circles is high. There is also a real possibility that individuals from the right-wing terrorist online milieu will put their words into action and turn to violence. In addition, new right-wing extremist groups, some of whose members adhere to terrorist ideology, are more prepared to take action. There is also a threat of violence on the part of a small group of sovereigntists.[146]

While jihadist groups usually play little attention to critical infrastructure as a target, some people have called for attacks to be carried out on the aviation sector. As described in the June 2024 Terrorist Threat Assessment for the Netherlands, al-Qaeda in the Arabian Peninsula (AQAS) issued a video calling for attacks on civilian aircraft belonging to US, British and French-Dutch airlines, including those of Air-France-KLM. Despite this incitement, the threat represented by al-Qaeda and its regional branches in the Netherlands and against Dutch interests abroad, including civil aviation, is likely to be limited.[147] In addition, the extensive media coverage of forest fires in different parts of the world sometimes leads to incitement in jihadist propaganda to start similar fires in order to cause damage and casualties. As far as we know, no forest fires have actually been started by terrorists or extremists with an ideological motive.[148]

The fact that right-wing terrorist organisations may also be able to target their attacks on critical infrastructure is evidenced by accelerationist publications describing how large-scale attacks on critical infrastructure, such as the electricity grid, telecommunications and oil transport must be carried out in order to help start a race war.[149] The Terrorist Threat Assessment for the Netherlands of December 2023 referred in this context to the Terrorgram Collective, via which, among other things, manuals for bomb-making and sabotaging critical infrastructure are distributed.

7 Accelerationism is right-wing extremist ideology that seeks to create chaos by means of terrorist violence in order to hasten racial war and the replacement of democracy with a national socialist and white ethnostate.

The Terrorgram Collective is a major resource for right-wing extremists and accelerationists worldwide that consists of an online network of different channels on the Telegram communication app.[150] However, the threat of actual right-wing terrorist attacks on critical infrastructure in Europe seems limited. In Europe, the threat from right-wing terrorists comes mostly from individuals. These are often vulnerable minors or young adults who become radicalised over a short period of time and then commit violence on a small scale. An attack on critical infrastructure requires a certain degree of organisation and preparation that these individuals are not capable of for the time being.[151]

Foreign terrorist attacks on critical infrastructure

Attacks which have been carried out abroad are proof that terrorist and extremist groups are able to target (sub-processes of) critical infrastructure. In Germany, for example, the left-wing extremist group *Vulkangruppe* set fire to an electricity pylon near a Tesla factory in March 2024 because they wanted to sabotage the factory. The fire caused a power cut that affected tens of thousands of residents in the region, as well as the plant.[152] Unlike the Netherlands, Germany has a sizeable, radical and active far-left scene. The threat of attacks on critical infrastructure by left-wing extremists in Germany has also increased recently. However, this is unlikely to have much impact on the small group of left-wing extremists in the Netherlands.[153]

The French railway system was sabotaged at the start of the Olympic Games in July 2024. The presumed suspects were members of a left-wing extremist group, although French authorities have not identified all the perpetrators. Equipment was damaged at three locations along the railway tracks in France. Dozens of underground fibre-optic cables which are used to transmit safety information for train drivers were burnt out. This act of sabotage resulted in trains being cancelled and hundreds of thousands of passengers were affected.[154] Fibre-optic cables belonging to telecom companies were also cut at several locations in France. This affected several providers and disrupted fixed and mobile telephony at local level.[155] This phenomenon was not new because fibre-optic cables were also cut well before the Olympics took place in France.[156]

In the United States a suspected far-right group carried out an attack on an electricity grid in 2022 that left 45,000 residents without power.[157] The same was also suspected to have happened in several other incidents in the US.[158]

Employees with extremist views

Critical providers may have to deal with employees who hold various extremist views and who may pose an insider threat, for example if they have access to sensitive information or systems.

The June 2024 Terrorist Threat Assessment for the Netherlands describes, for instance, how right-wing extremists have become interested in joining the military, partly because they can gain experience with weapons and combat and because of the association with brotherhood and masculinity.[159]

In the same vein, the December 2024 Terrorist Threat Assessment for the Netherlands states that several organisations in the Netherlands are having to deal with individuals who had declared themselves to be 'autonomous' or 'sovereigntist' extremists. Individuals who call themselves sovereigntists believe that the Dutch government does not exercise legitimate power over them and that they can decide for themselves whether Dutch laws and regulations apply to them. These sovereigntists mostly have a desire to create an alternative world which is independent of institutions.[160] In total, there are several tens of thousands of adherents to sovereigntist thought in the Netherlands. Between several dozen and a hundred of them believe a violent confrontation with the government will eventually become inevitable. In the Netherlands a limited number of self-declared sovereigntists are employed at government institutions or in critical sectors. Some of them have access to sensitive information in connection with their jobs. Their self-proclaimed sovereigntist identity may be at odds with the professional integrity associated with their work.[161]

3.3 Activists also target critical infrastructure

Various protests and activist campaigns in the Netherlands and Europe in recent years have shown that critical sectors can be targeted or affected by activists[8] and demonstrators. Because there is no systematic research on activism in relation to critical infrastructure, it is impossible to establish whether there has been an increase in activism that has targeted critical providers in recent years. However, there have been several examples in the past few years of activities which have caused short-term disruption to critical infrastructure such as airports, road infrastructure and a lock system. National security interests were not compromised in the process. If the scale, frequency and/or duration of such activities increase, they could become a threat to national security.

There have, for example, been several incidents in recent years which have targeted the aviation sector. In November 2022, climate activists from Greenpeace and Extinction Rebellion managed to gain access to the eastern part of Amsterdam Airport Schiphol (Schiphol-Oost). They proceeded to sit down under private jets to prevent them from taking off. Several activists also chained themselves to planes.[162] In March 2024, Extinction Rebellion blocked several access roads to the Tefaf art fair in Maastricht to protest against private jets landing at Maastricht Aachen Airport for the art fair.[163]

8 The aim of activists is to convince others of a particular point of view, but in doing so they do not pursue undemocratic goals nor do they use undemocratic methods. Although activists do break the law sometimes, they do not do so with the intention of undermining the democratic rule of law.

In December 2024, climate activists from Extinction Rebellion were arrested at Schiphol Airport after they had purchased tickets and had passed through security control only to pour a large amount of brown liquid on the floor in protest at KLM's loyalty savings programme.[164]

In Germany, climate activists from *Letzte Generation* blocked runways at Frankfurt airport in July 2024. The protest involved them gluing themselves to the tarmac. Air traffic was halted for hours as a result, and 270 of the 1,400 scheduled flights were cancelled that day.[165] In May that year, climate activists had also blocked access roads to the runway at Munich airport.[166]

Activists are also targeting maritime infrastructure. In July 2024, Extinction Rebellion blocked crucial access routes to the Port of Rotterdam.[167] In September 2024, Extinction Rebellion and its sister organisation *Geef Tegengas* occupied the *Botlekbrug* bridge, which is a key link for road, rail and shipping traffic for the Port of Rotterdam and the Maasvlakte. They did so in protest against expansion of the gas industry.[168] In August 2024, Extinction Rebellion activists blocked the IJmuiden lock complex by gluing and chaining themselves to the gate of the *Noordersluis* lock. Although they were targeting cruise shipping, the blockade also affected all shipping traffic in the North Sea Canal (*Noordzeekanaal*).[169] In June 2024, Greenpeace activists occupied a drilling platform near the island of Schiermonnikoog to campaign against gas extraction plans to the north of the island.[170]

Activists also target major roads to increase the social impact of their actions. For example, Extinction Rebellion have blocked the A12 and the A10 motorways several times in recent years in protest against fossil subsidies.[171] Protests by farmers have also resulted in motorways being blocked on several occasions in the Netherlands. Tractors, hay bales and arson were some of the tactics used to bring traffic to a standstill.[172]

3.4 Criminal activity: a potential threat to critical infrastructure

Critical infrastructure can also be threatened by criminal activity. Although it often takes the form of cyberattacks by criminals, it may also involve subversive crime or physical acts.

Cybercrime targeted at critical infrastructure

The actions of cybercriminals are motivated by financial gain and are not (primarily) intended to disrupt society. Nevertheless, their attacks can have such an impact that they affect national security interests. The capabilities of some cybercriminal groups are comparable to that of state actors.[173]

In the past, some criminal groups deliberately let it be known that they did not target critical infrastructure. Indeed, to do so would have been unwise because it would bring them to the attention of intelligence and investigative agencies. On the other hand, there could be a tendency in critical sectors to pay ransoms more quickly for the sake of business continuity thereby making the organisations in question an attractive target for criminals after all. In practice, criminals often behave opportunistically. This means that although cybercriminals do not deliberately attack critical infrastructure systematically it is, in principle, not ruled out either.[174]

Although criminal cyberattacks have not caused social disruption in the Netherlands in recent years, several incidents do show how critical sectors can be affected by them. This applies, for example, to the energy sector. One example of such an attack was when it became impossible to carry out a trial of Dutch wind turbines at the Oude Maas Wind Farm in early 2022 due to a ransomware attack on German wind turbine manufacturer Nordex. The energy sector in Denmark was the target of a major cyberattack in May 2023. A total of 22 energy companies were compromised due to vulnerabilities in manufacturer Zyxel's firewalls.[175] Research by SektorCERT, the cybersecurity centre for Denmark's critical sectors, revealed that the attack was made possible because companies had failed to install security updates.[176] Thanks to SektorCERT's sensors the attack was quickly detected and a large-scale power outage prevented.[177]

The maritime sector has also been targeted by cybercriminals in recent years. The Dutch maritime service provider Royal Dirkzwager was the target of a ransomware attack by the 'Play' ransomware group. Royal Dirkzwager registers all incoming and outgoing seagoing vessels in the Port of Rotterdam. The company was unable to provide a number of services to customers, including the system that gives customers a real-time view of when ships arrive and the ROAM service which is used to monitor maritime traffic.[178] The hacker also leaked confidential information from the organisation, including employee IDs, passports and contracts. The company needed almost a week to fully restore its systems and resume services.[179]

The National Cybersecurity Assessment 2024 revealed that healthcare organisations are regular victims of cyberattacks. These often involve ransomware, extortion using stolen data, or both. Up to now the majority of these attacks have been perpetrated abroad and impacted the provision of care.[180] In the UK, for example, operations and blood transfusions were cancelled at several hospitals in June 2024 after a supplier of pathology services fell victim to a ransomware attack by Russian cybercriminals from the Qilin group.[181] In July 2024, blood banks in the United States suffered a ransomware attack which resulted in more than 250 hospitals having to activate their blood shortage protocols.[182] As far as is known, these attacks had no impact on the provision of care in the Netherlands. However, organisations were blackmailed using stolen data and data was leaked.[183]

Subversive criminality

Subversive criminality not only poses a threat to society and the rule of law, but can also represent a threat to critical infrastructure. This is especially evident at seaports, where organised crime gangs use infrastructure for, among other things, drug trafficking. The fact that criminals need to use certain infrastructure, means they do not benefit from damaging or sabotaging it. However, their activities can put pressure on the functioning of this infrastructure. For example, logistics processes are disrupted by persons illegally retrieving drugs at terminals. In addition, port employees and inspections are put under pressure, intimidated or recruited. Some employees choose to work in other sectors for fear of also becoming a victim of this behaviour. This makes it difficult to recruit the staff that are needed to keep the infrastructure operational.[184]

Theft of copper

One example of criminal activity that directly harms critical infrastructure is the theft of copper, for example from lightning conductors, cabling and railway tracks. If a railway line is affected, trains will no longer be able to use it or traffic will be limited and trains will have to travel slowly.[185] The use of measures such as camera surveillance and the installation of fences resulted in a sharp decrease in instances of copper theft on the railways in recent years.[186] In addition to railways, energy companies, such as those operating solar farms, also have to contend with copper theft.[187]

Insider threats

Insider threats can play a role in the various threats facing the Netherlands. Some insiders have personal motives for their actions, such as frustration, political beliefs or financial gain. Others collaborate with the malicious acts of state actors, terrorists, activists or criminals voluntarily or under duress. Insider threats can also be unintentional, with careless actions exposing a critical provider to a particular threat. Finally, insiders can also be individuals who deliberately ignore rules, such as security guidelines. As a result, they render a critical provider vulnerable to threats or system failure. Insiders may operate within a critical provider's organisation, or in the often complex chain of suppliers. [188]

The Signpost Six Insider Risk Trend Report 2025 charts the various trends in the field of insider threats. It transpires that money problems are the main driver of insider threats. The fact that companies are improving their cyber and physical security is also causing malicious actors to choose to recruit insiders for, among other things, espionage, pre-positioning and sabotage.[189]



Climate change is increasingly causing extreme weather events in the Netherlands as well. Natural elements pose an increasing threat to critical infrastructure.

4. Natural threats to critical infrastructure

There are a variety of natural threats to critical processes and our critical infrastructure is facing the increasing threat posed by the effects of climate change in particular.
The following section discusses the threats due to climate change, earthquakes, space weather and infectious diseases.

4.1 Climate change poses a growing threat to critical infrastructure

Climate change is accelerating and becoming more severe than previously thought and this is creating new threats and exacerbating existing ones.[190] Based on climate models, the Intergovernmental Panel on Climate Change (IPCC) expects the global climate to have warmed by 1.5 degrees by around 2033. The European Netherlands is warming up approximately twice as fast as globally, and it is already 2.3 degrees warmer than in around 1900.[191] This means the Netherlands is already facing serious, direct and indirect consequences of climate change and will continue to do so in the coming years.[192] The consequences include rising sea levels and more frequent and more extreme weather events. On the one hand, heat and drought will increase and, on the other, extreme rainfall will become a more frequent occurrence. It is therefore increasingly likely that the Netherlands will experience disruption or failure of critical infrastructure due to climate change.[193]

At the same time, the exact consequences of climate change and their precise impact on critical processes are difficult to estimate.[194] The Netherlands Environmental Assessment Agency (*Planbureau voor de Leefomgeving*, PBL) concludes in the report entitled 'Climate risks in the Netherlands - The current state of affairs (*Klimaatrisico's in Nederland - De huidige stand van zaken*)' that it is difficult to get a complete overview of the complex risks due to climate change because of the large number of possible combinations, the accumulation of climate risks, the chain effects and the side effects of climate adaptation. The sum of multiple risks may therefore turn out to be greater than expected.[195] For instance, the accumulation of extreme rainfall as well as high river discharges and higher sea levels will make drainage especially difficult.[196]

In addition, the extent and speed of the impact of climate change depends on specific circumstances, the social context and the implementation of climate adaptation policy. The increased dependency of the public and businesses on electricity, ICT and logistics networks, among others, also makes the Netherlands more vulnerable to the effects of climate change on critical infrastructure like this.[197] It is also the case that extreme weather can impact multiple critical processes at the same time, while a higher probability of natural threats also means an increased probability of different threats coinciding.[198]

4.1.1 Extreme weather as a consequence of climate change

The Delta scenarios[9] of the National Delta Programme present several possible future scenarios based on a plausible range of climate change, the Netherlands' efforts to reduce greenhouse gas emissions and socio-economic developments.[199] All scenarios predict a substantial increase in the water challenges facing the Netherlands. Shortages of freshwater will increase during the summer, there will be more flooding due to rainstorms and the effects of that flooding will become more severe.[200]

Extreme precipitation

The number of heavy showers with high precipitation is increasing due to climate change.[201] In summer this is due to peak showers and in winter to long periods of rain.[202] The situation can become so extreme that the water system can no longer cope, resulting in more frequent floods.[203] Flooding can be disruptive when critical networks, such as the electricity grid, gas grid, or communication networks and the Internet, cease to function. Roads may become impassable and hospitals, transformer stations and sewage treatment plants may fail due to flooding.[204] In recent years,

9 In 2024 Deltares was commissioned by the Delta Commissioner and the Ministry of Infrastructure and Water Management to compile a new set of Delta scenarios. These are based on the latest insights from, among others, the Royal Netherlands Meteorological Institute (KNMI), the Netherlands Environmental Assessment Agency and Wageningen University.

extreme precipitation in several European countries led to, among other things, power cuts, public transport shutdowns and airport closures.[205]

One example is the extreme rainfall in July 2021 in southern Limburg and in the Ardennes and Eifel regions where a major weather system caused waterlogging and flooding. Locally more than 160 mm of precipitation fell in 48 hours in southern Limburg. More than 250 mm fell in 48 hours in some locations in the Ardennes and the Eifel regions. In other countries there were 200 casualties and prolonged outages of essential services such as electricity and transport. In the Netherlands, localised infrastructure temporarily failed and was damaged. At some locations it took six months to rectify the damage.[206]

In October 2024, extreme rainfall in Valencia caused the heaviest flooding in Spain this century.[207] It caused over 200 deaths and large parts of the city's infrastructure were damaged. In some places around Valencia, 400 millimetres of rain fell in a single day. There was a clear link to climate change. The warm Mediterranean Sea had caused extra evaporation and warm air caused extra heavy rainfall and a so-called cold pool caused the rain front to linger in the same place.[208]

What is more, in the Caribbean part of the Kingdom the probability of severe hurricanes is increasing and the hurricane season is lasting longer and longer. In 2022 there were power outages in some parts of Bonaire after heavy rainfall flooded parts of the island.[209]

Climate change also increases the likelihood of katabatic winds.[210] These can occur during heavy thunderstorms as air cools sharply due to very heavy rainfall. The cold air falls onto the surface of the Earth and creates very severe wind gusts.[211] One occurred, for example, in the municipality of Leersum in June 2021 where it caused seven gas leaks due to falling trees in addition to nine injuries and damage to houses.[212] Four high-voltage pylons in the municipality of Oosterwolde were blown over as a result of an extreme katabatic wind.[213]

Extreme heat and drought in summer

Climate change also causes both extreme heat and drought in the summer. Prolonged drought can put pressure on critical processes such as drinking water supply and inland shipping.[214] Wildfires are also becoming more prevalent and they will more frequently result in damage and the failure of critical infrastructure.

Freshwater shortages

The Delta scenarios show that shortages of freshwater will become more and more common during the summer. The supply of freshwater is declining as a result of increasing evaporation, longer periods of drought, lower river flows and the increasing salinisation of groundwater.[215] Groundwater salinisation is partly due to subsidence and reduced flows from rivers during periods of extreme drought. [216] Rising sea levels are also contributing to salinisation via groundwater, rivers and sea locks, especially in coastal areas.*217* At the same time, demand for water is increasing in order to flush water systems (salinity control) and irrigate agricultural areas, as well as for drinking water and nature and the rewetting of low-lying peatlands. The Delta scenarios conclude that the expectation is that, by 2050, it will be increasingly difficult to keep sufficient freshwater available for all of its current uses.[218]

Pressure on the supply of drinking water

Both groundwater and surface water are also used for drinking water abstraction. These water sources are not only under pressure from increasing drought and salinisation. The quality of both sources is suffering due to pesticides, nitrate from manure and residues from medicines and cosmetics. In addition, the demand for drinking water is increasing due to population and economic growth. Consequently, several factors are combining to increase the vulnerability of drinking water supplies.[219] In 2023, the National Institute for Public Health and the Environment (*Rijksinstituut voor Volksgezondheid en Milieu*, RIVM) warned of regional shortages in the supply of drinking water and that, without action from 2030 onwards, shortages are expected to occur at all ten water companies.[220] If no measures are put in place, the shortfall would be over 100 million cubic metres, slightly less than the consumption in a province like Overijssel. Even now, drinking water companies sometimes have insufficient drinking water available and that is forcing them to halt supplies to businesses.[221] An action plan by the central government, the provincial authorities and water companies is intended to prevent any shortages by 2030.[222]

Effect of drought and heat on critical processes

There are numerous examples of how drought and heat can represent a threat for critical processes. In the summer of 2022, for example, drought resulted in significantly reduced water levels in our inland waterways which, in turn, had a significant impact on the loads that shipping could carry. Among other things the more frequent dry spells make it necessary to adjust infrastructure, logistics and vessel structures in order to continue maximising the potential of inland shipping.[223] Flood defences and dykes are also susceptible to drought. Extreme drought can cause cracks to appear in dykes and damage to flood defences.[224] Cracking due to drought is most common in the case of peat dykes.[225]

Heat and drought also cause problems on the railways. For example, movable railway bridges may expand due to heat and therefore no longer open or close. In addition, high temperatures increase the risk of rail buckling, which causes kinks in the rails themselves. Soil subsidence caused by drought can also result in uneven subsidence of the track or platforms.[226]

Increasing drought may also affect industries such as the chemical sector, for example due to a shortage of process and cooling water and firefighting water and a limited supply of raw materials or products due to low water levels.[227]

Wildfires

The risk of wildfires in the Netherlands is high. According to the Wildfire Report '23 (*Natuurbrandsignaal '23*)[10] wildfires will become more intense due to climate change and the Netherlands will have to deal with uncontrollable wildfires more often and these wildfires will be increasingly difficult to quell using current firefighting tactics, technology and capacity.[228] Once again rising temperatures, the greater likelihood of drought in summer and falling groundwater levels are an important factor because they cause vegetation to become increasingly combustible and this will lead to more frequent direct and indirect damage and the failure of critical infrastructure in the spring and the summer. Moreover, the close connection between nature and the physical living environment in the Netherlands means wildfires can quickly cause significant damage to critical infrastructure. [229] Roadside fires can, for example, cause railways and roads to be closed due to the space needed for emergency services, or poor visibility due to smoke. Much of the main road network is susceptible to closure as a result of smoke from wildfires which burn or smoulder for a long period of time, while even smaller fires can have a potentially significant social impact when they occur at critical points on the main road network.[230] Electricity, telecommunications or drinking water supplies could also be affected in the event of an uncontrollable fire. If a critical transformer fails, a local wildfire could even cause regional power outages.[231] An increase in (simultaneous) wildfires will also put greater pressure on the firefighting system because firefighting resources will be insufficient to meet a higher demand for assistance.[232]

4.1.2 Sea level rise due to climate change

Sea levels around the world are rising more quickly as a consequence of accelerating climate change. This sea level rise is also evident along the Dutch coast. Currently, the rise is a few millimetres a year (3.7 millimetres). Depending on greenhouse gas emissions, the projected cumulative sea level rise in 2050 is 16 to 38 centimetres.[233] According to the KNMI's latest climate scenarios (2023), the sea level off the Dutch coast is likely to rise by a maximum of 1.2 metres up until 2100. After 2100 the rate of sea level rise will increasingly depend on the rate of warming and whether or not parts of the Antarctic ice sheet become unstable. If the Antarctic ice sheet becomes unstable, this rise could even reach 2.5 metres by 2100 and 17.5 metres by 2300. The chances of this happening are small, but the consequences of such a sea level rise would be extreme.[234]

The rise in sea levels in the Netherlands will mainly affect water safety and the availability of freshwater. Research by the Sea Level Rise Knowledge Programme (*Kennisprogramma Zeespiegelstijging*) highlights the fact that the current approach involving dyke reinforcements, storm surge barriers, sand replenishment and pumping for flood protection means the Netherlands can probably continue to protect itself technically from flooding until sea levels have risen by 3 metres. However, this implies considerable effort and changes to the use of space because the ongoing rise in sea level will require ever more extensive sand replenishment and ever greater reinforcements of flood defences. Storm surge barriers will also have to close much more frequently and eventually be replaced.[235]

4.2 Earthquakes

Earthquakes have the potential to cause disruption or failure of critical processes. This is partly because many critical infrastructures, such as pipes and cables, are located underground.[236] However, there are no known recent incidents involving disruption to or failure of critical processes due to an earthquake in the Netherlands.

An earthquake is a seismic movement of the earth's crust. Earthquakes can have a natural cause or be induced by humans. Both types of earthquakes occur in the Netherlands.[237] Earthquakes are not affected by climate change. As gas production in the Groningen field ceased at the end of 2023, both the likelihood and force of earthquakes are decreasing there.[238] Most natural quakes in the Netherlands occur in Limburg.[239] In 2024, 47 earthquakes occurred in the Netherlands, including 40 induced and 7 natural earthquakes. This number is lower than in 2023 when there were 62 earthquakes.[240]

4.3 Threat to critical infrastructure posed by space weather

Some critical processes use advanced technologies that may be vulnerable to space weather.[241] There are several space weather phenomena that can affect critical infrastructure and all of these originate from the sun's activities. During the 11 year solar cycle, there are periods when the sun is very active and periods when it is calm. [242]

There are three main phenomena produced by the sun that cause space weather on Earth:

1. Solar flares. These are intense bursts of energy in the form of electromagnetic radiation, such as X-rays. They can cause temporary interference in communications and navigation.
2. *Coronal mass ejections* (CMEs). This is a process by which a large

10 The Wildfire Report '23 (*Natuurbrandsignaal '23*) was drafted by a consortium consisting of the Netherlands Institute for Public Safety (*Nederlands Instituut Publieke Veiligheid*, NIPV), the Royal Netherlands Meteorological Institute (KNMI), Wageningen University & Research (WUR), the VU Amsterdam and Deltares.

amount of solar plasma containing charged particles, such as protons and electrons, is released from the sun. When these particles reach Earth, they can cause a geomagnetic storm which disrupts the planet's magnetosphere.

3. *Proton storms*. These storms consist of very fast-moving, high-energy protons which can cause damage to satellites through particle radiation.[243]

When such a solar flare, coronal mass ejection or proton storm is directed towards Earth, it affects our atmosphere.[244]

Earth is in a space weather peak in the years 2024 - 2026. On 10 and 11 May 2024, for example, there was a global geomagnetic storm of the most severe category. Geomagnetic storms can affect the higher layers of the atmosphere, such as the thermosphere and ionosphere. This, in turn, can interfere with radio communications and satellite navigation systems.[245] Long-range communication is very important for aviation and in a highly disturbed ionosphere this contact can become difficult or even impossible. Given that space weather disrupts the ionosphere, satellite signals may also be disrupted by the ionosphere.[246] As described in section 3.1.1, numerous satellites rely on GNSS for timing and positioning and the disruption to or failure of these can cause major chain effects.

The potential impact of a geomagnetic storm on satellites was evident, for example, when SpaceX launched Starlink satellites in February 2022. Of the 49 launched satellites that were supposed to enter low Earth orbit, 40 were lost after launch due to a geomagnetic storm. The storm caused a lot of drag and the satellites fell back into the atmosphere and burned up.[247]

In exceptional cases, electricity grid operators may also experience problems due to a solar storm.[248] Geomagnetic storms can disrupt the Earth's magnetic field, which in turn induces electrical currents in electricity grids. These disturbances can lead to network outages, especially in areas where the earth's crust is poorly conductive.[249] This threat exists mainly in northern areas and it last occurred on a large scale in Canada in 1989 when millions of people were without power for hours due to a severe geomagnetic storm. Such disruption is unlikely to occur in the Netherlands due to our geographical location, highly conductive soil and short, densely meshed electricity grids.[250]

4.4 Threat to critical infrastructure posed by infectious diseases

The COVID-19 pandemic showed that a large-scale outbreak of an infectious disease can have major consequences for society. Human infectious diseases can lead to deaths and illness and, in a severe pandemic, can also result in a lack of sufficient acute care.[251]

A number of developments have taken place that may indicate an increased risk of a large-scale outbreak of infectious diseases in the longer term. For example, more and more animal species are susceptible to bird flu.[252] For a few years now mammals such as cows have become infected, as have humans sporadically.[253] The variant circulating among cows in the US is not currently spreading from human-to-human. However, the likelihood of mutations doing so is increasing as the virus circulates freely among mammals in the US. Various epidemiologists and virologists have been referring to the situation in the US as worrying for months now, partly due to the lack of preventive measures, monitoring and the slow sharing of information with scientists.[254]

In addition, global warming is increasing the likelihood of new pandemics. This is partly because mosquitoes and ticks are becoming prevalent in locations they have never been before where they may come into contact, for example, with sick animals.[255]

Finally, the public is becoming less and less willing to be vaccinated and there have been new developments in bioinformatics and AI.[256] Some experts warn of the possibility of malicious actors using AI models in the future to develop biological weapons, for example in the form of an infectious virus.[257] While current models are not capable of this, the possibility of future, even more advanced models being able to create such weapons is something we need to monitor closely.[258]



The NAFIN network, an important fibre-optic network for maintaining national security, went down on Wednesday 24 August 2024. As a result, air traffic at Eindhoven Airport came to a complete halt.

5. Threats arising from the failure of critical processes themselves

National security can also be compromised when critical processes fail due to human error, system failure or chain effects. In such instances, the critical process failure is thus not due to the actions of malicious actors or natural threats. Nevertheless, these kinds of threats can increase the impact of human and system failures, for example when flood defences fail due to a technical problem during a period of extremely bad weather and significant rainfall.[259]

5.1 Human and system failures

Human failure involves failure or disruption of a critical process due to inadvertent human error. System failure is the result of a technical fault in the system itself. Several examples of such failures show that a seemingly minor technical or human error can have major consequences for critical processes and, in extreme cases, can even pose a threat to national security.

In the summer of 2024 a software error resulted in two large-scale outage incidents which severely impeded, among other things, the provision of hospital care, the aviation sector and the functioning of government. One of the effects was a global outage of millions of Microsoft systems due to a faulty update of CrowdStrike's software in July 2024.[260] This led to the failure or disruption of critical processes in various countries. Some banks were temporarily unable to make transfers, some TV channels went down, port terminals were at a standstill and flights had to be cancelled at many airports.[261] Although national security was not compromised in the Netherlands, several critical processes were also affected by the failure. Hospitals in Emmen, Hoogeveen, Stadskanaal and Doetinchem had to scale down care temporarily and transfer patients to other hospitals for emergency care. Flights also had to be cancelled at Schiphol and Eindhoven airports, and buses in the province of Utrecht and regions of Amersfoort and Almere were cancelled temporarily. Customers of the KNAB digital bank were unable to access the financial services provider's app.[262] The CrowdStrike outage shows how vulnerable the digitised society is and that such failures can result in large-scale outages. The existence of digital monocultures, in which many organisations depend on a small number of providers within the wider digital ecosystem, can lead to large-scale effects.[263]

In the Netherlands various digital processes were disrupted by a software error on a Ministry of Defence network in August 2024. The cause of the problems was down to how access was being provided to the Netherlands Armed Forces Integrated Network (NAFIN). This heavily secured network connects Ministry of Defence locations with each other and it is also used at data centres which serve various ministries and police stations. An error in the software code caused a time synchronisation issue on the network. Emergency services encountered problems with their communication and alarm systems, making it more difficult for them to stay in contact with each other. Civil servants from various ministries were unable to log on to work systems. Eindhoven Airport uses the same network and was also affected because planes were unable to take off or land there.[264] The failure even impacted the operations of the Coast Guard (*Kustwacht*) because their communication and alert system malfunctioned, meaning that they could temporarily not be contacted by ships in distress, as well as the Royal Netherlands Sea Rescue Institution (*Koninklijke Nederlandse Redding Maatschappij*, KNRM) and air traffic control.[265]

The critical process of 'communication with and between emergency services via 112 and C2000' has also experienced outages due to system failures in recent years. In 2019 the 112 emergency number was down for some time due to a breakdown in the systems of telecoms provider KPN. This was caused by the malfunctioning of a digital counter in the telephone system.[266] The C2000 communication system, which police, fire brigade, ambulance and defence services staff use to communicate, has regularly been disrupted by system failures. In June 2023, for

example, control rooms experienced problems in communicating with emergency responders on the street due to a networking problem between control rooms and C2000 central equipment.[267] On New Year's Eve in 2024/2025, the C2000 system suffered a malfunction which was possibly caused by overloading.[268]

Air Traffic Control the Netherlands (*Luchtverkeersleiding Nederland*, LVNL) suffered a failure in April 2024 which was caused by incorrect preparations for an update of new software in the air traffic control (AAA) system. The organisation was able to fall back on the AAA's so-called backup mode and, when this also proved unreliable, it reverted to its backup system (Phoenix). The malfunction resulted in almost no air traffic to and from the Netherlands but once AAA had been restarted the air traffic control system started working again and normal service could resume.[269] A number of aircraft could not take off and some landings were diverted to Belgium. Because the failure occurred late in the evening, the impact was limited.[270]

Human or system failure can also coincide with other threats, such as extreme weather. Amsterdam faced the risk of flooding on 2 November 2023 due to an accumulation of threats which led to high water levels caused by heavy precipitation, storm Ciarán and a failure at the IJmuiden pumping station. A malfunction meant that the sluice gates at the IJmuiden pumping station were unable to close. The sluice gates are open at low tide to discharge excess water into the sea but close again at high tide. The technical problem meant they were unable to close and were open for some time at high tide. As a result, a huge wave of sea water entered the North Sea Canal in the early morning and the IJ river level also increased. Once the problem had been discovered, a team of engineers quickly closed the valves by hand. The combination of the malfunction, high water levels and storm Ciarán resulted in a water level of -12 centimetres, while it is normally -40 centimetres. To protect Amsterdam from flooding the 14 locks and flood defences along the IJ River were quickly closed to prevent the water level in the canals from rising even further. The Zeeburg Pumping Station was then activated at full power to restore the city's water level to where it should be. Closing the locks between Amsterdam and the IJ river, among others, caused the water to subside to the desired level of around -40 cm Amsterdam Ordnance Datum (*Normaal Amsterdams Peil*, NAP) within 24 hours.[271]

Some problems arise within critical processes which have no clearly identifiable cause, such as the railway accident at Voorschoten station when a goods train collided with a crane that was being transported on several trucks in the night of 4 April 2023. The crane ended up in the other track and was hit by a passenger train. The crane driver was killed and 20 people were taken to hospital. No train traffic was possible between Leiden and The Hague for over two weeks. Investigations by the Dutch Safety Board (*Onderzoeksraad voor Veiligheid*) found that there were several factors that may have contributed to the accident, but the investigation could not identify a direct cause.[272]

5.2 Chain effects

The interdependencies within critical national infrastructure mean that a disruption to a single critical process can result in chain reactions that impact other critical processes. These are also referred to as cascading effects.[273] Critical processes are also connected to all kinds of non-critical processes. Consequently, disruptions to these non-critical processes can also have major chain effects on critical processes. A good example of this were the chain effects of the aforementioned NAFIN failure (non-critical) on, among others, emergency services and air traffic (critical).

The increasing complexity of systems and dependencies between systems and processes and the many mutual and hidden dependencies within and between critical processes make it difficult to estimate the chain effects of a disruption to critical processes properly. In addition, these dependencies are constantly changing due to technological developments and the updating of systems and infrastructure.[274] Electricity outages in particular have major chain effects[275] and they tend to occur unexpectedly. Since electricity can only be transmitted when the grid is live, the electricity grid has no buffering capacity. As a result, the effects are immediate for all parties involved. The majority of electricity outages are normally rectified within two hours and so do not lead to any social disruption. In the case of a large-scale or very complex outage, the cause may not always be immediately identifiable and it is difficult to estimate the time required to rectify the situation.[276] The impact of electricity outages on various critical processes often becomes noticeable within hours.[277] For example, power outages of just a few hours can cause telecoms to go down and as a result the public are unable to call 112. Large-scale outages quickly cause the failure of regular means of communication, such as the Internet and TV.[278] As such, the electricity network is so essential to Dutch society that a failure could lead to serious social disruption and therefore pose a threat to national security.[279]

Natural gas and electricity supplies are also closely linked and cannot function (for long) without each other. Because the equipment that controls the natural gas supply is powered by electricity and only limited emergency measures can be taken, the natural gas supply is unable to function without electricity. Similarly, gas-fired power plants cannot function without natural gas because the gas plants will have no fuel to operate the generators.[280]

In the Thematic report on the threat to critical infrastructure (*Themarapportage bedreiging vitale infrastructuur*) (2022), the National Security Analyst Network developed a scenario for the failure of electricity supply in Europe. Although many of the critical processes could operate for some time using an emergency power supply, it is uncertain whether this would work in practice. While the effect of power outages on other critical processes is difficult to estimate, the National Security Analyst Network's scenario shows that 24 hour power outages in the Netherlands could cause train

traffic to be (partially) shut down, debit card payments to become impossible at shops without an emergency power supply and objects such as pumping stations to cease functioning within a short period of time.[281]



A power cut could bring train traffic to a halt. For example, an outage in June 2025 prevented train traffic to and from Schiphol Airport.

6. Political, economic, social and technological factors

Various political, economic, social and technological factors (PEST factors) affect the critical infrastructure itself, as well as the threats to it and its resilience. In doing so they also influence the impact of concrete incidents arising from threats. Technological development can, for example, change the means used by malicious actors to disrupt critical infrastructure. At the same time, technological development offers critical providers new opportunities to increase their resilience to threats. The critical infrastructure itself may change due to energy transition or digitalisation, for example. Such changes, in turn, also affect the threat and the level of resilience. The most important PEST factors are listed below.

6.1 Increasing dependency on digital systems

A key feature of critical infrastructure is that it is increasingly dependent on digital systems, such as in healthcare and logistics. In addition, the complexity of systems and the dependencies between systems and processes are increasing,[282] for example because they are interconnected or because critical processes use the same hardware or software.[283] The interdependencies make it difficult to estimate the effect of disruption to one critical process on other critical processes.[284]

In times of rising geopolitical tensions, the threat of disruption to digital systems through cyberattacks, sabotage and espionage may increase.[285] The Netherlands is also an attractive target for malicious actors for several reasons. For instance, the Netherlands has a high-quality knowledge economy and we are at the forefront of certain technologies. The Netherlands is also home to a variety of international organisations that process information that could be of interest to malicious actors.[286] Another reason why the Netherlands is an attractive target is that the country is one of the top 5 most important digital hubs worldwide.[287] This is partly because there are landing points for ten international submarine data cables in the Netherlands and the presence of Internet exchanges including Amsterdam Internet Exchange (AMS-IX) and (co-location) data centres. [288] Finally, the fast, cheap and reliable Internet infrastructure in the Netherlands makes it attractive to malicious actors to use as a base from which to launch cyberattacks against the public, organisations or governments in other countries.[289]

Most modern (critical) infrastructure is susceptible to attacks whereby malicious actors penetrate and manipulate digital systems.[290] Digitalisation means that cyberattacks, for example, pose a real danger of large-scale outages of electricity grids that connect different power plants and ensure that electricity reaches households and businesses. A successful cyberattack on a power network can cause a chain effect with significant physical consequences. These include outages and damage to power plants and other critical infrastructure such as water supplies, transport and communications.[291]

Cyberattacks are also a daily occurrence at financial institutions.[292] Europe's financial infrastructure is highly interconnected and companies in the financial sector depend on a limited number of digital service providers. If hackers carry out a cyberattack on one such company, they may impact several and the companies themselves can potentially infect each other.[293]

Operational technology (OT) is crucial when it comes to controlling, monitoring and managing numerous critical processes. OT systems underpin important physical processes such as raw material production and processing, drinking water purification, lock operation and electricity distribution. Incidents in OT environments can also damage industrial equipment and the surrounding environment. In extreme cases, casualties may occur. The increasing integration of operational technology and information technology (IT) increases the attack surface and makes OT systems more vulnerable to cyberattacks.[294]

Cyberactors appear to be interested in compromising OT and for that reason there exist types of malware that can be used to sabotage OT systems.[295] Since the end of 2023, Microsoft has seen an increase in the number of reports of attacks targeting Internet-exposed, poorly secured OT devices.[296]

In a broader digital ecosystem, digital processes are highly interconnected meaning that even non-critical organisations can be an attractive stepping stone to infiltrate critical providers for malicious actors.[297]

6.2 Technological developments

Technological developments will significantly influence the security environment in the future. On the one hand, they can boost existing threats to critical infrastructure or make it more vulnerable to threats. On the other hand, new technology can also be used to increase the resilience of critical infrastructure, for instance in the context of defending against (digital) attacks. Technology can also be used to solve certain challenges facing society, such as climate change, thereby reducing threats to critical infrastructure.

Advanced technology is becoming more widely accessible and available worldwide. A technology race is taking place between states, especially in the field of AI, quantum technology and space technology. At the same time, non-state (commercial) parties are becoming increasingly important for the development of new technology. Large technology companies like SpaceX, Meta and Alphabet (Google) now wield great economic and geopolitical power.[298]

Artificial intelligence

A good example of the above is the rapid development of generative AI. Since the introduction of ChatGPT in late 2022, many AI models have become available worldwide that are publicly accessible and can generate text, images, audio, video and deepfakes for free or relatively cheaply. Meanwhile, the United States and China are engaged in an AI tech race, with both countries investing heavily in AI development. At the same time these new AI applications are mainly being developed and marketed by big tech companies and that is creating new dependencies on those companies.[299] AI also amplifies existing threats to critical infrastructure, for example, by allowing malicious actors to use this technology to look for vulnerabilities in the digital systems of critical infrastructure and potentially launch cyberattacks on them.[300]

In addition to AI, robotics and autonomous systems are also becoming more widely available. Previously, such technologies used to be primarily owned by state actors, but now even non-state actors can use technologies such as commercially available drones and do-it-yourself kits for genetic modification (biotechnology) without having to spend too much money. As a result, these technologies can also be used by malicious actors such as criminals or terrorists.[301]

Space technology

In the field of space technology there are three developments which are relevant for national security. First of all , there is the militarisation of space. States such as China, the United States and Russia are integrating space into conventional military operations. There is also a lack of focus on the digital security of space technology. Satellites are used for a wide range of military and civilian applications, including GPS, earth observation and telecommunications. Any disruption of GPS can, for example, have disruptive supply chain effects on critical infrastructure. However, there is little understanding of the potential vulnerabilities of space infrastructure. Finally, an increasing number of commercial parties are operating in space and this will (potentially) create new dependencies on commercial parties.[302]

Quantum technology

Applications of quantum technology are still in their infancy, so the potential impact is still partly unknown. However, from a national security perspective, it is essential to start anticipating the effects of all manner of quantum technology applications. The advent of the quantum computer is particularly relevant to critical infrastructure.[303] The expectation is that it will be possible to use such computers to break current cryptographic standards, allowing protocols and sensitive data that are now well protected with encryption to be decrypted after all in times to come.[304] Quantum computers therefore have the potential to cause disruption or failure of critical processes in the future. It is not yet clear when this technology will be capable of this, but for some parties it is already important to start implementing post-quantum cryptography.[305] Encrypted data that is intercepted and stored now could potentially be decrypted later using a quantum computer and that means that a future powerful quantum computer already poses a risk to national security.[306]

6.3 Energy transition

The energy transition, which involves reducing energy demand, phasing out fossil fuels and increasing the use of renewable energy sources, may have implications for critical infrastructure. As more and more businesses and households switch to electricity, available capacity is not keeping up with demand. This will put pressure on the security of supply and may increase the number of power cuts at regional level due to a lack of grid capacity. Increasing reliance on solar and wind power is also affecting security of supply. Insufficient supplies of solar and wind power over a long period of time need to be compensated with other energy sources such as hydrogen or biomass.[307]

The impact of the energy transition on critical infrastructure and its interconnectedness is very evident in the close relationship between energy facilities and digital infrastructure. Electricity grid

usage is at such a high level in many places in the Netherlands that there is no capacity to connect new large-scale consumers in the coming years. However, it is essential that the electricity grid offers sufficient capacity at the local level in order for digital infrastructure to function. Additional electricity is, for example, needed to expand the 5g network and connect new homes to the digital infrastructure. At the same time, a reliable digital infrastructure is a prerequisite for the energy transition, as smart energy networks place high demands on digital connectivity.[308]

In addition, the energy transition requires large quantities of minerals and metals for which Europe is heavily dependent on countries such as China and the Democratic Republic of Congo. The supply of these materials could hamper the energy transition and, at the same time, Europe's dependency on them could be used as a means of applying geopolitical pressure.[309]

Lastly, the energy transition goes hand in hand with digitalisation and that makes the new energy infrastructure, in the form of, for example, smart meters and charging stations, vulnerable to digital attacks and acts of sabotage which target the grid.[310] Research by the Dutch Authority for Digital Infrastructure (*Rijksinspectie Digitale Infrastructuur*, RDI) shows that the explosive growth in the number of solar panel installations is being accompanied by an increase in malfunctions affecting these installations. The RDI investigated 9 inverters and none of them fulfilled the applicable cybersecurity standards. As a consequence, solar panel systems are easy to hack and can be disabled or used for DDoS attacks. In addition, five of the nine inverters, which convert the energy produced by a solar panel into AC voltage for the grid, were found to be capable of causing failures themselves.[311]

6.4 Shortages on the labour market

There are shortages on the labour market and that will continue to be the case for the foreseeable future due to an ageing population and flattening productivity growth.[312] Staff shortages can make critical providers less resilient to threats and, in an extreme case, can themselves cause disruption to or failure of critical processes.

The State Commission on Demographic Developments by 2050 describes in the report entitled Moderate growth (*Gematige groei*) that there will be a peak in Dutch population ageing in the next 10 to 15 years, which will result in a permanently 'older' society as we approach 2050.[313] According to research by McKinsey shortages on the labour market could triple to a shortage of 1.4 million people by 2030. Existing shortages will increase particularly in technical jobs, care and welfare.[314]

The shortage of staff with technical expertise may lead to critical infrastructure providers being unable to find sufficient numbers of qualified personnel. Critical providers may be unable to install state-of-the-art systems as a result, and there may also be problems in the long run if there is a lack of technical expertise for the operation and maintenance of systems. Human intervention is necessary in order to mitigate any disruption to automated processes, particularly in the event of an incident, for example when bridges and locks need to be manually controlled because automated controls become disrupted or fail. The increasing complexity and dependencies within systems also mean that specific knowledge and expertise is required to manage and maintain the systems and respond to incidents.[315]

The shortage of technical staff poses a latent threat that may result in an inability to maintain the resilience of critical infrastructure.[316] Back in July 2024, for instance, the Cyber Security Council warned in a letter to the Minister of Economic Affairs about the effects of shortages in the cybersecurity labour market on the Netherlands' digital resilience and strategic digital autonomy.[317] In addition, malicious actors may start identifying which organisations have the greatest shortages and potentially the weakest defences in order to target them.[318]

Ageing will even have a doubling effect in the care sector because the ageing population will mean that, on the one hand, fewer care staff will be available and, on the other, that more people will require care services.[319]

6.5 Economic developments

Economic developments worldwide can affect critical processes, for example in the form of price increases or trade restrictions imposed on critical suppliers in respect of raw materials. As a small, open economy within the Eurozone, the Netherlands remains vulnerable to international financial shocks and problems in other countries can have a significant impact on our economy. Banking crises or other problems affecting players on the financial markets, fiscal crises (in the Eurozone), trade disputes or the geopoliticisation of global trade can therefore have a relatively large impact on the Dutch economy.[320]

The global economy has become increasingly fragmented in recent years. According to the IMF, countries worldwide took more than 2,500 industrial policy measures in 2023, 70% of which are having a disruptive effect on trade. The Dutch economy is sensitive to this fragmentation because our economy is largely dependent on international trade. This makes the Netherlands vulnerable to disruptions in global supply chains and trade and capital restrictions.[321]



On the bottom of the North Sea lies a network of Internet cables and power cables from wind farms. An unmanned surface vessel helps ensure the safety of essential subsea infrastructure.

7. Conclusion

This threat landscape report shows that critical infrastructure faces an accumulation of diverse threats. In particular, hybrid attacks by state actors, including physical and digital sabotage, espionage and pre-positioning and abuse of strategic dependencies are a growing threat. The consequences of ever-accelerating climate change will also have an increasing and still partly unpredictable impact on critical infrastructure.

When these threats materialise in concrete events and critical processes lack sufficient resilience, the risk of disruption or failure arises. This risk factor is particularly increased when multiple threats, including human and system failures, occur simultaneously. National security may be compromised as well. Due to complex, ever-changing and sometimes hidden interdependencies, disruption of one critical process can also have major chain effects on other critical processes. What is more, several examples of (cyber) espionage and pre-positioning for sabotage have revealed that, even when there is no disruption or outage, malicious actors can attack the integrity and confidentiality of critical processes.

At the same time, often far-reaching political, economic, social and technological developments are causing the critical infrastructure itself, its resilience and the threats facing critical processes to change. This makes it even more important for national security to assess periodically the state of the triad of threats and the interests and resilience of critical processes.

Given that threats are constantly changing, it is important to keep relevant knowledge up to date. The NCTV is helping to do this by publishing products such as the State Actors Threat Assessment, the National Cybersecurity Assessment, the Terrorist Threat Assessment for the Netherlands and various thematic reports.

The threats described in this threat landscape report underline the importance of resilient critical infrastructure. This starts with an insight into the current resilience of critical processes, which will be interpreted using the resilience analyses that the government departments perform for each critical process. In doing so, they can use the conceptual framework developed in this threat landscape, along with the described threats, as a starting point.

Sources

1 'Rijksbrede Risicoanalyse Nationale Veiligheid' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022. https://www.nctv.nl/onderwerpen/vitale-infrastructuur
2 '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024. https://magazines.defensie.nl/defensiekrant/2022/41/03_hybride-dreiging-gas_41
3 https://www.nctv.nl/onderwerpen/vitale-infrastructuur/aanpak-vitaal
4 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
5 '*Tussenbalans van het Kennisprogramma Zeespiegelstijging*' (Mid-term review of the Sea Level Rise Knowledge Programme), Sea Level Rise Knowledge Programme, November 2023.
6 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
7 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024. '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
8 '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024.
9 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
10 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
11 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
12 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
13 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
14 https://www.nctv.nl/onderwerpen/vitale-infrastructuur
15 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2019.
16 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
17 'Resilience quantified A method for understanding resilience to threats to national security', RAND Europe, 2024.
18 https://www.nctv.nl/onderwerpen/vitale-infrastructuur.
19 'Resilience in turbulent times - Geopolitical risks and financial institutions', The Dutch Central Bank, November 2024.
20 Letter to parliament on Resilience to military and hybrid threats, 6 December 2024.
21 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
22 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024. 'The Netherlands in a Fragmenting World Order', The Netherlands Scientific Council for Government Policy (, WRR), 01-07-2024.
23 Letter to parliament on Resilience to military and hybrid threats, 6 December 2024.
24 *Jaarverslag AIVD 2022* (2022 AIVD Annual Report).
25 Questions by MPs Bontenbal and Boswijk (both from the Christian Democratic Alliance (*Christen Democratisch Appèl*, CDA) to the Ministers of Foreign Affairs and Defence on the article entitled 'Russia plotting sabotage across Europe, intelligence agencies warn', Ministry of Defence, 18 June 2024.
26 *Jaarverslag AIVD 2023* (2023 AIVD Annual Report).
27 '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024.
28 '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024.
29 '*Themarapportage ongewenste inmenging en beïnvloeding democratische rechtsstaat*' (Thematic Report on undesirable interference and influence on the democratic rule of law), National Security Analyst Network, July 2022.
30 '*Dreigingsbeeld militaire en hybride dreigingen*' (Military and Hybrid Threats Assessment), Ministry of the Interior and Kingdom Relations, AIVD and MIVD, December 2024.
31 Letter to parliament on Resilience to military and hybrid threats, 6 December 2024.
32 '*Dreigingsbeeld militaire en hybride dreigingen*' (Military and Hybrid Threats Assessment), Ministry of the Interior and Kingdom Relations, AIVD and MIVD, December 2024.
33 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
34 Letter to parliament on Resilience to military and hybrid threats, 6 December 2024.
35 State Actors Threat Assessment 2, AIVD, MIVD and NCTV, 2022.
36 Questions by MPs Bontenbal and Boswijk (both from the Christian Democratic Alliance (*Christen Democratisch Appèl*, CDA) to the Ministers of Foreign Affairs and Defence on the article entitled 'Russia plotting sabotage across Europe, intelligence agencies warn', Ministry of Defence, 18 June 2024.
37 'Russia plotting sabotage across Europe, intelligence agencies warn', Financial Times, 5 May 2024.
38 https://dataverse.harvard.edu/file.xhtml?fileId=10787750&version=2.0
39 'Chaos, Order and Power Politics HCSS Strategic Monitor 2025', HCSS, December 2024.
40 'German spying: 'Two men held over suspected Russian sabotage plot', BBC, 18 April 2024.

41 '*Drie Duits-Russische mannen beschuldigd voor sabotage en spionage in opdracht van Rusland*' (Three German-Russian men accused of sabotage and spying on behalf of Russia), Het Laatste Nieuws, 2 January 2025.
42 'Two British men charged with helping Russian intelligence', BBC, 26 April 2024.
43 '*Rusland zit achter reeks branden bij DHL-depots in Europa*' (Russia behind series of fires at DHL depots in Europe) NRC, 6 November 2024.
44 '*CNN: Rusland wilde topman van Duitse wapenfabrikant vermoorden*' (Russia wanted to kill CEO of German arms manufacturer), NOS, Thursday 11 July 2024.
45 https://english.radio.cz/czech-minister-tells-financial-times-russia-trying-sabotage-critical-8813329
46 '*Eemshaven militair terrein: en dan?*' (Eemshaven a military site: and then what?), Dagblad van het Noorden, 4 January 2025.
47 '*Nederlands spoor speelt cruciale rol in snelle mobilisatie NAVO, maar achterstallig onderhoud is groot probleem*' (Dutch rail plays crucial role in NATO rapid mobilisation, but overdue maintenance is a big problem), De Telegraaf, 21 April 2024. https://www.defensie.nl/onderwerpen/internationale-samenwerking/host-nation-support
48 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
49 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
50 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
51 '*Europa kwetsbaar voor sabotage*' (Europe vulnerable to sabotage), Reformatorisch Dagblad, 22 November 2024.
52 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
53 '*Duitse autoriteiten op het punt aanslagplegers Nord Stream te arresteren, dubieuze rol voor Polen*' (German authorities about to arrest Nord Stream attackers, with Poland playing a dubious role), Volkskrant, 14 August 2024.
54 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
55 '*Lek in gaspijplijn tussen Finland en Estland, Finse president spreekt van 'externe activiteit'* (Leak in gas pipeline between Finland and Estonia, Finnish president claims 'external activity'), NRC, 10 Oct 2023.
56 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024. 'A Chinese ship remains the focus of the investigation into Baltic Sea gas pipeline damaged last year', APnews, 25 April 2024.
57 'Kabelbreuken in Rode Zee mogelijk werk van Houthi-strijders' (Cable breakages in Red Sea possibly work of Houthi fighters), NRC, 27 February 2024.
58 '*Europa kwetsbaar voor sabotage*' (Europe vulnerable to sabotage), Reformatorisch Dagblad, 22 November 2024.
59 '*Saboteerden Russen stroomkabel Oostzee? 5 vragen over de Estlink 2*' (Did the Russians sabotage Baltic Sea power cable? 5 questions about the Estlink 2) De Telegraph, 26 December 2024.
60 '*Kapotvaren glasvezelkabel in Oostzee geen sabotage maar 'ongelukje''* (Broken fibre-optic cable in Baltic not sabotage but 'accident'), Volkskrant, 3 February 2025.
61 Letter to parliament on the report entitled 'Inventory of Vulnerabilities relating to Satellite Navigation Outage' (*Rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie*), Ministry of Infrastructure and Water Management, 7 March 2023.
62 '*Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023* (Annual publication by the Civil Aviation Incident Analysis Department 2023), Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport*, ILT), 15 August 2024.
63 '*Met grootschalige gps-jamming bereikt elektronische oorlogsvoering ook de NAVO-landen*' (Thanks to large-scale GPS jamming, electronic warfare is also affecting NATO countries) de Volkskrant, 14 March 2024.
64 '*De wereld draait op tijd. Maar dan moeten we wel exact weten hoe laat het is*' (The world keeps turning on time, but then we still need to know exactly what time it is), De Correspondent, 5 December 2024.
65 '*Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023*' (Annual publication by the Civil Aviation Incident Analysis Department 2023), Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport*, ILT), 15 August 2024.
66 '*Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten*' (False GPS signals mislead passenger planes over Middle East) NOS, 16 March 2024.
67 '*Jaarpublicatie Analysebureau Luchtvaartvoorvallen 2023* (Annual publication by the Civil Aviation Incident Analysis Department 2023), Human Environment and Transport Inspectorate (*Inspectie Leefomgeving en Transport*, ILT), 15 August 2024.
68 https://nos.nl/regio/noord-holland/artikel/597792-extreme-toename-van-meldingen-over-verstoring-gps-signaal-in-nederlandse-cockpits
69 '*Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten*' (False GPS signals mislead passenger planes over Middle East) NOS, 16 March 2024.
70 https://www.navnin.nl/new/2024/09/26/verslag-van-de-workshop-gnss-jamming-en-spoofing-op-12-09-2024/
71 https://www.marinelink.com/blogs/blog/finland-detects-jamming-of-satellite-navigation-and-spoofing-on-102058 https://www.reuters.com/world/europe/finland-warns-hostile-activities-by-russia-2024-10-23/
72 *Finland merkt verstoring van navigatiesignalen en 'spoofing' op zee*: '*Schepen verdwalen*' (Finland is noticing disruption of navigation signals and 'spoofing' at sea: Ships are getting lost), Het Laatste News, 31 October 2024.
73 GPS Spoofing, OPSGROUP, 6 September 2024. '*Valse gps-signalen misleiden passagiersvliegtuigen boven Midden-Oosten*' (False GPS signals mislead passenger planes over Middle East), NOS, 16 March 2024.
74 GPSJAM GPS/GNSS Interference Map
75 'America's Asymmetric Vulnerability to Navigation Warfare: 'Leadership and Strategic Direction Needed to Mitigate Significant Threats', Marc J. Berkowitz, 18 July 2024.
76 Letter to parliament on the report entitled 'Inventory of Vulnerabilities relating to Satellite Navigation Outage' (*Rapport Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie*), Ministry of Infrastructure and Water Management, 7 March 2023. https://www.dlr.de/en/media/videos/2021/video-what-would-a-day-without-space-look-like https://www.strict.nl/blog/inzicht-in-gps-jamming-en-spoofing-toepassingen-gevolgen-en-maatregelen
77 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
78 *Jaarverslag MIVD 2023* (2023 MIVD Annual Report).
79 Letter to Parliament on the progress being made with regard to the Strategy to Protect North Sea Infrastructure, Ministry of Infrastructure and Water Management, 10 June 2024.
80 Letter to Parliament on the progress being made with regard to the Strategy to Protect North Sea Infrastructure, Ministry of Infrastructure and Water Management, 10 June 2024.
81 *Jaarverslag MIVD 2023* (2023 MIVD Annual Report).
82 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
83 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
84 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
85 'Cybersecuritybeeld Nederland 2023' (National Cybersecurity Assessment 2023)', NCTV, 3 July 2023.
86 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
87 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
88 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.

89 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
90 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
91 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
92 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
93 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
94 *Jaarverslag AIVD 2023* (2023 AIVD Annual Report).
95 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
96 '*MIVD onthult werkwijze Chinese spionage in Nederland' (MIVD reveals modus operandi of Chinese espionage in the Netherlands)*', Ministry of Defence, 6 February 2024..
97 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
98 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
99 'FBI shuts down China's 'Volt Typhoon' hackers targeting U.S. infrastructure', CNBS, 31 January 2024.
100 https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-peoples-republic-china-prc-targeting-commercial-telecommunications
'Chinese hackers are deep inside America's telecoms networks', The Economist, 12 December 2024.
101 'U.S. Wiretap Systems Targeted in China-Linked Hack', The Wall Street Journal, 5 October 2024.
102 https://www.defensie.nl/actueel/nieuws/2024/09/05/mivd-waarschuwt-russen-hebben-het-gemunt-op-westerse-hulp-aan-oekraine
103 '*Cybersecuritybeeld Nederland 2023*' (National Cybersecurity Assessment 2023), NCTV, 3 July 2023.
104 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
105 'Hacking the Cosmos: Cyber operations against the space sector. A case study from the war in Ukraine, Center for Security Studies - ETH Zurich, October 2024.
106 '*Pro-Russische groep legt websites Nederlandse havens plat*' (Pro-Russian group takes down Dutch ports websites), RTL News, 14-06-2023.
107 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
108 https://therecord.media/cyber-army-russia-us-sanctions
109 *Jaarverslag AIVD 2023* (2023 AIVD Annual Report).
110 '*Albanië verbreekt diplomatieke banden met Iran na cyberaanval*' (Albania cuts diplomatic ties with Iran after cyberattack), NOS, 8 September 2022.
111 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
112 https://www.nctv.nl/onderwerpen/desinformatie
113 'Resilience in turbulent times - Geopolitical risks and financial institutions', The Dutch Central Bank, November 2024.
114 'Resilience in turbulent times - Geopolitical risks and financial institutions', The Dutch Central Bank, November 2024.
115 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
116 Letter to parliament on China policy developments, a shift in the balance, 13 January 2023. '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024.
117 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
118 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
119 'Fasten your seatbelts: How to manage China's economic coercion', MERICS, 25-08-2022.
120 'China's economic coercion. Evolution, characteristics and countermeasure', European Parliamentary Research Service, November 2022.
121 'China's use of export controls, International Institute for Strategic Studies', 27 February 2025.
122 '*Groene zonnepanelen uit Nederland: China's bijna-monopolie op zonne-energie*' (Green solar panels from the Netherlands: China's almost total monopoly on solar power), De Groene Amsterdammer, 12 June 2024.
123 '*Ons leger loopt gevaar'; Nederland dreigt productie ijzersterke vezel te verliezen aan Chinese concurrentie: 'Strategisch risico'* ('Our army is at risk'. The Netherlands risks losing production of high tensile strength fibre to Chinese competition: 'Strategic Risk'), De Telegraaf, 9 November 2024.
124 '*Strategische Monitor 2023: Barsten en Blokken*' (The Strategic Monitor 2023: Cracks and Blocks: Confrontation and Cooperation in a World of Changing Coalitions) Clingendael and HCSS, January 2024.
125 'China's use of export controls, International Institute for Strategic Studies', 27 February 2025.
126 '*Strategische Monitor 2023: Barsten en Blokken*' (The Strategic Monitor 2023: Cracks and Blocks: Confrontation and Cooperation in a World of Changing Coalitions) Clingendael and HCSS, January 2024.
127 '*Strategische Monitor 2023: Barsten en Blokken*' (The Strategic Monitor 2023: Cracks and Blocks: Confrontation and Cooperation in a World of Changing Coalitions) Clingendael and HCSS, January 2024.
128 Letter to parliament on China policy developments, a shift in the balance, 13 January 2023.
129 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
130 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
131 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
132 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
133 Letter to parliament on China policy developments, a shift in the balance, 13 January 2023.
134 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
135 '*Nederland te afhankelijk van Rusland voor nucleaire medicijnen*' (The Netherlands too dependent on Russia for nuclear medicine), NOS, 22 August 2024.
136 '*Competitie tussen grootmachten en maatschappelijke stabiliteit in Nederland. De risico's van Russisch gas, Chinese grondstoffen en Taiwanese chips voor vitale-sectoren.*' (Great power competition and social stability in the Netherlands: The risks of Russian gas, Chinese raw materials and Taiwanese chips to vital sectors), The Hague Centre for Strategic Studies, April 2023.
137 https://ibestuur.nl/artikel/als-het-gaat-om-digitale-technologie-zijn-we-te-afhankelijk/
138 Annual report and final budget of the Ministry of Economic Affairs and Climate Policy (*Ministerie van Economische Zaken en Klimaat*) 2023. *Agenda Digitale Open Strategische Autonomie* (Digital Open Strategic Autonomy Agenda)

139 'Too late to act? Europe's quest Policy Brief for cloud sovereignty', Clingendael, March 2024.
140 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
141 '*DNB: burgers moeten beseffen dat financiële dienstverlening uit kan vallen*' (The public has to realise that financial services could fail), NRC, 21 October 2024.
142 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
143 *Versterkte dreigingen in een wereld vol kunstmatige intelligentie* (Increased threats in a world full of artificial intelligence), NCTV, AIVD and MIVD, December 2024.
144 Agenda Digitale Open Strategische Autonomie (Digital Open Strategic Autonomy Agenda)
145 *Versterkte dreigingen in een wereld vol kunstmatige intelligentie* (Increased threats in a world full of artificial intelligence), NCTV, AIVD and MIVD, December 2024.
146 'Terrorist Threat Assessment for the Netherlands December 2024', NCTV, December 2024.
147 Terrorist Threat Assessment for the Netherlands, June 2024.
148 https://monitoring.bbc.co.uk/product/b00036gf
149 'Terrorist Threat Assessment for the Netherlands 55', NCTV, October 2021. 'Terrorist Threat Assessment for the Netherlands 57', NCTV, November 2022.
150 'Terrorist Threat Assessment for the Netherlands December 2023', NCTV, December 2023.
151 'Terrorist Threat Assessment for the Netherlands December 2024', NCTV, December 2024.
152 '*Kosten van stroomstoring bij Tesla-fabriek lopen 'in de negen cijfers''* (Cost of power outage at Tesla factory runs 'into nine figures'), NOS, 5 March 2024.
153 'Terrorist Threat Assessment for the Netherlands December 2024', NCTV, December 2024.
154 '*Extreemlinkse activist gearresteerd na sabotage spoorwegen Frankrijk*' (Extreme left activist arrested after sabotaging railways France), NOS, 29 July 2024.
155 '*Glasvezelnetwerken gesaboteerd in Frankrijk, Olympische Spelen niet gehinderd*' (Fibre-optic networks sabotaged in France, Olympics not affected), Trouw, 29 July 2024.
156 '*Raadselachtige sabotage treft internet in Frankrijk*: '*Een incident op deze schaal is nog nooit gebeurd*'' (Mysterious incident of sabotage targets Internet in France: An incident on this scale has never happened before), De Volkskrant, 27 April 2022.
157 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
158 The Far-Right's Fascination with the U.S. Electric Grid, UNICORN RIOT, 19 December 2022
159 'Terrorist Threat Assessment for the Netherlands June 2024', NCTV, June 2024. *Jaarverslag MIVD 2023* (2023 MIVD Annual Report).
160 '*Met de rug naar de samenleving Een analyse van de soevereinenbeweging in Nederland*' (Turning its back on society - An analysis of the sovereignty movement in the Netherlands), AIVD, Nationale Police and the NCTV, 9 April 2024.
161 'Terrorist Threat Assessment for the Netherlands December 2024', NCTV, December 2024.
162 '*Ruim 200 klimaatactivisten gearresteerd op Schiphol, alle actievoerders weg*' (Over 200 climate activists arrested at Schiphol Airport, all activists have left), Nos, 5 November 2022.
163 '*Noodverordening Maastricht Airport verlengd na protest Extinction Rebellion*' (Maastricht Airport emergency ordinance extended after Extinction Rebellion protest), NOS, 9 March 2024.
164 '*Bijna 100 klimaatbetogers opgepakt na actie voorbij controles Schiphol*' (Nearly 100 climate protesters arrested following protest after they had passed through Schiphol security control), NOS, December.
165 '*200 Flugausfälle nach Kleber-Attacke in Frankfurt*' (200 flight cancellations after superglue protest in Frankfurt), Neue Presse, 26 July 2024., *Flughafen Frankfurt lahmgelegt*' (Frankfurt Airport paralysed), Frankfurter Neue Presse, 26 July 2024.
166 *Politiker reagieren empört auf Flughafen-Blockade* (Politicians respond to airport blockade with indignation), Tagesschau, 18 May 2024.
167 https://www.rijnmond.nl/nieuws/1853646/extinction-rebellion-weggestuurd-bij-haven-rotterdam-parallelbaan-a15-weer-open
168 https://www.rijnmond.nl/nieuws/1884672/demonstratie-op-de-botlekbrug-is-slechts-het-begin-zeggen-activisten
169 '*Extinction Rebellion blokkeert opnieuw doorgang cruiseschip IJmuiden, gemeente ontbindt actie*' (Extinction Rebellion again blocks passage of cruise ships at IJmuiden, the municipality manages to bring the protest to an end), Trouw, 11 August 2024.
170 '*Greenpeace-activisten bezetten boorplatform bij Schiermonnikoog*' (Greenpeace activists occupy drilling platform near Schiermonnikoog), NOS News, Tuesday 4 June 2024.
171 https://nos.nl/artikel/2518386-blokkade-extinction-rebellion-beeindigd-a10-is-weer-vrij *Zijn er staatsrechtelijke blokkades op de snelweg voor demonstranten?* (Can demonstrators be prevented from blocking railways under the constitution?) | Erasmus University Rotterdam (eur.nl)
172 https://www.rtvoost.nl/nieuws/2311207/boeren-voeren-met-branden-en-blokkades-actie-zo-zag-dat-er-maandagavond-uit https://www.rtl.nl/nieuws/artikel/5317581/boerenprotesten-traktoren
173 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
174 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
175 '*Grootste cyberaanval' op Deense vitale infrastructuur raakte 22 energiebedrijven´* ('Massive cyberattack' on Danish critical infrastructure affected 22 energy companies, security.nl, 14 November 2023.
176 '*Grootste cyberaanval' op Deense vitale infrastructuur raakte 22 energiebedrijven´* ('Massive cyberattack' on Danish critical infrastructure affected 22 energy companies, security.nl, 14 November 2023.
177 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024.
178 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024. https://www.security.nl/posting/789992/Maritiem+dienstverlener+Royal+Dirkzwager+getroffen+door+ransomware
179 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
180 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
181 'Russian crime group behind London hospitals cyberattack, says expert', The Guardian, 5 June 2024.
182 'Ransomware attack on major US blood centre prompts hundreds of hospitals to implement shortage protocols', The Reford, 31 July 2024.
183 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
184 https://www.portofrotterdam.com/nl/bouwen-aan-de-haven/veilige-haven/ondermijning
185 https://www.prorail.nl/veelgestelde-vragen/waarom-is-koperdiefstal-zo-n-probleem-op-het-spoor
186 '*Aantal koperdiefstallen op het spoor vorig jaar drastisch afgenomen*' (Number of thefts of copper along the railway lines decreased dramatically last year), nu.nl, 9 January 2023.
187 https://www.bnr.nl/nieuws/bouw-infrastructuur/10546386/koperdiefstal-zonneparken-indirecte-kosten-zijn-een-groot-probleem
188 For guidelines on how to deal with insider threats in the cyber domain, see: 'Omgaan met insider threats' (Dealing with insider threats), National Cyber Security Centrum, 28 February 2024.
189 Insider Risk Trend Report 2025, Signpost Six, January 2025.
190 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
191 'Climate Change 2023 Synthesis report.', IPCC. 2023.

192 'Klimaatrisico's in Nederland; De huidige stand van zaken.' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
193 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022. '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
194 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022. '*Klimaatrisico's in Nederland: De huidige stand van zaken*.' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
195 '*Klimaatrisico's in Nederland: De huidige stand van zaken*' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
196 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
197 '*Klimaatrisico's in Nederland: De huidige stand van zaken*' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
198 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024.
199 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
200 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
201 Royal Netherlands Meteorological Institute (*Koninklijk Nederlands Meteorologisch Instituut*, KNMI). (9 October 2023). KNMI'23 climate scenarios for the Netherlands. Available at: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
202 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
203 Royal Netherlands Meteorological Institute (*Koninklijk Nederlands Meteorologisch Instituut*, KNMI). (9 October 2023). KNMI'23 climate scenarios for the Netherlands. Available at: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
204 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
205 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
206 '*Juli 2021 overstroming en wateroverlast in Zuid-Limburg*' (July 2021 waterlogging and flooding in South Limburg), Deltares, 26 April 2022.
207 https://www.knmi.nl/over-het-knmi/nieuws/waarom-viel-er-de-afgelopen-dagen-zoveel-regen-in-spanje
208 '*Bizar, maar dit is slechts het begin, minder wordt het niet*' (Bizarre, but this is just the beginning, it is only going to get worse), Algemeen Dagblad, 2 November 2024.
209 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
210 *KNMI: klimaatverandering wordt meer voelbaar, valwind als in Leersum gaat vaker voorkomen* (Climate change is becoming more and more tangible and katabatic winds like the one that occurred in Leersum will occur more and more frequently) RTV Utrecht regional television broadcaster, 25 October 2021.
211 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
212 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
213 https://www.rtl.nl/nieuws/nederland/artikel/5237270/kabels-hoogspanningsmast-boerderij-vluchten-valwind
214 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024. 'Letter to Parliament on the Future of Inland Navigation', Ministry of Infrastructure and Water Management, 30 November 2022.
215 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
216 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024.
217 '*Tussenbalans van het Kennisprogramma Zeespiegelstijging*' (Mid-term review of the Sea Level Rise Knowledge Programme), Sea Level Rise Knowledge Programme, November 2023.
218 '*Deltascenarios-2024 - Zicht op water in Nederland*' (Delta Scenarios 2024 - An insight into water in the Netherlands), Deltares, April 2024.
219 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024.
220 https://www.rivm.nl/nieuws/snel-actie-nodig-om-drinkwatertekort-in-2030-te-voorkomen
221 '*Als er niets gebeurt, is straks overal een watertekort. Zo moet het water uit de kraan drinkbaar en betaalbaar blijven*' (If nothing is done there will soon be water shortages everywhere. Tap water has to remain drinkable and affordable), NRC, 12 January 2025.
222 https://www.nieuwsienw.nl/home_old1717146098/2966196.aspx
223 'Letter to Parliament on the Future of Inland Navigation', Ministry of Infrastructure and Water Management, 30 November 2022.
224 https://www.rijkswaterstaat.nl/water/waterbeheer/droogte-en-watertekort/verdeling-water-bij-droogte
225 https://www.onswater.nl/actueel/nieuws/2023/07/19/droogte-zorgt-voor-problemen-voor-nederlandse-dijken
226 The railways - Climate adaptation
227 https://www.europoortkringen.nl/chemie-informeert-rijk-over-impact-droogte/
228 '*Natuurbrandsignaal '23*' (Wildfire Report '23), Netherlands Institute of Public Safety, 23 January 2023.
229 'Letter to parliament on progress towards an integral approach to wildfire management', Ministry of Agriculture, Nature and Food Quality (*Ministerie van Landbouw, Natuur en Voedselkwaliteit*), 13 June 2024.
230 '*Natuurbrandsignaal '23*' (Wildfire Report '23), Netherlands Institute of Public Safety, 23 January 2023.
231 '*Natuurbrandsignaal '23*' (Wildfire Report '23), Netherlands Institute of Public Safety, 23 January 2023.
232 '*Natuurbrandsignaal '23*' (Wildfire Report '23), Netherlands Institute of Public Safety, 23 January 2023.
233 Royal Netherlands Meteorological Institute (*Koninklijk Nederlands Meteorologisch Instituut*, KNMI). (9 October 2023). KNMI'23 climate scenarios for the Netherlands. Available at: https://www.knmi.nl/research/ publications/knmi-23-klimaatscenario-s-voor-nederland
234 '*Tussenbalans van het Kennisprogramma Zeespiegelstijging*' (Mid-term review of the Sea Level Rise Knowledge Programme), Sea Level Rise Knowledge Programme, November 2023.
235 '*Tussenbalans van het Kennisprogramma Zeespiegelstijging*' (Mid-term review of the Sea Level Rise Knowledge Programme), Sea Level Rise Knowledge Programme, November 2023.
236 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
237 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
238 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
239 *Themarapportage klimaat- en natuurrampen* (Thematic report on climate and natural disasters), The National Network of Safety and Security Analysts, 2022.
240 https://www.knmi.nl/over-het-knmi/nieuws/jaaroverzicht-aardbevingen-2024
241 '*Uitleg over Ruimteweer*' (Explanation of Space Weather), KNMI.
242 '*KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven*' (KNMI investigates effects of space weather on our daily lives), KNMI, 9 May 2022.
243 https://magazines.defensie.nl/vliegendehollander/2015/05/ruimteweer

244 '*KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven*' (KNMI investigates effects of space weather on our daily lives), KNMI, 9 May 2022.
245 https://www.knmi.nl/over-het-knmi/nieuws/geomagnetische-storm-verwacht-door-uitbarsting-op-de-zon
246 '*KNMI onderzoekt effecten van ruimteweer op ons dagelijks leven*' (KNMI investigates effects of space weather on our daily lives), KNMI, 9 May 2022.
247 'SpaceX to lose up to 40 Starlink satellites after geomagnetic storm', the Guardian, 9 February 2022.
248 https://www.knmi.nl/over-het-knmi/nieuws/geomagnetische-storm-verwacht-door-uitbarsting-op-de-zon
249 https://www.knmi.nl/over-het-knmi/nieuws/knmi-onderzoekt-effecten-van-ruimteweer-op-ons-dagelijks-leven
250 https://www.newscientist.nl/nieuws/krachtige-zonnevlam-veroorzaakte-tijdelijke-radiostoring/
251 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022. https://www.nctv.nl/onderwerpen/vitale-infrastructuur
252 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
253 '*WHO slaat alarm over vogelgriep, al is kans op nieuwe pandemie klein*' (WHO sounds alarm over bird flu, even though the chance of a new pandemic is small), NOS, 21 April 2024.
254 '*Kans op nieuwe pandemie, Amerikaanse aanpak vogelgriep één groot gokspel*' (New pandemic possible, US approach to bird flu one big guessing game), NOS. 11 January 2025.
255 '*Bij een nieuwe pandemie is er in Nederland weer een tekort aan IC's en tests*' (If a new pandemic were to occur, the Netherlands would once again be short of ICUs and tests), NRC, 22 February 2024.
256 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
257 '*OpenAI: geringe kans dat ChatGPT recept geeft voor biologische wapens*' (OpenAI: slim chance of ChatGPT providing a recipe for biological weapons), RTL News, 01-02-2024, https://www.rtlnieuws.nl/economie/artikel/5432595/kleine-kans-dat-openai-recept-geeft-voor-biologische-wapens 'Capabilities and risks from frontier AI: A discussion paper on the need for further research into AI risk', AI Safety Summit, October 2023.
258 'Capabilities and risks from frontier AI: A discussion paper on the need for further research into AI risk', AI Safety Summit, October 2023.
'The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study.' Mouton, Christopher A., Caleb Lucas, and Ella Guest (RAND Corporation), 2024. https://www.rand.org/pubs/research_reports/RRA2977-2.html.
259 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
260 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
261 '*Benut grootste computerstoring ooit als leerzame brandoefening*' (Use the biggest computer failure ever as an educational fire drill), NRC Handelsblad, 27 July 2024.
262 *Over de hele wereld is er hinder van de computerstoring. Wat is er aan de hand, en hoe kan het opgelost worden?*' (Computers are failing all over the world. What is going on and how can it be resolved?), NRC Handelsblad, 19 July 2024.
263 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
264 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
265 https://nos.nl/artikel/2535038-extra-schepen-vliegtuig-en-inzet-politie-hielpen-kustwacht-storing-door
266 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
267 'Letter to parliament on the status of the renewal and replacement of C2000 in the summer of 2023', Ministry of Justice and Security, 14 June 2023.
268 '*Frustratie over hapering communicatiesysteem politie*: '*Problemen spelen al jaren*'' (Frustration at malfunctioning police communication system: 'There have been problems for years'), NOS, 2 January 2025.
269 *Storing luchtverkeersleidingssysteem*(Air traffic control system malfunction)
270 '*Storing luchtverkeersleiding wordt extern onderzocht*' (Air traffic control failure under external investigation), NOS, 25 April 2024.
271 '*Klimaatrisico's in Nederland: De huidige stand van zaken*' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
272 'Spoorwegongeval Voorschoten' (Railway accident at Voorschoten), Dutch Safety Board, May 2024.
273 '*Klimaatrisico's in Nederland: De huidige stand van zaken*' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
274 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
275 '*Klimaatrisico's in Nederland: De huidige stand van zaken*' (Climate risks in the Netherlands: The current state of affairs), Netherlands Environmental Assessment Agency, 14 May 2024.
276 '*Nationaal Crisisplan Elektriciteit*' (National Electricity Crisis Plan), Ministry of Economic Affairs and Climate, February 2022.
277 '*Nationaal Crisisplan Elektriciteit*' (National Electricity Crisis Plan), Ministry of Economic Affairs and Climate, February 2022.
278 '*Nationaal Crisisplan Elektriciteit*' (National Electricity Crisis Plan), Ministry of Economic Affairs and Climate, February 2022.
279 '*Nationaal Crisisplan Elektriciteit*' (National Electricity Crisis Plan), Ministry of Economic Affairs and Climate, February 2022.
280 '*Nationaal Crisisplan Elektriciteit*' (National Electricity Crisis Plan), Ministry of Economic Affairs and Climate, February 2022.
281 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
282 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
283 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
284 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
285 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022. 'The Netherlands in a Fragmenting World Order', The Netherlands Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*, WRR), 01-07-2024.
286 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
287 'The Netherlands in a Fragmenting World Order', The Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid, WRR), 01-07-2024.
288 '*De staat van de digitale infrastructuur. De ruggengraat van onze digitale economie.*' (The state of the digital infrastructure. The backbone of our digital economy), Ministry of Economic Affairs and Climate Policy, January 2024.
289 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.

290 'New Technologies, Changing Strategies: 'Five Trends in the Hybrid Threat Landscape', HCSS & TNO, May 2024.
291 Invisible frontlines Safeguarding the European Energy Infrastructure, Danish Institute for International Studies, 2024.
292 '*Hybride dreigingen en maatschappelijke weerbaarheid*' (Hybrid threats and societal resilience), Advisory Council on International Affairs, 04-06-2024.
293 '*DNB: burgers moeten beseffen dat financiële dienstverlening uit kan vallen*' (The public has to realise that financial services could fail), NRC, 21 October 2024.
294 '*Cybersecuritybeeld Nederland 2023*' (National Cybersecurity Assessment 2023), NCTV, 3 July 2023.
295 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
296 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
297 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
298 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
299 PM: NCTV AI publication
300 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
301 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
302 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024.
303 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024.
304 '*Bereid je voor op de dreiging van quantum computers*' (Prepare for the threat of quantum computers), AIVD, September 2021. '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
305 '*Bereid je voor op de dreiging van quantum computers*' (Prepare for the threat of quantum computers), AIVD, September 2021. '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
306 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
307 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*' (National Security Trend Analysis 2024 - in-depth exploration), The National Network of Safety and Security Analysts, 2024.
308 '*De staat van de digitale infrastructuur. De ruggengraat van onze digitale economie.*' (The state of the digital infrastructure. The backbone of our digital economy), Ministry of Economic Affairs and Climate Policy, January 2024.
309 'Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
310 '*Trendanalyse Nationale Veiligheid 2024 – Verdieping op de Trendanalyse*', The National Network of Safety and Security Analysts, 2024. '*Nederlandse hacker kon 4 miljoenzonnepaneelsystemen in 150 landen overnemen*' (Dutch hacker was able to take over 4 million solar panel systems in 150 countries), Follow the Money, 12 August 2024.
311 '*Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen*' (Investigation into interference issues and cyber security inverters for solar panels), Dutch Authority for Digital Infrastructure, 23 May 2023.
312 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024. '*Bouwen aan een toekomstbestendige arbeidsmarkt*' (Building a future labour market that works), McKinsey, June 2024.
313 '*Gematigde groei*', (Moderate Growth) State Commission on Demographic Developments by 2050, January 2024.
314 '*Bouwen aan een toekomstbestendige arbeidsmarkt*' (Building a future labour market that works), McKinsey, June 2024.
315 '*Themarapportage bedreiging vitale infrastructuur*' (Thematic report on the threat to critical infrastructure), The National Network of Safety and Security Analysts, 2022.
316 '*Rijksbrede Risicoanalyse Nationale Veiligheid*' (National Risk Assessment of the Kingdom of the Netherlands), The National Network of Safety and Security Analysts, 2022.
317 '*CSR signaalbrief cybersecurity arbeidsmarkt*' (Notification Letter concerning the cyber security labour market), Cyber Security Council, 4 July 2024.
318 '*Cybersecuritybeeld Nederland 2024*' (National Cybersecurity Assessment 2024), NCTV, 28 October 2024.
319 '*Gematigde groei*', (Moderate Growth) State Commission on Demographic Developments by 2050, January 2024.
320 '*Trendanalyse Nationale Veiligheid 2024 – Hoofdrapport*' (National Security Trend Analysis 2024 - Main Report), The National Network of Safety and Security Analysts, 2024.
321 'Resilience in turbulent times - Geopolitical risks and financial institutions', The Dutch Central Bank, November 2024.

Publication
National Coordinator
for Security and
Counterterrorism (NCTV)
P.O. Box 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

More information
www.nctv.nl
info@nctv.minjenv.nl

Photos
ANP

August 2025