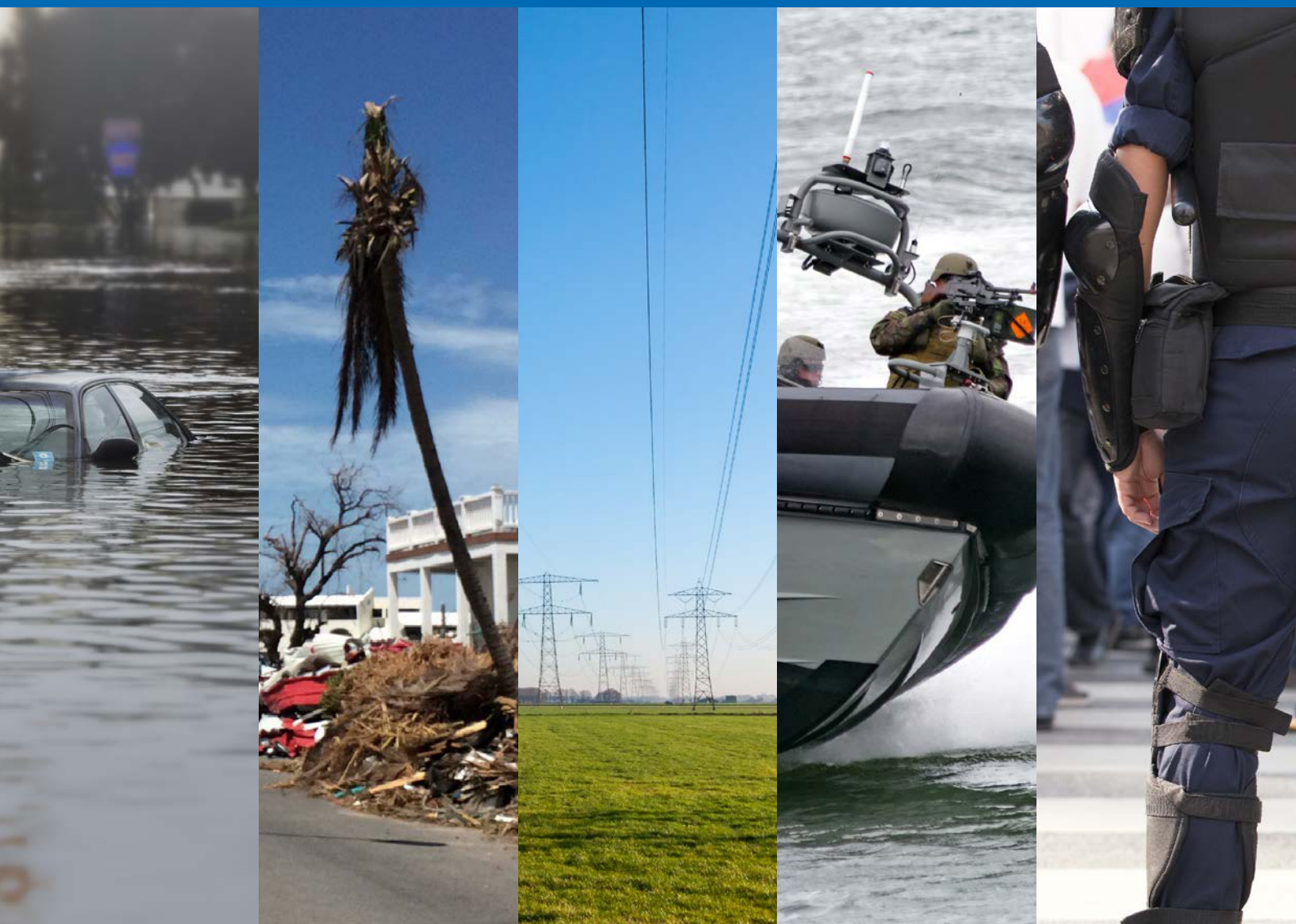
National Security Trend Analysis 2024

In-Depth Exploration of the Trend Analysis

National Network of Safety and Security Analysts



National Security Trend Analysis 2024

In-Depth Exploration of the Trend Analysis

National Network of Safety and Security Analysts

Publication details

This Trend Analysis has been compiled by the National Network of Safety and Security Analysts at the request of the NCTV.

The National Institute for Public Health and the Environment (RIVM)
The Netherlands Organisation for Applied Scientific Research (TNO)
The Netherlands Institute of International Relations 'Clingendael' (Clingendael)
SEO Amsterdam Economics (SEO)
The General Intelligence and Security Service (AIVD)
The Military Intelligence and Security Service (MIVD)
Research and Documentation Centre (*Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC*)

Contact: *anv@rivm.nl*

This publication contains the English translation of the *Trendanalyse Nationale Veiligheid 2024 – Verdieping*.
Please consult the Dutch language version for the original text.

Contents

Introduction

This In-Depth Exploration of the National Security Trend Analysis 2024 has been compiled by the National Network of Safety and Security Analysts (ANV) at the request of the National Coordinator for Counterterrorism and Security (NCTV). The Trend Analysis charts the most important developments for national security and thus serves as a foundation for updating the implementation of the Security Strategy for the Kingdom of the Netherlands. The Trend Analysis builds on the findings of the National Risk Assessment of the Kingdom of the Netherlands (NRA) that was prepared by the ANV in 2022 (ANV, 2022).

The National Security Trend Analysis consists of two parts:
- The Main Report;
- The In-Depth Exploration of the Trend Analysis.

The In-Depth Exploration of the Trend Analysis contains an overview of the developments for each of the ten threat themes discussed in the NRA (section A). This is followed by an overview of the developments in eight different technology areas with potential implications for national security (section B). This report also includes a further explanation of the methodology used (section C) and a brief introduction into the ANV (section D).

A summary and integral picture of the developments can be found in the Main Report, which also includes cross-thematic, strategic insights that emerge from the Trend Analysis. In addition, it discusses the possible implications for further strategy development.

Section A
Overview of developments per threat theme from the NRA

This section provides an overview of the key developments for each threat theme outlined in the National Risk Assessment (NRA).[1] Depending on the classification and content of the threat theme in question, the following topics are discussed for either the theme in its entirety or the underlying threat categories:

- The most important findings and conclusions from the Trend Analysis
- A general overview of the findings and state of affairs compared to the NRA
- A further explanation of the threat assessment based on possible developments

[1] Note: the topic of organised crime is not an individual threat theme in the NRA, but has been included as a separate theme here to match the classification used in the Security Strategy

A.1 Climate and natural disasters

Key findings and conclusions

As part of the theme of Climate and natural disasters, four types of threats that could affect national security have been analysed in the National Risk Assessment. These are floods, extreme weather events, wildfires and earthquakes. The NRA has previously identified that climate change has a major impact on these threats. Compared to the insights presented in the NRA, climate change continues to accelerate and may have greater effects than previously thought. As a result both the impact and likelihood of extreme weather events, floods and wildfires are increasing.

General overview of findings and state of affairs compared to NRA

Extreme weather events

The climate scenarios of the Royal Netherlands Meteorological Institute (KNMI, 2023) show that average temperatures in the Netherlands have continued to increase and will continue to rise even faster than anticipated. Higher temperatures translate into an increase in extreme weather events, such as extreme heat, drought and precipitation. The predictions for Dutch summers are particularly striking. Summers will get a lot hotter and the frequency and intensity of heat waves will increase (PBL, 2024). In a world that is 2 degrees warmer, summer heat in the Netherlands could reach 45 degrees Celsius around the year 2100. Due to the heat island effect, temperatures in cities, especially at night, are 5 degrees higher on average than in the countryside (KNMI, 2023; Nu.nl, 2023). Cities will therefore be the first to be confronted with the negative effects of the warming (EEA, 2022; Academische Werkplaats Gezonde Leefomgeving, 2023).

Heat waves are already the deadliest natural disasters worldwide and this will only get worse in the coming years (UN, 2023). No less than 31% of heat-related deaths in the Netherlands can be attributed to climate change. This corresponds to almost 250 deaths per year (RIVM, 2021). The higher temperatures at night are especially dangerous because the body has no chance to recover from the heat.

In addition to an increase in temperature, it may also become significantly drier than previously thought. According to the driest KNMI scenario, the average precipitation deficit in 2100 could be 79 percent greater than in the past thirty years (KNMI, 2023). In this driest scenario, an average summer in the future (in 2100) will be about as dry as an extremely dry summer today. At the same time, the number of heavy showers with a lot

of rainfall in a short time also increases (KNMI, 2023). The number of downpours per year in the Netherlands has almost doubled in a century. We see a shift towards showers that are heavier (more rain per shower) and more intense showers (more rain per time unit) (KNMI, 2023). In addition, wind gusts may become stronger during showers, the likelihood of fall winds increases and the largest hailstones are likely to become even larger.

Temperatures are also rising in the Caribbean part of the Kingdom of the Netherlands (hereinafter: the Kingdom). As a result, extremely high temperatures can be reached. For instance, the summer of 2023 was the hottest ever with temperatures between 40 and 50 degrees Celsius (Stamper, 2023). Such high temperatures can cause health damage. Loss of biodiversity can also occur. Fading corals are proof of this. On the other hand, the amount of *Sargassum* (choking seaweed), which pollutes beaches, is growing (Central Bank of Curaçao and Sint Maarten, 2023). Not only are temperatures going up, the wind will also blow harder and the total amount of rainfall is expected to decrease (KNMI, 2023). However, there will also be moments of extreme precipitation, such as in November 2022 when Bonaire suffered massive rainfall that flooded parts of the island (NOS, 2023). In the Windward Islands, the likelihood of severe hurricanes with lots of rain increases. The frequency of hurricanes of the heaviest category will increase to once every 20 to 34 years in the future (until 2050), compared to once every 39 years now (KNMI, 2023). The Leeward Islands are not directly hit by these hurricanes, which tend to follow a more northerly route. However, there are signs that their route will gradually move southwards. This means that the Leeward Islands will feel the effects of passing hurricanes (in the distance) more often, for instance through heavy rainfall. An increase in heavy rainfall can in turn lead to (an acceleration of) erosion. The more extreme temperatures, fading coral and polluted beaches can be a threat to residents and tourism. The Caribbean economy runs on tourism. Its decline would therefore have major economic consequences. In addition, coral die-off can also affect the fishing industry, as healthy corals are important hiding and breeding places for fish. In addition, climate-related natural disasters, such as hurricanes, can cause major financial losses and disrupt critical processes, society and the economy (Central Bank of Curaçao and Sint Maarten, 2023).

Floods

As described above, higher temperatures increase the chance and intensity of extreme weather events. The KNMI climate scenarios show that these events could become so extreme that the water system will probably no longer be able to cope (KNMI, 2023).

On the one hand, the number of heavy showers with a lot of rainfall in a short period of time is increasing. This also increases the risk of excess water and flooding. On the other hand, the Netherlands is becoming considerably drier, especially during the summer. This may lead to freshwater shortages for drinking water production, nature, agriculture, industry and other water consumers faster than originally anticipated. It is expected that the current freshwater buffer of the IJsselmeer will become insufficient more often than once every 5 years from 2050 onwards (KNMI, 2023). The Netherlands will thus face two opposing problems.

Apart from extreme weather events, the rising sea level will also affect the water system. Sea level rise will continue at an ever-faster pace (PBL, 2024). Currently the rise is a few millimetres per year, but this is expected to have increased to several decimetres per year (16 to 37 cm) by 2050. This increases the likelihood of flooding and thus the risk to people, their surroundings and the environment (KNMI, 2023). In the Caribbean part of the Kingdom, sea level rise poses a particular threat to the low-lying parts of the Leeward Islands. Incidentally, floods in this area (and vulnerability to them) are not only due to climate change. The removal of natural barriers such as mangroves, deforestation and large-scale construction projects in coastal areas also play a part.

Wildfires

Besides creating problems in the water system, higher temperatures also increase the risk of wildfires (PBL, 2024). The number and intensity of wildfires are increasing worldwide. In addition, the duration of the wildfire season has risen by 27% since 1979 (OECD, 2023). Due to the effects of climate change, the Netherlands will also face wildfires more frequently (KNMI, 2023). As drought and heat intensify each other, wildfire risk is increasing faster than climate change (NIPV, 2023). Also, wildfires are more and more often becoming intense fires that cannot be extinguished and the likelihood of several of such fires coinciding is increasing. This may create such great pressure on the firefighting system that the limits of firefighting capabilities are reached (NIPV, 2023).

Earthquakes

Earthquakes are not affected by climate change. For induced earthquakes, the most important development is that gas extraction in Groningen has been stopped as of October 2023. The Groningen field has been permanently closed as of 19 April 2024, which means that start-up during emergencies is no longer possible (Government of the Netherlands, 2024). Stopping gas extraction ensures that both the probability and strength of earthquakes will decrease. In recent years, the total number of earthquakes in Groningen has gone down. The largest number of

earthquakes with a magnitude greater than 1.5 was recorded in 2013 (30). The number was much lower in 2018 (15), 2019 (11), 2020 (16), 2021 (12), 2022 (12) and 2023 (9) (KNMI, 2024). However, a risk of earthquakes will continue to exist for a long time because of the pressure differences built up in the ground due to gas extraction. There are no known developments that influence the threat of natural earthquakes.

Explanation of threat assessment

The ever-accelerating climate change is affecting threats within multiple threat categories. These are extreme weather events, floods and wildfires. Their likelihood and impact are increasing.

Higher temperatures translate into more extreme weather events, such as extreme heat, drought and precipitation. On the other hand, the number of ice days is decreasing. Snowstorms are therefore less likely to occur. The higher temperatures also mean that the extreme weather events can become more severe and therefore haver greater impact. For example, the number of fatalities due to heat will increase in the coming years. In addition, exposure to UV radiation is going up, increasing the risk of chronic diseases such as skin cancer (PBL, 2024). Extremely high temperatures can also cause a lack of basic needs. Rising temperatures will create a freshwater shortage for drinking water production, nature, agriculture, industry and other water users sooner than anticipated. This can put pressure on the availability of drinking water and options for personal hygiene. Almost half of the people also have very few options in their home to cool off when it is persistently hot. This affects the availability of a safe living environment. In addition, due to the heat island effect, it can be up to 5 degrees warmer in cities than in rural areas. And it is precisely in the cities that many vulnerable groups of people can be found, for example in schools and hospitals. This can also affect the availability of a safe living environment, as well as the continuity of essential healthcare. When temperatures become so high that it is temporarily unsafe to go outside, people's daily lives will be disrupted. Going to school or work, using social facilities or doing grocery shopping may not be possible for a short period of time.

With regard to the water management system, the most striking prediction is that it could become extremely dry, but that there could be short bursts of very heavy rainfall as well. The Dutch water system must therefore be prepared for the impact of two threats that are at opposite ends of the spectrum. The impact of wildfires may increase due to the high probability of their occurrence combined with a further densification of the Netherlands. People will have to flee more often, direct and indirect damage and failure of critical infrastructure will become more common, and irreparable damage to flora and fauna will occur more frequently. In addition, people's health will be threatened more often (NIPV, 2023).

A.2 Infectious diseases

Key findings and conclusions

The situation for all developments described in the NRA remains largely unchanged. There have been no changes affecting national security. However, new technological developments within bioinformatics and AI will affect infectious disease risks now and in the future. Also, declining vaccination coverage may have implications for the population's immunity against a wide range of infectious diseases.

General overview of findings and state of affairs compared to NRA

The COVID-19 pandemic has made it clear that a pandemic of such magnitude impacts a wide range of national security interests. Since the pandemic, there has been an increase in research into high-risk pathogens worldwide. This heightens the risk of the intentional or unintentional release of one of these pathogens from a laboratory (Kaiser, 2023). Furthermore, outbreaks of the avian influenza virus (bird flu) remain relevant. Since an increasing number of animal species can become infected by the influenza virus, this may have consequences for the emergence of variants that can spread to humans.

A recent RIVM report (on vaccination coverage in 2022) shows a drop in the percentage of children who are vaccinated as part of the National Immunisation Programme. Moreover, the vaccination coverage has fallen below 90% for the first time in a long period (NOS, 2024). This means that several infectious diseases may make a comeback.[2] An explanation for the decline in vaccination coverage seems to be that more parents have a negative view of vaccination these days. Confidence in vaccines has declined, for example due to the COVID-19 pandemic. The decreasing vaccination coverage is cause for concern, since the risk of an outbreak of serious infectious diseases increases when the minimum vaccination coverage is not reached. In addition, the declining vaccination coverage is a trend that is seen in the last two years. Needless to say, if the vaccination coverage continues to fall, the likelihood of infectious disease outbreaks will further increase. Although the measures taken during the COVID-19 pandemic resulted in a sharp drop in the number of reported cases, we now see a slight upward trend in these number for many infectious diseases (RIVM, 2023a; RIVM, 2023b).

[2] An important note to make is that since 1 January 2022, it is no longer possible to share personal data without consent. Therefore, some vaccinations are reported anonymously. These anonymous reports are not included when determining the vaccination coverage, resulting in underreporting.

Technology can affect the risks posed by infectious diseases to national security in several ways. Thanks to developments in bioinformatics, infectious diseases and zoonoses can be diagnosed ever quicker. The further development of artificial intelligence might contribute to this in the future, for instance by lightning-fast DNA analysis of potential pathogens or pathogen monitoring of wastewater. A possible downside of such developments is that information on harmful agents and their production may well become more accessible to people with malicious intentions (see also section B.7 on biotechnology). However, production constraints related to funding, infrastructure and materials remain to exist (Carter, 2023). In addition, improvements in outbreak surveillance and modern techniques will make it easier to detect sources of food contamination early on, reducing the risk of crisis due to an outbreak. On the other hand, food and livestock are more often transported internationally and produced on a larger scale, which may actually increase such a risk.

Finally, a number of other developments may potentially affect national security. Monitoring for the presence of plant diseases in ornamental and food crops, for example, is ongoing. If a highly damaging variant, such as Tomato brown rugose fruit virus (ToBRFV) or Xylella fastidiosa, endangers food production, this could have an impact on national security. In addition, a side effect of the COVID-19 pandemic is the reduced spread of resistant bacteria and hence a decrease in their numbers. However, the situation seems to be returning to normal and a catch-up effect has been observed in 2023. Climate change might also lead to an increased risk of infectious diseases in the Netherlands, due to, for instance, new vectors settling more easily, viruses dividing faster or the presence of contaminated water. At present, however, other social, biological and economic factors still play a more important role (RIVM, 2024).

Explanation of threat assessment

The threat assessment for infectious diseases has not changed significantly from the one outlined in the NRA. A number of factors may increase the risk of an outbreak, though, such as the number of laboratories conducting research on high-risk pathogens and the increasing number of animal species that can become infected with the influenza virus. The influence of developments in technology, such as in bioinformatics and artificial intelligence, can have both positive and negative effects on the impact of infectious diseases on national security. The effects of an outbreak depend on the type of infection and the measures (that can be) taken. It is important to note here that the effects would probably be more severe in the Caribbean part of the Kingdom, because the measures that can be taken are more limited. People depend on imports for almost 100% of foodstuffs and medication. In addition, resources and (medical) capacity are lacking.

A.3 Major accidents

Key findings and conclusions

The state of affairs described in the NRA for the major accidents threat theme mostly remains current. However, some shifts have taken place with regard to radiation accidents in the context of the war in Ukraine. The probability of such accidents has been assessed at the beginning of the war by parties other than the ANV (RIVM, 2024). Compared to these earlier assessments, the risks are now generally considered to be lower. However, they are of course highly dependent on how the war progresses and the location and intensity of fighting or shelling (ANVS, 2023).

General overview of findings and state of affairs compared to NRA

As noted in the NRA, there have been relatively few developments in the field of radiation accidents in recent years. No recent studies have been published regarding accident scenarios for the Borssele nuclear power plant, for instance. However, a new specification of the accident scenarios is being prepared and expected to be published in late 2024. This means that the source terms and starting points will change. Should the decision be made to build one or more new nuclear power plants, it will still take many years before they will be operational.

Regarding potential accidents involving chemicals, the transport of hydrogen-rich energy carriers and CO_2 is expected to increase. Plans for hydrogen and CO_2 are in an advanced phase and are currently being implemented (Gasunie hydrogen network and Porthos CO_2 (Gasunie, 2024; Porthos, 2024)).[3] Another development, which has been going on for some time now, concerns the ageing of chemical plants. As installations continue to age, the likelihood of an incident will only increase further. Incidents show that this still is a relevant issue. Its impact on national security remains limited, though. Finally, past monitoring has shown that during transport of flammable liquids and gases by rail especially, exceedances occur on the Brabant route. At the same time, several cities along the Brabant route have ambitions in terms of spatial development around the railway. The 2022 rail monitoring report shows that the extent to which the risk ceiling is exceeded is the same as in previous years (AVIV, 2023). Spatial development around the railway also continues to cause an increase in the group risk. This could potentially increase the impact of an accident.

[3] Also see section A.10 about critical infrastructure.

Besides the acute effects of exposure to chemicals, increasing attention has been paid in recent years to long-term health effects on people living in the vicinity of industrial plants. In 2023, RIVM conducted a study on the contribution of Tata Steel Netherlands to the health risks of local residents (Geelen, 2023). *"The research confirms that the emissions from the Tata Steel site contribute to the quantities of particulate matter, nitrogen dioxide, polycyclic aromatic hydrocarbons (PAHs) and metals in the immediate surroundings. In particular, the emissions of particulate matter, nitrogen oxides and dust, odour and noise nuisance increase the likelihood of adverse health effects. As a result, local residents have a slightly elevated risk of asthma, lung cancer and premature death."* Following on from the study on Tata Steel Netherlands, RIVM started an exploratory study on the health effects of Chemours and the Western Scheldt on local residents, which was commissioned by the Ministry of Infrastructure and Water Management (RIVM, 2024b). Although the long-term health effects of industrial plants on local residents is not directly a national security issue at present, it may influence decisions and considerations regarding the establishment of (new) industry and thus (undesirable) strategic dependencies.

Explanation of threat assessment

The risks of major accidents are not fundamentally different from those foreseen in the NRA. However, the trends identified in the NRA continue. The threat assessment therefore remains unchanged.

A.4 Social polarisation, extremism & terrorism

For the threat theme of social polarisation, extremism and terrorism, we will consider the following two threat categories separately: social polarisation on the one hand and (non)-violent extremism and terrorism on the other. Extremism and terrorism are considered together because relevant developments show a lot of overlap.

Threat category of social polarisation

Key findings and conclusions

The threat assessment has not changed substantially. However, given the increasing importance of the topics of climate and migration, it is likely that the risk of further polarisation surrounding these themes will also increase in the future. There is also an increased risk that existing polarisation will be exacerbated as a result of influencing and disinformation campaigns by malicious actors, helped in part by the ever-greater accessibility of generative AI (see also section B, Technology assessment).

General overview of findings and state of affairs compared to NRA

Political and social polarisation remains a significant challenge in the context of national security. Dutch citizens report that they feel that social divisions and intolerance are on the rise (ANV, 2022). Views regarding culture and identity are one of the dividing lines along which polarisation is visible. In addition, in recent years the topics of climate and migration in particular have determined people's (political) identity in many cases, and these are the themes around which polarisation has grown especially. Since October 2023, the war in Gaza has also developed into a politically and ideologically divisive issue, where there is social divisiveness regarding the Dutch government's desired response to the crisis (Movisie, 2023).

The type of media consumed largely influences the formation of opinions on policy issues and on the government in general. A majority of Dutch people still use multiple news sources and are not in a so-called filter bubble. The variation in the use of media brands and news sources did decrease in 2023 compared to 2022, though (Dutch Media Authority, 2023). This decline is mainly at the expense of channels with origins in traditional media, such as radio, television and print, and can be seen especially among younger age groups (18-45-year-olds). These groups increasingly get their news from digital platforms such as X and TikTok (Mulder, 2023).

As a result of stricter action by major media platforms to combat the spread of fake news, there is a visible shift of

disinformation from public social media to private social media channels such as Telegram groups, for example. This may further increase the risk of so-called 'echo chambers', which are also more difficult to monitor.

Besides the opportunities offered by private channels for spreading fake news, we also see developments on the production side of disinformation. The possibilities for low-effort production of disinformation have soared since 2022 thanks to generative AI.[4] Not only is it possible to produce fake news on a larger scale, and in a more microtargeted manner, these apps and systems are also becoming increasingly accessible to ordinary users, thus lowering the threshold for use. This has increased the number of potential threat actors. When the NRA was drafted in 2022, this accessibility was already flagged as a development.

Threat category of (non)-violent extremism and terrorism

Key findings and conclusions

For this threat theme, the threat has increased. Due in part to the war in Gaza, Quran vandalism in the Netherlands and Scandinavia, and calls for violence by supporters of terrorist organisations, the threat of extremism and terrorism has increased. The national threat level has also been raised. In addition, anti-institutional extremism, right-wing extremism and, to a lesser extent, left-wing extremism, remain a threat to national security in various ways.

General overview of findings and state of affairs compared to NRA

Low trust in government institutions since the COVID-19 pandemic has manifested itself in, among other things, *anti-institutional extremism* and an increase in conspiracy thinking, with an overlap between these two groups.[5] Despite COVID-19 losing importance as a theme, the anti-government movement seems to have grown in size. At the same time, it also started focussing on other issues (AIVD, 2023). Characteristic of the narrative of anti-institutional extremists is the idea that the Dutch population is at war with an evil, internationally operating elite that controls the government, the judiciary, the media and science, among other things. This narrative undermines the democratic constitutional system by eroding public trust in institutions. It also contributes to a threatening, intimidating and intolerant atmosphere. To a limited extent, the narrative leads to a conceivable threat of violent extremism. So far, the number of violent incidents has remained limited, but the threat of violence has become more realistic in recent years (AIVD, 2023). Besides the use of intimidation or violence and the undermining of the democratic constitutional system, the threat originating from anti-institutional extremism is also the narrative's wider radicalising and socially polarising effect.

Within the context of anti-institutional extremism, the sovereign citizen movement in the Netherlands is growing. Although the exact size of this group is difficult to pinpoint, the AIVD estimates that at least several tens of thousands of people currently identify as 'sovereign' (AIVD, 2024). Their numbers are expected to increase further in the coming years. These individuals believe that Dutch laws and regulations do not apply to them, a belief that mostly stems from the same conviction regarding a malicious elite that has been outlined above. They mostly aspire to create a parallel, alternative world, free of oppression from this supposedly evil elite. The majority of these people (sometimes called autonomists) advocate for change within the boundaries of the current democratic constitutional system, for example through achieving a degree of self-sufficiency. However, a smaller proportion fundamentally rejects the system as well as its legitimacy and deliberately does not abide by laws and regulations, even though this sometimes has major personal consequences, such as eviction or mounting debts. Finally, a very small subgroup believes in the inevitability of a violent struggle with the government (AIVD, 2024).

Anti-institutional extremism overlaps with right-wing extremism in some areas. This is particularly evident around topics such as the great replacement theory and the idea of a *great reset*. In addition to an emphasis on anti-Islam and anti-immigration rhetoric, right-wing extremism focuses increasingly on racial purity and the aforementioned great replacement theory. Anti-Semitism is also a central element, but it is increasingly linked to the ideas of repopulation and racial weakening (AIVD, 2024). The AIVD indicates that the greatest threat within right-wing extremism comes from so-called accelerationism, which serves as the biggest source of inspiration for potential perpetrators of violence and helps to successfully recruit new supporters.[6] Right-wing extremist discourse in general has become increasingly normalised since the 2015 refugee crisis. At the same time, due to stricter moderation on major online platforms, right-wing extremists are increasingly diverting to less mainstream alternatives and encrypted chat services, which are more difficult to monitor by intelligence services.

[4] For more information, see the Technology assessment in Section B.

[5] Trust in political institutions such as the government and the House of Representatives is lower than trust in non-political institutions such as the judiciary and police. See: CBS, 2023.

[6] Accelerationism is a right-wing extremist ideology. Its supporters aim to unleash a race war through terrorist violence, with the aim of creating a white ethnostate.

In recent years, left-wing extremism has focused primarily on activism through demonstrations and civil disobedience. The most important focal points are climate and racism, around which broader coalitions are formed. The threat of left-wing extremism lies mainly in protests getting out of hand, and the potential crossing of the line from activism to extremism as a result of social developments. In addition to 'long-running' themes such as racism and climate, the war in Gaza has recently mobilised a lot of left-wing activism. This has resulted in demonstrations in both the Netherlands and the rest of Europe, as well as the United States.

In addition to left-wing activism, the war in Gaza has also caused an increase in anti-Semitism, which could be to the benefit of those who promote a right-wing extremist ideology. At the same time, an increase in anti-Islamic sentiment can also be observed. The threat to both these groups has increased, and has resulted in both Jewish and Islamic institutions receiving (additional) protection.

As a result of the war in Gaza, the threat of Islamic extremism and jihadism has also increased (NCTV, 2023a). This was one of the reasons for the NCTV to raise the threat level to 'substantial' in 2023. Europe has seen several attacks inspired by the events in Gaza since the start of the war (Reuters, 2023a). In addition, several terrorist 'cells' have been dismantled since October 2023, which may have been planning to carry out attacks on European soil (Reuters, 2023b). Earlier, the NCTV also signalled the threat posed by the Afghan branch of ISIS (*Islamic State Khorasan Province*). This ISIS-directed threat continues to exist, even if many attack plots are foiled. The attack in Moscow in March 2024 is illustrative of this threat (NCTV, 2023b).

A.5 Foreign subversion of the democratic constitutional system

The theme of foreign subversion of the democratic constitutional system comprises three different threat categories that are assessed separately: hybrid threats, foreign influencing, and espionage. Each of these three categories is discussed below. In the NRA, the topic of organised crime also falls under the threat theme of foreign subversion of the democratic constitutional system. However, organised crime is included in the Trend Analysis as a separate theme (A.6) to match the classification used in the Security Strategy.

Threat category of hybrid threats

Key findings and conclusions

The *nature* of the threat itself has not changed, but the threat level has increased, though, as a result of increased competition between the great powers. The deployment of hybrid means in itself is not a new phenomenon. However, in recent years we have seen an expansion of the ways in which these means are deployed, and an expansion in the types of intended targets. One of the most striking examples of a form of hybrid conflict was already visible at the time of publication of the NRA, in the form of Europe's dependence on Russian gas and Putin's restrictions on gas supplies. Russia used these energy policies to put European societies under pressure in an attempt to break the united support for Ukraine. With increasing global tensions, there is also a growing threat that actors will use these hybrid instruments more often and to a greater extent.

General overview of findings and state of affairs compared to NRA

The scale and frequency at which ever-more assertive and aggressive states are using hybrid instruments for the purpose of interference and influencing have continued to increase over the past two years. This increase is being facilitated, among other things, by technological developments. The ever-increasing integration of digital technologies into all aspects of society also creates new vulnerabilities, including in critical infrastructure and digital services.

Threat category of foreign influencing

Key findings and conclusions

The nature of the threat assessment has not changed, but we do see that the threat outlook has become bleaker as a result of increased competition between the great powers. The most prominent example of this are the influencing and destabilisation activities that Russia has deployed in Europe since the start of the war in Ukraine. In addition, China and other states continue to make influencing attempts. Influencing is done increasingly through disinformation campaigns around elections and major international issues. This risk has grown over the past two years due to the new possibilities offered by the rapid developments in the field of generative AI for information manipulation, and the development and spread of misleading information. Against the background of deteriorating geopolitical relations, this means that the risk of disinformation campaigns regarding, for

example, the European elections in 2024 has increased (Ramdharie, 2024).

General overview of findings and state of affairs compared to NRA

Foreign influencing and interference are a persistent threat. This includes influencing diaspora communities as well as influential individuals or politicians. The AIVD identifies that in the past two years, countries such as China, Russia, Iran, Turkey and Morocco have continued to attempt to influence diaspora communities with the aim of strengthening the (dependency) relationship with the home country, or to exert influence on Dutch democratic society through these communities (AIVD, 2023). In some cases, we see a change in the method or frequency of foreign influencing and interference. For example, at the beginning of the war in Ukraine, Russia intensified its attempts to influence its own diaspora abroad through disinformation campaigns aimed at reinforcing a sense of victimisation (Scott, 2022). When influencing one's own diaspora, the focus is likely to be on nearby foreign countries and to a lesser extent on far-off foreign countries, such as the Netherlands (Houtkamp & Drost, 2023). In addition, Russia still runs large-scale information campaigns in Ukraine itself, and we have seen over the past two years that it also targets its influencing operations directly at societies in Europe. For example, the war in Gaza prompted an influencing campaign in France aimed at increasing social division around this issue (Albertini, 2023). Foreign influencing can also result in spillover effects. A recent example are the riots between Eritrean groups in The Hague in February 2024 (NOS, 2024).

Threat category of espionage

Key findings and conclusions

The threat outlook for this category has become slightly worse, due to growing tensions between the great powers. Espionage is increasingly used as a means for information gathering, covert influencing and sabotage (preparation). At the same time, there is also increasing attention to and awareness of the threat of espionage within key sectors.

General overview of findings and state of affairs compared to NRA

Identifying intelligence officers operating in the Netherlands remains a focus of the Dutch security services, with current investigations concentrating mainly on Russian and Chinese intelligence officers (MIVD, 2023). Dutch intelligence services are also increasingly attentive to the threat of cyber espionage by foreign state actors and see an increasing number of digital espionage attempts by these state actors at Dutch government institutions, such as the armed forces, ministries and embassies (MIVD, 2023). In 2023, several foreign intelligence services have not only targeted the central government and key sectors, but also specific institutions and local governments (AIVD, 2024a). The current acceleration of technological developments and the opportunities that it offers for cyber-attacks, have increased the risk of complex sabotage and espionage operations.

Multiple attacks on underwater infrastructure have taken place globally in recent years (Kingston, 2024). This has resulted in seabed warfare now being a major concern for intelligence services, among others. Until 2023, it mainly involved actions by Russian groups. However, reports of Houthi attacks on underwater cables in the Red Sea show that non-state actors can use this tool as well (Martin, 2024).

In light of the increase in cyber espionage, dependence on foreign suppliers of technology is also a growing concern. Indeed, using so-called backdoors, technology can be employed for data collection or espionage. In response to this threat, strategic policy choices are made based on security considerations. However, complete decoupling is impossible. Because of concerns regarding dependence on foreign technology companies and platforms, the national Cyber Security Council has advised to invest more in national technology companies, thus reducing this dependence (Okano-Heijmans, 2023).

Espionage and foreign influencing can also be facilitated through participations or takeovers by hostile actors in critical sectors of the Dutch economy. This risk is reduced through the Act on Security Screening of Investments, Mergers and Acquisitions (Vifo Act). Taking effect in 2023, it introduced a security screening for investments, mergers and takeovers that may pose a risk to national security (Ministry of Economic Affairs and Climate Policy, 2023). The espionage penalisation bill is also an important measure to better combat espionage in a broader sense (AIVD, 2024b).

A.6 Organised crime

Key findings & conclusions

The state of affairs and dynamics described in the NRA for organised crime are mostly still valid. This applies to the undiminished high pressure that organised crime can exert on institutions linked to the functioning of the democratic constitutional system and to the use of facilitators in various sectors. A number of trends may potentially manifest themselves more strongly in the coming period, though, including in the area of cybercrime. However, the most notable development within this threat theme is a very sharp increase in the use of explosives as a means of intimidation (among other things). This development has changed the threat outlook for organised crime in the sense that the pressure on physical safety, economic security and socio-political stability has increased.

General overview of findings and state of affairs compared to NRA

In general, due to the obviously covert nature of organised crime, it is particularly complex to make a reliable statement about its exact extent. This is true, for instance, in terms of the quantity and type of narcotics trafficked, produced and transited. Nevertheless, the pressure from organised crime in the form of (violent) threats to journalists, public administrators, politicians and prosecutors, among others, remains as high as ever. As identified in the NRA, the consequence of this may be that people are increasingly unwilling to do these jobs, are hampered in their functioning or possibly give in to criminal interests.

A lot of political and administrative attention is still being paid to fighting organised crime. This is evident from structural funding and ongoing projects in the field of legislation and (international) cooperation (Ministry of Justice and Security, 2023). However, the exact effect of these actions and their possible impact on the organised crime threat assessment is difficult to gauge. This is partly because the effectiveness of investments and policies may only materialise over multiple years and partly because of the inherently covert nature of organised crime. However, if policies prove successful and the pressure on criminals subsequently increases, there is a danger that this could lead to a (temporary) increase in threats and other forms of (physical) violence aimed at, among others, people working for the institutions responsible for policy implementation. At the same time, organised crime is a topic that has to compete with other pressing issues such as those surrounding climate change and the increased pressure on international stability and cooperation. This bears the risk that the (financial) capabilities to fight organised crime

may come under pressure. Given the additional resources allocated, this is however not yet an issue of concern.

To carry out their activities, criminals depend in part on people who act as facilitators, whether forced or not. These include, for example, corrupt contacts at logistics hubs such as ports. The more people there are who are in a vulnerable position or are easily influenced, the easier it will be for criminals to find facilitators or victims of criminal exploitation. In recent years, concerns have often been raised in this context about the use of increasingly younger youths to pick up drugs from shipping containers or to deploy improvised explosive devices. At the same time it is plausible that, partly as a result of climate change or decreased international stability, the level of (irregular) migration will be high in the coming years. With an immigration process that is already under pressure, it is quite possible that more and more people will disappear from the radar or end up in a vulnerable position. Obviously, far from everyone who is in an unstable or vulnerable situation will become involved in organised crime in any type of way. However, the greater the pressure and instability, the larger the group of vulnerable people.

When it comes to violence from organised crime, the number of liquidations in the European Netherlands remains relatively low for the time being, despite a small increase. At the same time, however, there are signs of a hardening of the criminal world (WODC, 2021; 2023). Proof of this hardening is, for example, a rise in excessive violence in the form of not only the increasingly frequent deployment of explosives, but also in kidnappings of (family members of) criminals. The very sharp increase in the use of explosives over the past two years is a striking development within the theme of organised crime. There is a more than fourfold increase from about 200 attacks and attempted attacks in 2022 to 900 in 2023 (Netherlands Police, 2023). Most of them can be linked (as far as this is possible at all) to offenders associated with organised (drug) crime. To a smaller extent, we also see copycat behaviour by others. Explosives, including in the form of heavy fireworks, are very easy to obtain and are an effective means to intimidate people,[7] put them under pressure or ensure that (buildings belonging to) competitors in the criminal world attract the attention of the police and judiciary. Their use as a means of intimidation is much less risky and considerably cheaper for the person who orders these attacks than, for instance, a liquidation. Although the numbers of fatalities or injuries have not been large so far, they are expected to increase in the future. Not only are explosives being used more frequently, they are also becoming increasingly heavier. This not only results in major economic damage to buildings, for example, but can also be very dangerous for people in the area.

A final development regarding the potential for violence from organised crime is that more and heavier weapons will likely end up on the European black market in the coming years as a result of the war in Ukraine. This may also make it easier for criminals to acquire these weapons. It explicitly not only concerns small calibre firearms, but possibly also weaponry with more capabilities such as anti-tank weapons, land mines, grenades, etc. (Van Nierop, 2023).

In the area of cybercrime, the number of registered manifestations in the Netherlands remains high but stable (NCTV, 2023). There is, however, a strong suspicion of underreporting and there are indications that many parties refrain from filing a police report. This can be for fear of reputational damage, but also because it is sometimes cheaper, for instance in the case of ransomware, to meet the demands than bear the possible (indirect) costs of a police investigation. Cybercrime is generally believed to have taken on industrial proportions in recent years in terms of victims, damages and revenues. Despite the (temporary) plateauing of the recorded number of cybercrime incidents, these numbers could rise sharply again in the coming years. This is due to the scalability as well as profitability of cybercrime (NCVT, 2023), including in the form of ransomware attacks.[8] Within Europe, an increase in cyber-attacks by criminals on critical sectors in particular has already been observed (NCTV, 2023; UK NCSC, 2023). If this trend also becomes evident within the Netherlands, it will result in more frequent disruptions of, for instance, the electricity supply. All the more so when at the same time an increase in the use of wiperware is seen, which can wipe entire systems (NCTV, 2023; UK NCSC, 2023).

The wider availability and accessibility of generative AI could further facilitate and automate cybercrime in the future. Some possible applications include increasingly sophisticated forms of WhatsApp fraud (voice and image), extortion or blackmail by (threatening) the spreading of AI-generated images and deliberately passing on disinformation (such as manipulated camera footage) to the police and investigation services. See also chapters A.9 and B.1 regarding this topic.

The war in Ukraine shows a mixture of state actors and non-state criminal groups within both Russia and Ukraine carrying out cyber-attacks back and forth (crime as a

[7] These may not only include other criminals, but obviously also local residents and people working at institutions associated with the functioning of the democratic constitutional system.

[8] Not only criminal actors, but also some state actors with an anti-Western agenda use ransomware attacks, among other things, to get financial resources.

service). Although Russia is currently largely focused on Ukraine in this regard, this situation may change. This is true especially given the deteriorating relations between Russia and the West due to sanctions imposed on Russia and support for Ukraine (NCTV, 2023).

Explanation of threat outlook

In summary, the dynamics with regard to organised crime are not fundamentally different than identified in the NRA. However, some of the above developments do have potentially more serious consequences for national security and thus result in a worsened threat outlook.

First, due to the widespread use of explosives, it is likely that organised crime will produce more (innocent) victims than previously thought. The use of explosives has made organised crime and the threat that it poses more visible to a larger group of people than anticipated. This may affect, among other things, people's confidence that some of the institutions associated with the democratic constitutional system will be able to cope with the situation. It is also possible that people working for these institutions may be pressured or intimidated in this way. This could undermine their functioning. Furthermore, given the hardening of the criminal world, it cannot be ruled out that the number of liquidations may also increase again in the coming years.

Finally, and also in light of the recent wide accessibility of AI techniques, there is the potential that various forms of cybercrime (whether or not as part of a hybrid campaign) could lead to greater economic damage. All the more so when critical sectors are (also) targeted. Especially when there is little back-up capacity, as in the Caribbean part of the Kingdom, this could lead to serious disruptions of the critical process in question. This could put pressure on the availability of basic needs (physical safety).

A.7 International and military threats

The threat theme of international and military threats contains four different threat categories that are treated separately here. They are: fragility in the vicinity of the Netherlands; pressure on multilateral (security) organisations; conflict between centres of power, and proliferation of weapons of mass destruction.

Threat category of fragility in the vicinity of the Netherlands

Over the past two years, political and economic instability have increased in large parts of the world in the vicinity of the Kingdom. The spillover effects of this instability are impacting our national security interests.

General overview of findings and state of affairs compared to NRA

The war in Ukraine has a major impact on our national security. Not only does the war affect Dutch economic security and social and political stability, the territorial threat and risk of military confrontation with Russia have also increased.

In addition to the all-out war in Ukraine, there are also (smaller-scale) conflicts and military tensions in other regions in the vicinity of the Kingdom. The dormant unrest between Serbia and Kosovo in the Balkans has escalated into active conflict situations several times over the past two years. Moreover, Russia is trying to fuel these tensions, thus undermining the stability in the region. The war between Azerbaijan and its ethnic Armenian enclave of Nagorno-Karabakh has also added to the fragility to the east of Europe in the past two years. The previously latent conflict escalated into an active conflict partly due to changing regional and global power dynamics and has resulted in thousands of refugees and a humanitarian crisis. The conflict may have implications for (surrounding) regions struggling with similar questions of territorial integrity and self-determination (Landgraf et al., 2024).

In recent years, geopolitical competition over the Arctic has increased, intensifying since Russia's invasion of Ukraine. As a result of the war, regional cooperation with Russia in the Arctic has been halted. At the same time, ties between Russia and China have become stronger. This brings with it the risk that China, in cooperation with Russia, may also start activities in the Arctic (Wall & Wegge, 2023).

We also see spillover effects of the war in Gaza, both in the region and in Europe. Apart from the destabilising effect of the war itself, the Western reaction to the war can also have a negative effect. The perception of Western partiality or

inaction by international security organisations can serve as a breeding ground for extremism and jihadism in the region. Economic hopelessness and political repression and instability remain an important factor in the perpetuation of that breeding ground. However, outrage and anger over the war in Gaza can have a radicalising effect in this regard on (vulnerable) groups and individuals in the region and beyond (Marcetic, 2023; Al Hussein, 2024).

In the past two years, a series of coups and coup attempts in Burkina Faso, Sudan, Gabon, Niger and Guinea, among others, have further exacerbated instability in Central and North Africa (Reuters, 2023a). Growing food insecurity also adds to the region's overall fragility and contributes to large regional refugee movements in the case of the Sudan conflict, for example. These regional refugee flows have a further destabilising effect on countries in North Africa, which have already witnessed growing authoritarianism and political instability over the past two years (Diwan et al., 2024). Some of these refugee flows may then also move towards Europe. This may put even more pressure on limited means and capacities for providing shelter, possibly leading to further polarisation around the issue of migration within European societies.

Stability in the region surrounding the Caribbean part of the Kingdom is also under pressure. The risk of spillover effects from geopolitical competition in Latin America remains unchanged, especially from competition between Russia and the West. At the same time, China is also expanding its interests in Latin America, in particular in Venezuela. For now, President Maduro is managing to maintain a balance between Moscow and Washington. However, he is following an unpredictable and irregular course, which President Putin is taking advantage of by strengthening Venezuela's ties to him. Maduro's unpredictable policy was also evident in 2023 during the crisis surrounding the dispute between Venezuela and Guyana over the Essequibo territory. There is also instability in the border region between Venezuela and Colombia. The growing competition between various armed groups and criminal organisations in Colombia focuses on control of illegal trade routes, and this competition leads to an explosion of violence. The Colombian government has no control over parts of the rural border region with Venezuela. The instability in Venezuela in particular has a direct impact on the security interests of the Caribbean part of the Kingdom.

Threat category of pressure on multilateral (security) organisations

Key findings and conclusions

The multilateral order is under pressure. This pressure translates, among other things, into increased bloc formation and paralysis within multilateral organisations (Clingendael Institute, 2024).

General overview of findings and state of affairs compared to NRA

Partly as a result of the changing world order, there is an increasingly clear trend of growing bloc formation in certain multilateral (security) organisations. At the same time, we see that other partnerships such as NATO and the EU have actually been given a boost by the urgency of the war in Ukraine. In the past two years, the EU has taken steps to improve its defence capabilities. In 2023, the European Parliament voted in favour of the ASAP Act, which frees up 500 million euros to scale up the European arms industry for ammunition and missile production. The 2023 EDIRPA agreement, which sets out a joint procurement policy for weapon systems and ammunition, also aims to strengthen the industrial and technological capacity of member states for the benefit of the EU's defence capabilities (European Parliament, 2023).

The US attitude towards multilateralism and multilateral security institutions is of great importance for the strength of these organisations. The US has partially re-embraced multilateral values under president Biden. This is evidenced by, among other things, his return to the World Health Organization and the Paris Climate Agreement.

Threat category of conflict between centres of power

Key findings and conclusions

Increased great-power competition, related proxy conflicts in various parts of the world, and growing escalation potential have a negative impact on national security interests.

General overview of findings and state of affairs compared to NRA

Against the backdrop of growing great-power competition, tensions between China and Taiwan are mounting, which in turn could escalate US-China tensions as well. Taiwan has warned that tensions with China have risen sharply due to China's increased military activities and exercises near Taiwan. This also increases unrest between the US and China.

In addition to tensions with Taiwan, China also has a fraught relationship with India. Since the outbreak of the war in Ukraine and in the context of increased tensions between the great powers, India has taken on a new, more important role in the international security landscape. India has traditionally been non-aligned and, for the time being, would like to remain so. At the same time, tensions with China are growing as a result of a border dispute that flares up with some regularity. Just like China, India also

has strong (military) ties with Russia, and has continued to trade with Russia despite the war in Ukraine. At the same time, given the tensions with China in the region, India is an important security partner for the US, and we see the US trying to strengthen its ties with India through economic and military cooperation (Ayres, 2023). While great-power competition can have a major impact on the emergence of tensions and the development of proxy conflicts, national or regional conflicts can, in turn, also have repercussions on the great powers and their mutual relations. The war in Gaza has important spillover effects on tensions between other (great) powers, both regionally and in the West.

Threat category of proliferation of weapons of mass destruction

Key findings and conclusions

Due to the increased tensions between the great powers, we see existing arms races speeding up and new arms races emerging.

General overview of findings and state of affairs compared to NRA

Pressure on multilateral arms control regimes has mounted in recent years as a result of increased competition between great powers. For example, Russia paused the *New Start Treaty*, and the US responded by stopping to provide the data that it was required to share under the Treaty (Williams, 2023). Russia has also withdrawn from the *Comprehensive Nuclear Test Ban Treaty* (CTBT) (Bugos, 2023). China has been further expanding its nuclear capabilities at record pace in recent years. The country now imports more uranium from Russia than ever before (Dolzikova, 2023). At the same time, China and the US held nuclear arms control talks for the first time in five years in November 2023. Although these conversations have been an important opening, the meetings have not yet resulted in any further steps (Reuters, 2024).

In contrast to the developments in talks with China, there are no positive developments in the relationship with Iran with regard to the nuclear issue. Since the US withdrew from the JCPOA under former President Trump in 2018, a functional follow-up to the nuclear arms control agreements with Iran seems far away. The quarterly reports from the International Atomic Energy Agency (IAEA) clearly show that Iran is continuing its nuclear programme. According to IAEA weapons inspectors, Iran has now managed to enrich uranium to 84%. This is close to the 90% required for a nuclear weapon, even though this is not done on a large scale yet, as is the case with lower enrichment percentages. Although Iran indicates that its nuclear programme is only intended for peaceful purposes, the objective of the increased enrichment remains unclear (Reuters, 2023b).

In addition to its negative effect on nuclear proliferation, increased competition between the great powers has also increased the risk of new arms races. The past two years have seen an increase in competition in new weapons technology, including hypersonic weapons and AI-enabled weapon systems (Pincus, 2023). With regard to chemical and biological weapons, developments in generative AI have lowered the knowledge threshold, potentially allowing a broader spectrum of actors to develop the capabilities to create chemical and biological weapons. For more information, see A.2 Infectious diseases.

A.8 Economic threats

Within the theme of economic threats, five threat categories are discussed: strategic dependencies & contraction or distortion of international trade; threats to the Netherlands' role as an important logistical hub; foreign interference in industry; and destabilisation of the financial system.

Key findings & conclusions regarding economic threats

The economic threats described in the NRA remain largely current. The geopolitical turmoil and associated (economic) competition and conflict contribute most to new uncertainties. The biggest shock comes from the war in Ukraine, which has resulted in sanctions and higher energy prices and indirectly in broader inflation and higher interest rates. The initial shock has been largely absorbed, but the war still incurs costs (aid and shelter). There has also been an increased focus on geopolitical risks, e.g. surrounding strategic dependencies and knowledge security. Manifestations of this are, for instance, export restrictions and new industrial policies. Infrastructure, and thus trade, also remains susceptible to disruptions of a deliberate and non-deliberate nature. In financial markets, credit risks have increased due to higher interest rates, among other things. This has resulted in several high-risk events, but without major financial consequences.

Threat categories of strategic dependencies & contraction or disruption of international trade

The biggest (economic) shock since the publication of the NRA in 2022 has been the further spillover of the war in Ukraine. This has had various effects, for instance through associated public costs (e.g. military support, refugee reception) and the vitality of the economy (higher gas prices and wider inflation, increased uncertainty; Government of the Netherlands, n.d.-a; Ministry of Defence, n.d.; Ministry of Finance, 2023). As it turned out, the risks regarding the strategic dependence on Russia (for gas, among other things) had been underestimated, but alternatives were found quickly (e.g. energy saving, LNG; Government of the Netherlands, 2023a). The gradual introduction of tougher sanctions against Russia has mostly spared Western economies, but has also resulted in the measures being less effective.

Especially at the beginning, the war between Israel and Hamas also created uncertainty within financial markets. And if further escalated, it could affect the vitality of the Dutch economy (Koenis, 2023). A few months after the outbreak of war, however, this effect seems limited and world trade has been affected more in particular by attacks of Houthi rebels on shipping lanes in the Red Sea. In April 2024, the direct confrontation between Israel and Iran threatened to cause escalation in the region and thus possibly impact, for example, oil prices.

After years of further liberalisation of world trade, we have seen a turnaround in recent years due to the COVID-19 crisis, the war in Ukraine and the subsequent energy crisis. The rise of and economic conflict with China also lead to an increased number of trade restrictions and forms of state support. For instance, under pressure from the United States, the Netherlands has introduced increasingly extensive export restrictions on ASML's advanced chip machines since 2019 (ASML, 2023; 2024). Also, the European Commission has launched several investigations into trade-distorting measures by the Chinese government (including for electric cars; European Commission, 2024). Within Europe, the uneven support for domestic industries to help them cope with higher energy prices is creating distortions in the internal market for the time being (European Commission, 2023). In the United States, US industry is supported through the Inflation

Reduction Act. The focus on industrial policy has thus greatly increased.

Climate change (see also section A.1) is set to cause material damage and other rising costs (mitigation and adaptation investments) in the (very) near future – for instance due to extreme weather events. In addition, there may be wider economic effects due to disrupted trade, both directly (inaccessible trade routes) and indirectly (e.g. crop failures). For example, drought of historic proportions has greatly reduced the capacity of the Panama Canal (Jumelet, 2023).

Threat category of threats to the Netherlands' role as an important logistical hub

For several reasons, Dutch infrastructure is a risk factor for economic vitality in the Netherlands. For instance, following on from Nord Stream II, there is the threat of (physical) sabotage of underwater infrastructure, such as for energy supply and internet connections (Ministry of Defence, 2024; NOS, 2023a). In this context, the North Sea Infrastructure Protection Programme has been set up in the Netherlands (AIVD, 2024). Other risks stem from the large investments required to maintain the overall infrastructure, which increasingly leads to delays and hold-ups, partly due to staff shortages (Prorail, 2023; Kompeer, 2023). Extreme weather events, such as prolonged periods of drought, are also becoming more common and thus more frequently disrupt trade routes at home and abroad, including shipping lanes (see also the chapter on climate and natural disasters; Van der Maas, 2023; ING, 2023).

We also see an increase in social and political attention for (the effects on) the environment in recent years, for instance when it concerns aviation and polluting industry (NOS, 2023b; Evofenedex, 2023). This can have an effect on economic decisions, both by Dutch politics and (international) businesses. In addition, legal restrictions with regard to nitrogen still apply and grid congestion has further increased as a result of the energy transition (Rooijers, 2024; Government of the Netherlands, 2024). Moreover, stricter (or legally enforced) environmental standards related to manure or water quality threaten to create additional obstacles for both businesses and citizens (Van der Boon & Gras 2024; Van der Boon & Kakebeeke, 2024; Vestergaard, 2023).

Threat category of foreign interference in industry

Cyber threats (see also the relevant threat theme) remain highly topical for both financial institutions and the wider business community. Strategic attention of companies for this problem is growing. However, companies may still be vulnerable if organisations in their supply and outsourcing chains are less well-prepared.

Also, the AIVD and MIVD are warning once more for (cyber) espionage at Dutch businesses, still citing China as the main threat (AIVD, 2024; Ministry of Defence, 2024). Partly because of the risks of leaking advanced knowledge and technology, export restrictions have been imposed on ASML.

The rise of new digital technologies – such as AI and (further in the future) quantum technology – carries risks, both direct (technology as a weapon or instrument of power) and indirect (companies and research institutions falling behind, thus affecting the vitality of the Dutch economy). However, if risks are contained too strictly it can actually limit growth opportunities for the domestic knowledge economy as well. New European laws and regulations to safeguard fundamental rights, for instance, may also create new hurdles for European businesses.

Finally, the Netherlands has developed and introduced policies to limit sensitive takeovers and investments and interference by foreign actors, including the Vifo Act (Government of the Netherlands, 2023b; Ministry of Economic Affairs and Climate Policy, 2023). European regulations targeting critical providers (see also the relevant threat theme) also safeguard economic security (Government of the Netherlands, 2022; AFM, 2024).

Threat category of destabilisation of the financial system

Rising inflation in the Western world has caused a sharp increase in interest rates. A combination of increasing interest rate and credit risks, reduced liquidity in financial markets and the persisting relatively high inflation create a permanently high risk to financial stability (DNB, 2023a; b). Several bank failures in early 2023 in the US (including Silicon Valley Bank) and Switzerland (Credit Suisse) were concrete evidence of this.

The Dutch banking sector is turning inwards. Following Brexit, banks have not returned to the Netherlands. The Dutch banking sector is no longer as prominent as it was around, say, the year 2000. In addition, the crypto market carries risks for the financial system. The collapse of a major player in the financial sector can have a major impact on investor confidence, leading to a recession or (financial) crisis. Nevertheless, the collapse of crypto platform FTX in 2022 had no major financial consequences.

A.9 Cyber threats

Key findings & conclusions

Cyber-attacks are commonplace. Threat assessments from recent years show that the digital threat remains substantial and is subject to constant change. At the same time, cyber-attacks with a highly disruptive impact on national security have so far not taken place in the Kingdom. Due to the increase in scale and automation of attacks, new technologies used and increased dependencies, it remains important to establish solid digital security in order to protect national security interests (NCTV, 2023; ENISA, 2023; AIVD, 2024).

General overview of findings and state of affairs compared to NRA

Artificial Intelligence applications: threats and opportunities

In recent years, Artificial Intelligence (AI) has developed rapidly. This technology area has many applications, also within cybersecurity. The use of AI within cybersecurity is not new, but has gained new momentum with the emergence of generative AI (see also the technology watch and assessment later on in this In-Depth Exploration of the Trend Analysis). Malicious actors can use this technology to develop malware, disinformation campaigns, or automate and execute larger-scale cyber-attacks. The use of Generative Adversarial Networks (GAN) can hamper detection of cyber-attacks. The scalability and personalisation options of AI-assisted cyber-attacks pose a risk in particular. AI can also be used to determine the best timing of a cyber-attack, when its impact is potentially greatest. Besides economies of scale and reduced detection abilities, the availability of Large Language Models (LLMs) that can create malware makes it easier for malicious actors to carry out attacks (NCTV, 2023; UK NCSC, 2024).

At the same time, AI can also be used to defend against cyber-attacks. This involves the application of algorithms to automate defence mechanisms or better detect attacks. This creates a race between attackers and defenders (Janjeva et al., 2023). Nevertheless, such AI-based automatic defence mechanisms generally require a good dataset in order to train the mechanism, which is lacking in many organisations (Lohn, Knack et al, 2023).

AI is being applied in many different sectors besides cybersecurity, such as healthcare, finance, mobility and the military. The increase in the use of AI thus increases the importance of AI security. AI can be manipulated by manipulating the input data or the algorithm itself. This can lead to systems that use AI being disrupted or misled.[9] In 2017, for example, Google's algorithms were

[9] In the Technology watch and assessment of the In-Depth Exploration (section B), the predictability problem is further explained under AI.

manipulated so that they mistook a turtle for a weapon (Vincent, 2017). And in 2019, a group of Chinese hackers showed that a Tesla car could be manipulated in such a way that the car suddenly changed lanes and started riding towards oncoming traffic. Given the expected widespread use of AI, the potential impact of such attacks is high. An obvious example in a military context: missile defence systems can be manipulated to ignore a threat, or weapon systems can self-destruct or attack the wrong target (Galle, 2022).

To gain control over the rapid developments in this technology area, the Artificial Intelligence Act is being drafted in the European Union. It concerns legislation that categorises AI applications and bans those that are deemed high-risk. Examples of high-risk applications include indiscriminate scraping of the internet and CCTV images to create facial recognition databases, biometric categorisation of groups based on sensitive characteristics such as political affiliation or religion, and systems that can recognise emotions in work- or education-related organisations (European Parliament, 2023). At the same time, the effectiveness of such attempts to regulate AI has yet to be proven. For example, there are concerns about the extent to which the regulation will actually have a global effect on the further development of AI (Krasodomski, Buchser, 2024).

Cyber-attacks as a geopolitical tool

The war in Ukraine and geopolitical tensions have led to an upsurge in hacktivism and state-sponsored cybercrime groups. For example, the European Parliament's website went down after it had labelled Russia a sponsor of terrorism (Van Sant, 2022) and attacks were carried out after the announcement of arms deliveries to Ukraine and during Ukrainian President Zelensky's visit to the Netherlands (NCSC, 2023). Both pro-Russian and pro-Ukrainian groups frequently carry out DDoS attacks (NCTV, 2023).[10] Hacktivist attacks are attacks carried out for ideological or political motives. These attacks are usually not sophisticated and their (operational) impact generally remains limited. At the same time, such attacks also have another objective, namely to spread fear and influence the population. Notable in this context was the hack of children's television channel BabyTV, when Russian propaganda footage was broadcast on two separate occasions (NOS, 2024). So far, there have not been any high-impact cyber incidents in the Netherlands with a clear link to the war in Ukraine (NCTV, 2023). Another trend in this context is the increased use of wiperware, a form of malware that erases data from systems. Wiperware is not new, but since 2022 an increase in its deployment can be observed in the context of the war in Ukraine. For the time being, these attacks are the work of state actors. However, in the future, cyber criminals may also carry out such attacks on a large scale for financial gain (NCTV, 2023; Manky, 2023).

The digital threat from state actors also remains relevant. In early 2024, the MIVD reported the presence of malware on a Ministry of Defence network (NCSC & AIVD, 2024). This malware called COATHANGER was most likely deployed by China with the objective of espionage. Although the damage was limited, as the malware had only gained access to an isolated research network, this incident shows that the Netherlands remains a target for espionage by state actors. Depending on geopolitical developments, these actors may also try to sabotage systems through digital attacks in the future, with potentially significant societal impact.

Whereas China previously focused mainly on intellectual property theft, the digital threat from China is now becoming more geopolitical in nature. On an ever-greater scale, vulnerabilities are being identified and systematically exploited (Cary, 2023). For example, US intelligence warns of preparatory activities for sabotage by cyber groups affiliated with China (such as Volt Typhoon). Such activities target IT systems of critical US infrastructure (CISA, 2024). In addition to such preparations, digital attacks on critical infrastructure are commonplace in the war in Ukraine (on both the Russian and Ukrainian sides). Given the volatile geopolitical situation, this means that the (digital) resilience of critical sectors is also moving up on the agenda within the Kingdom (Ministry of Defence, 2024).

Digital strategic autonomy

In the context of ever-increasing digitisation and automation, digital 'strategic autonomy' is receiving increasing attention. Among others, the Digital Open Strategic Autonomy Agenda identifies for a number of policy priorities which ongoing, or new, actions are being taken to mitigate high-risk strategic dependencies (at different levels) in the digital domain. These include dependencies on large US companies in various sectors, such as in the area of cloud infrastructure (Government of the Netherlands, 2023). In early 2024, for example, there was uproar over the intention of SIDN (Netherlands Domain Registration Foundation) to move domain registration of the .nl domain to US-based Amazon Web Services (AWS) (Schellevis, 2024; Hofmans, 2024). Another example is Portbase, the Port of Rotterdam's Port Community System, which moved to AWS in 2018 (Portbase, 2018). According to critics, this trend creates undesirable dependencies on a foreign party. Incidents could result in longer recovery

[10] Distributed Denial-of-Service; an attack where a server has to handle a very large number of requests at the same time, which can block traffic to and from the website and cause the service's server to crash (go down)

times for Dutch infrastructure, since AWS is required by law to prioritise restoring US government services in case of emergencies. Moreover, dependence on one organisation creates single points of failure, where disruption of the services of a large cloud provider could potentially have major impact. It should be noted here that cloud infrastructure is set up in such a way that it is unlikely that all services in both America and Europe will be hit at the same time or fail completely due to an incident. However, the dependence on these American companies could be used as a geopolitical instrument by the US government.

The NRA outlined that cryptography is becoming increasingly important for the functioning of the internet. It also indicated that the privacy and security of online data that cryptography provides is at odds with the desire of detection and enforcement agencies to weaken cryptography by building in master keys to help get a better picture of criminal activity. The debate on this topic was recently revived by a European legislative proposal that would allow European public authorities to require browser providers to incorporate master keys. Following resistance from cybersecurity researchers, scientists and the industry, last-minute changes were made to address concerns about weakening cryptography (iBestuur, 2023). The discussion regarding this topic shows that this issue is still current.

In the longer term, quantum computing is promising technology with a major impact on cryptography, as also outlined in the NRA. In this respect, continued attention should be paid to strengthening the ability of the Netherlands to develop its own reliable cryptographic products under the National Crypto Strategy (NCS). Although quantum technology is not yet mature enough to surpass the computing power of current traditional computers, preparation for the post-quantum era is moving up on the agenda (AIVD, 2023). Cryptography is discussed more extensively in the technology watch and assessment, as part of the quantum technology section.

Cybercrime

The threat of cybercrime is largely unchanged. The deployment of ransomware in particular remains a method of attack that can cause significant damage. Although many businesses became a victim of ransomware in 2023, resulting in significant financial damage, incidents with social impact, such as the NotPetya, WannaCry or Colonial Pipeline attacks, did not occur (NCTV, 2023). At the same time, a larger group of criminals is gaining access to (ransomware) tools, due to, among other things, the aforementioned developments within AI. In a generic sense, a proactive approach towards cybersecurity is therefore required in order to become more resilient to all kinds of cyber-attacks and cybercrime.

At the same time, efforts are being made at the European level to improve cybersecurity in order to be less susceptible and vulnerable to cybercrime, among other things. Under the proposed EU cyber resilience act, companies are required to ensure that their products are cybersecure, complementary to the NIS-2 regulation. Any company putting "products with digital components" on the European market must be able to demonstrate compliance with a number of cybersecurity requirements (Cyber Risk, 2024). Such certification is based on the secure by design principle, which entails that cybersecurity is an integral consideration in the design and development of IT products.

Cybersecurity in space

In 2023, several organisations have identified cybersecurity in space as an issue that will become increasingly important in the longer term (Kaczmarek, 2024; ESA, 2024; NIST, 2024). As satellites are used for a wide range of military and civilian systems (such as GPS, Earth observation and telecommunications), incidents affecting the availability, integrity and/or confidentiality of these satellite services could potentially have a major impact (ENISA, 2022). In the technology watch and assessment, cybersecurity in space is discussed more extensively within the space technology section.

Threat assessment implications

The digital threat remains as high as ever, with national security interests potentially being affected in various ways. For instance, territorial security (and specifically digital security) can be affected by the deliberate deployment of cyber-attacks by states, state-affiliated hackers and cybercriminals. Given the volatile geopolitical situation, but also the increasing accessibility of techniques to carry out cyber-attacks, cyber-attacks will continue to be the order of the day. In recent years, state actors have penetrated networks mainly for the purpose of espionage or to conduct reconnaissance activities (NCTV, 2022b). Depending on how the threat will evolve, it is possible that state actors or affiliated cybercriminals will carry out more sabotage-oriented attacks in the coming years. Such attacks may have an impact on physical safety if, for example, chemical plants are hit or if the cyber-attack causes a lack of basic needs. Moreover, cascade effects on businesses, society and (critical) processes can also result in an impact on other security interests.

In addition to cyber-attacks, the outlined developments regarding, for example, digital strategic autonomy may have a long(er)-term impact on economic security. Moreover, social and political stability and the international legal order may be affected by, for example, the development and spreading of disinformation.

A.10 Threats to critical infrastructure

Key findings & conclusions

Various developments in areas such as geopolitical tensions, the energy transition, strategic dependencies and extreme weather events can impact the continuity and availability of critical infrastructure. Critical infrastructure is increasingly becoming an attractive target for malicious actors given the potential impact of its disruption. At the same time, critical infrastructure also has digital and physical vulnerabilities, which means that processes can also be non-intentionally disrupted or even fail.

General overview of findings and state of affairs compared to NRA

Critical infrastructure as a target

Recent years have shown that critical infrastructure has become an increasingly attractive target for state actors. Whereas previously digital attacks were mainly carried out with espionage and reconnaissance as their objective, the attack on the Nord Stream gas pipelines in September 2022 and the damaging of a gas pipeline and an undersea telecom cable between Sweden and Estonia shows that actors are prepared to actually engage in sabotage (Ministry of Defence of Sweden, 2023). It is worth noting here that it is important to prepare for composite threats, where several incidents occur simultaneously or shortly after each other. This applies, for example, to manifestations of extreme weather, but also to deliberate actions: state actors can carry out sabotage activities in such a way that they coincide with another event (maintenance, extreme weather), putting further pressure on the availability of a process. This requires an increased level of resilience.[11]

Besides state actors, activist or politically motivated groups also pose a threat. In early 2024, an electricity mast near a Tesla factory in Germany was set on fire by a left-wing extremist group (NOS, 2024). In 2022, a power grid attack in the United States left 45,000 residents without power. This attack is believed to have been carried out by a far-right group (Price, 2023; Huizinga, 2022). In the Netherlands we are also warned about the rise of left-wing, right-wing and anti-establishment extremism and a hardening of these movements (AIVD, 2023; 2024). In this context, more and more groups are focusing on climate change. Depending on the further hardening of these groups and their willingness to engage in sabotage, critical infrastructure in the Kingdom could also be targeted.

Digital vulnerabilities of critical infrastructure

Because of the generic dependence on digital systems, critical infrastructure is more strongly interconnected.

[11] Examples would be alternative recovery plans and (crisis) exercises in the chain.

An example of this is the dependence on GNSS, a well-known dependence that has recently regained attention with the publication of the IKUS II report (Government of the Netherlands, 2022). This report states that disruptive cascade effects can occur in the event of GNSS disturbances. However, it is not clear what exactly the dependencies are and what the potential impact of a disruption would be (see also the technology watch and assessment on the topic of space technology). With regard to GNSS dependence, the NRA already noted that space weather phenomena can have a major impact on critical processes (through direct disruption or through disruption of GNSS signals for timing and positioning), with the solar maximum increasing the likelihood of such space weather disruptions in the coming years (ANV, 2022).

Another example of dependence on digital systems is the increasing shift to cloud infrastructure, which is explained in more detail in A.9 Cyber threats (RDI, 2023; Vuilleumier, 2023). Digital sovereignty may also be threatened due to shortages of components, chips or equipment. This may result in an overreliance on foreign market players, leading to a loss of control over digital infrastructure and increasing the risk of espionage and data breaches (RDI, 2023; Vuilleumier, 2023). Given the increasing automation and dependence on digital systems of critical infrastructure, cyber incidents in the ICT supply chain can cause cascade effects within critical infrastructure.

In addition, digitisation makes critical infrastructure more vulnerable to cyber-attacks. The perception is that such attacks can generally be mitigated if it concerns isolated incidents. However, if an attack is combined with another, non-intentional event, things become much more complicated. Think of an attack on rail carriers at the time of major track maintenance, or an attack on water authorities during a storm. Such compounding or cascading threats with a deliberate component become more likely in a geopolitically volatile world (Wells, 2022).

Physical vulnerabilities of critical infrastructure

The summer of 2023 saw a wide variety of different phenomena related to extreme weather (forest fires, (hail) storms, floods), both inside and outside Europe. In a number of countries, extreme weather events led to power cuts, public transport was shut down and airports were forced to close, among other things (NOS, 2023a; b). In the Caribbean part of the Kingdom, the probability of severe hurricanes is increasing and the hurricane season is getting longer. In 2022, Bonaire experienced heavy rainfall that flooded parts of the island and resulted in power cuts in some places (NOS, 2022). In the future, extreme weather events may lead to more frequent failure of critical processes in the Netherlands as well.[12] The question is whether processes can be restored in time in case of failure. This is true especially since extreme weather is a common cause failure, where several processes can be affected by one incident at the same time. The phenomenon of compounding or cascading threats is also relevant in this context. After all, when the probability of natural threats increases, the probability of different threats coinciding also increases (Argyroudis, 2020). In addition, climate change and the increase in extreme weather phenomena also put pressure on the supply of utilities such as clean drinking water and energy: salinisation diminishes the groundwater quality. Periods of extreme heat or cold can create a peak load on the grid due to an increased demand for energy to run air conditioning or heating.

Resilience of critical infrastructure

In addition to developments in the threat landscape, the implementation of European legislation for physical, digital and economic resilience of critical infrastructure, among other things, is an important development for this domain (NCTV, 2024a). Besides the Critical Entities Resilience (CER) and Network and Information Security 2 (NIS2) directives, the Cyber Resilience Act (CRA) and the Digital Operations Resilience Act (DORA) are European regulations that are relevant for (some of) the critical infrastructure providers. For the critical infrastructure domain, this means that more organisations will have to comply with the legislation. The number of critical infrastructure providers will therefore increase. In addition, the organisations involved will have to meet stricter requirements, including the establishment of a duty of care for taking security measures and a duty to report incidents. The CER and NIS2 will be implemented during the course of 2024 (NCTV, 2024b).

Energy supply: challenges regarding the energy transition

The energy transition involves working towards a new energy system in which energy demand is reduced, fossil fuels are phased out and the use of renewable energy sources such as solar, wind and biomass energy (Trias Energetica) is increased (Ministry of Defence, 2023). Several aspects of this transition could have national security implications. First, as a result of the energy transition, more and more businesses and households are switching to electricity as an energy source. This electrification is creating an increase in energy demand. A lot of work is being done to expand the capacity of the electricity grid, but the increase in capacity cannot keep up with the increase in demand. There are already problems with getting every business and household connected to the electricity grid and, for example, charging stations need to be switched off at regular intervals because of this

[12] For example, the energy sector (TenneT, 2023)

capacity shortage. This puts pressure on the continuity of electricity supply and the number of power cuts at the regional (neighbourhood) level may increase due to the electricity grid's limited capacity. In addition, this bottleneck may delay the energy transition and thus the sustainability of our energy system (Government of the Netherlands, 2024). Calls from regional grid operators for energy storage methods and flexible use are therefore growing, both for the industry and households (Government of the Netherlands 2023a; TenneT, 2024).

Second, the energy transition is material-intensive, which will increase the demand for certain minerals and metals in the coming years. Europe is heavily dependent on countries such as China, Turkey and the Democratic Republic of Congo for the supply of these critical raw materials. The supply of these materials could therefore be a bottleneck for the energy transition and could also be used as a geopolitical instrument by the countries that the Kingdom depends upon. A delay in the energy transition could in turn coincide with limited capacity of the energy grid, which could put further pressure on continuity of supply (European Parliament, 2023).

A third aspect of the energy transition is the use of hydrogen as an alternative energy source and carrier. To use hydrogen, among other things, a nationwide hydrogen transport network needs to be built. The Netherlands has ambitions to become a global hydrogen hub, with hydrogen being imported, stored and transported in our country. The use of hydrogen also carries risks, as it is highly flammable. In addition, it is odourless, colourless and tasteless, which makes leak detection by human senses difficult. This raises issues about how hydrogen infrastructure can be set up in a safe way (Gasunie, 2023).

A fourth aspect relevant to continuity of supply is the increasing dependence on solar and wind energy. When there is a lack of solar and wind energy for an extended period of time, this is referred to as *dunkelflaute*, which puts pressure on continuity of supply. When planning the new energy system, *dunkelflautes* can be taken into account by accommodating for these periods with other energy sources such as hydrogen or biomass.

The final relevant aspect of the energy transition in the context of this Trend Analysis is that digitisation and energy transition go hand in hand: the new energy infrastructure will increasingly make use of digital products such as smart meters and charging stations. This results in an increase in the energy system's digital attack surface, which is amplified by the high speed at which technology is developed and implemented. Moreover, visibility of vulnerabilities in these digital products is often limited, which makes this infrastructure more vulnerable.

Drinking water supply: pressure on groundwater quality

An important trend is the impact of pollution and climate change on the quality of groundwater. Climate change leads to sea level rise, which in turn leads to salinisation of groundwater. Salinisation is also increasing due to land subsidence and because rivers become saltier during periods of extreme drought due to reduced water discharge (Geudens, 2022). Groundwater is the main source for the extraction of drinking water; in addition, drinking water is extracted from surface water. Moreover, the use of plant protection products, nitrate from manure and residues from medicines and cosmetics negatively affect the quality of ground and surface water (Government of the Netherlands, 2018). This accumulation of factors means that the vulnerability of the drinking water supply has increased (Government of the Netherlands, 2018). In 2023, RIVM has warned that there are regional shortages in the supply of drinking water and that if no measures are taken, the whole of the Netherlands will experience a structural shortage from 2030 onwards (Van Leerdam, 2023; ILT, 2024). The fact that a period of prolonged drought will put pressure on the supply of drinking water from groundwater has been emphasized once more in 2024 by the PBL Netherlands Environmental Assessment Agency (PBL, 2024).

Threat assessment implications

Several developments such as those described above will have an impact on the continuity and availability of critical infrastructures. This affects various national security interests, including physical safety and territorial security (damage to digital space).

The Kingdom's physical safety and territorial security can be affected in various ways within the threat theme of critical infrastructure. First, (digital) attacks by state or activist/political actors can lead to sabotage of critical infrastructures, thus constraining their availability. Second, extreme weather events (forest fires, floods, storms) can cut off parts of the Kingdom from power and lead to the shutdown of critical infrastructures such as public transport. The question is whether these infrastructures can be restored in time in case of failure, especially when several of them are affected at the same time (compounding threats). In addition, critical infrastructure has already proven to be a target for digital attacks, damaging the integrity of the digital space. Finally, increasing pressure on the electricity grid is threatening the continuity of supply.

Section B
Technology watch and assessment

Technological developments have a significant impact on society. Technological applications are being developed at a rapid pace and efforts are being made to gain a technological advantage over others. In addition to playing a vital role in, among other things, Dutch earning power, technology is important for addressing (international) societal challenges. At the same time, there is also a downside to technological developments, with technological applications posing a threat to national security in various ways.

The large number of strategies, policy documents and scientific analyses on this subject reflects the need to gain control over the speed, impact and future of technological developments. The *Nationale* Technologiestrategie was published in early 2024, but reports on technological trends are published on an ongoing basis internationally.

Seven technology areas are discussed below. These technology areas are large families of technologies with numerous applications, whether or not in combination with technologies from other families. Given the limited scope of this Trend Analysis, it is impossible to give a complete overview of relevant technologies for national security. However, we do provide a brief overview of a number of important technological developments that are relevant in the context of national security.

Various sources were used to arrive at the selection of technology areas, including the aforementioned Nationale Technologiestrategie (Government of the Netherlands, 2024), the Herijking Sleuteltechnologieën (Van Bree, 2023), the technology trend reports of NATO Science & Technology Organization (Reding, 2023) and various publications from the private sector.

Table 1. Selection of 7 technology areas for the National Security Trend Analysis, including their definition

Artificial Intelligence	Artificial Intelligence (AI) is an umbrella term for a family of methods, models and algorithms inspired by human thinking and action, aimed at developing the ability of systems to exhibit intelligent behaviour (ANV, 2020).
Space technology	Space technology is technology aimed at the use of space through satellites, ground and communication stations and possibly, in the future, space weapons (Bronkhorst, 2020; US Department of Defence, 2020; NATO, 2024).
Quantum technology	Quantum technology is based on specific phenomena from quantum physics (such as entanglement and superposition) and uses the special behaviour of energy and matter at atomic and subatomic scale, or in other words the smallest quantum particles, to calculate, communicate and compute in a radically new way (Van Bree, 2023; Government of the Netherlands, 2023).
Robotics and autonomous systems	Robots are mechanical devices that can autonomously perform tasks in the air, on the ground, on or under water. To perform these tasks, robots are equipped with control technology and sensors (such as cameras, thermometers and light sensors). The technology is aimed at developing methods, tools and resources in the fields of mechanical structure, remote control and autonomy (Bronkhorst, 2020).
Photonics technology	Photonics technology focuses on generating, transporting and detecting light waves and light particles, also called photons (Government of the Netherlands, 2023; Bronkhorst, 2020; Photondelta, 2024).
Energy technology	Energy technology is a broad field that includes a range of technologies for the production, storage, transport and use of energy, such as technologies to harness energy from the environment (fossil fuels, nuclear power and renewable energy sources) (Bronkhorst, 2020).
Biotechnology	Biotechnology involves the modification of organisms with the aim of improving the functioning of organisms, plants, people or animals (COGEM, 2023).

B.1 Artificial Intelligence

Artificial Intelligence (AI) is an umbrella term for a family of methods, models and algorithms inspired by human thinking and acting, aimed at developing the ability of systems to exhibit intelligent behaviour (or, in other words, mimic human skills such as reasoning ability, image and speech recognition and learning ability) (ANV, 2020; Van Bree, 2023). AI is a technology area in which developments and breakthroughs follow each other in rapid succession and which is an important enabling technology for other innovations (Government of the Netherlands, 2024). It has many application possibilities. In the fields of energy transition, healthcare, mobility and the military, among others, AI can be used for e.g. optimisation, prediction, monitoring and diagnostics (Government of the Netherlands, 2023a; 2024). At the same time, there are also concerns about the responsible application of data processing, learning ability and decision-support models.

In the context of national security, the emergence of generative AI is an important development. Generative AI enables, among other things, the automatic generation of texts and (moving) images based on user input. One application of generative AI is a Generative Adversarial Network (GAN), where one neural network judges the realism of the output of another neural network (Gonzalez et al., 2024). Popular generative AI applications are OpenAI's ChatGPT (text generation) and Sora (video generation). While generative AI offers many opportunities (e.g. for the continued development of chatbots), this development also has significant downsides. The same technology can be used to produce disinformation, for instance. Not only can it increase the amount of disinformation, but also its quality since fake images and text are hardly distinguishable from real ones. Deepfakes can also offer interaction, for example, instead of just presenting a video of a talking person. In addition, the technology offers possibilities to combine real images with synthetic images. Moreover, disinformation is increasingly targeted to the target audience, in order to have greater impact (Janjeva, 2023). At the same time, AI applications offer enhanced capabilities for disinformation detection, perpetuating the cat-and-mouse game between attackers and defenders (Janjeva, 2023).

The application of AI also has an impact on digital security. GANs make it easier for less tech-savvy cyber-attackers to experiment with techniques for carrying out cyber-attacks (Janjeva, 2023). Moreover, AI systems can take over certain tasks related to, for example, discovering vulnerabilities in software (Hazell, 2023). Again, the issue here is that such technology can be used by attackers as well as for cybersecurity (see also Section A.9 Cyber threats).

One of the challenges with the further development and application of AI is the so-called predictability problem. We cannot always accurately predict what an AI system is going to do. This may not only create undesirable outcomes, but can also result in declining trust in AI systems and (government) organisations using such systems in the longer term (Taddeo, 2022). On the one hand, this uncertainty embedded in the predictability problem is due to the fact that AI systems (especially machine learning systems) are vulnerable to data manipulation (intentional or otherwise), causing the system to fail in unpredictable ways. Deliberate manipulation of AI systems (adversarial AI) can potentially have a major impact in a military context, such as missile defence systems that ignore a threat, or weapon systems that self-destruct or attack the wrong target (Galle, 2022).[13] On the other hand, insight in the rationale used by a system to come to a conclusion or make a decision is often limited. In addition, current systems simply cannot always properly handle (new or unexpected) data outside the training or simulation environment and thus are not robust in operational situations (Nurkin, 2022). Especially in the defence and security domain, this creates challenges in the effective application of commercially available technology (e.g. due to confidentiality of this data). Insufficient further technological development focused on these challenges and loss of confidence in AI systems give rise to concerns about lagging development of AI in high-risk applications (such as the defence domain) (Reding, 2023).

One of the ways in which Europe in particular is trying to tackle the predictability problem is by developing regulations aimed at the responsible use of AI.[14] Suppliers in the European market must meet a number of requirements, which should safeguard the quality of AI systems and increase trust in such systems (Government of the Netherlands, 2024). In addition, meaningful human control is an important concept with regard to the application of AI in the defence and security domain during all phases of governance, design, development and use (Heijnen, 2024).

A more concrete challenge is the capacity within the Netherlands, but also in the EU, to scale up and compete with foreign parties. This has partly to do with access to

[13] See also Section A.9 Cyber threats.

[14] This includes the GDPR, Digital Market Act regulation (DMA), Digital Services Act regulation (DSA), DA, DGA, AI regulation, NIS2 regulation Cyber Resilience Act regulation (CRA), the Cyber Security Act regulation (CSA) and 'Aanwijzing Algoritmes' established by the Chief Information Officer (CIO) of the Ministry of Defence. See, among other things, 'Defensie Strategie Data Science en AI 2023-2027' (Government of the Netherlands, 2023a)

computing power and associated infrastructure (for which there is dependence on foreign cloud providers) and partly with access to data (to train AI systems) (Government of the Netherlands, 2024). The United States and China in particular are frontrunners in the further development of AI (both in terms of hardware and software) and thus largely determine how AI is applied and data is used (AIVD, 2024; Reding, 2023; Government of the Netherlands, 2024).

B.2 Space technology

Space technology is technology aimed at the use of space through satellites, ground and communication stations. The technology includes the development of methods, tools and resources in the field of satellite observation, satellite communications and space weapons for purposes such as PNT (positioning, navigation and timing), early warning and Earth observation (Bronkhorst, 2020; US Department of Defence, 2020; NATO, 2024). The main technological developments in space technology are miniaturisation and increasing affordability of satellite missions (the platforms themselves as well as the launching capabilities), a decrease in vulnerabilities and dependence on Earth-based satellites, increasing bandwidth, and the development of counterspace capabilities (such as anti-satellite (ASAT) and directed energy weapons). This results in increased interest in space launches by both states and commercial parties and thus provides the opportunity to test space technology faster, more frequently and more efficiently.

In line with this, the number of satellites launched has increased dramatically in recent years, with constellations of smaller satellites being launched in particular. Such constellations are effectively networks of hundreds or thousands of connected satellite systems delivering low-latency broadband data, among other things. Due to developments in the field of miniaturisation, more and more actors are gaining access to the technology. The satellites also become more stable and have flexible configurations that can be utilised for multiple purposes. Examples include observation and surveillance, weather forecasting, broadband communications and internet access for remote areas (GCHQ, 2022). Also emerging are responsive space capabilities, i.e. the ability to quickly launch a satellite with a smaller rocket (rather than a joint launch) in response to an acute threat (DARPA, 2024).

In the context of national security, three developments in space technology are relevant. The first important development has to do with the militarisation of space as a continuation of geopolitical competition on Earth. States like China, the United States and Russia are moving from passive military use of space to actively integrating space into conventional military operations (Reding, 2023; Projectteam Statelijke Dreigingen, 2021). In early 2024, for example, there was consternation over a Russian anti-satellite weapon, about which the US government issued warnings. While it is unclear whether it concerned a nuclear-powered satellite (the most likely option) or an actual nuclear weapon (which could do little damage in space, apart from the electromagnetic pulse), it is an indication that geopolitical tensions are extending into space (Lillis, 2024; Wayenburg, 2024; Starling, 2024). States are claiming their stake in space and develop resources in and technologies related to the space domain, especially in the area of counterspace (Projectteam Statelijke Dreigingen, 2021; Reding, 2023). Counterspace technologies are directed at gaining dominance in space over other actors, with offensive actions targeting satellites, ground systems or the communications between them (Secure World Foundation, 2024). Outdated international space law (originating from 1960-1980) is no longer fit to deal with the large number of active (non-state) actors and new activities in space (Goguichvli, 2021).

Another important development in space technology in the context of national security is the lack of attention for the digital security of space infrastructure. In this regard, see also sections A.9 Cyber threats and A.10 Threats to critical infrastructure. This results in a lack of understanding of potential vulnerabilities. Satellites are used for a wide range of military and civilian applications, such as GPS, Earth observation and telecommunications (ENISA, 2022). In the case of disruption of GPS (a specific GNSS signal), disruptive cascade effects can occur, for example in critical infrastructure (Government of the Netherlands, 2022). In addition to dependencies on satellites for the purpose of positioning or timing, satellites are also widely used for Earth observation. Phenomena such as air pollution, deforestation, melting of the ice caps, subsidence of dykes and soil, drought and sea level rise are monitored from space (NSO, 2022). Moreover, the increasing congestion in space and the associated accumulation of space debris make collisions (forcing satellites to divert), or even a catastrophic chain reaction scenario such as the Kessler Syndrome[15], increasingly realistic, thus making space sustainability more urgent (Wall, 2022). Incidents affecting the availability, integrity and/or confidentiality of these satellite services could thus potentially have major socio-economic impacts (ENISA, 2022; Projectteam Statelijke Dreigingen, 2021; OECD, 2022).

A final development in space technology that is relevant to national security is the increasing number of commercial

[15] A hypothetical but feared scenario where a collision in space creates more space debris, which in turn creates more collisions, thus resulting in a positive feedback loop.

parties that are active in space, such as SpaceX, Blue Origin and Virgin Galactic (Ben-Itzhak, 2022; Reding, 2023; You, 2022). Particularly in the US, large sums of private money are invested in the development of satellites, making access to space cheaper and more flexible (NSO, 2022). In the war in Ukraine, we see how the US company SpaceX's Starlink satellite constellation is being used for (disrupting) military communications and the Internet (Miller, 2022). At the same time, such dependence on a commercial party also constitutes a vulnerability, as there is no guarantee that SpaceX will continue to provide the service.

B.3 Quantum technology

Quantum technology is based on specific phenomena from quantum physics (such as entanglement and superposition) and uses the special behaviour of energy and matter at atomic and subatomic scale, or in other words the smallest quantum particles, to calculate, communicate and compute in a radically new way (Van Bree, 2023). Quantum technology is seen as an enabling technology for new products and services. Application of quantum technology for these new products and services is mostly still in its infancy. The potential impact of quantum technology applications is therefore still partly unknown (Bronkhorst, 2020). Nevertheless, in the context of national security it is necessary to anticipate all kinds of quantum technology applications. Quantum technology is usually subdivided into three application areas: quantum computing, quantum communication (including quantum key distribution) and quantum sensing (Van Bree, 2023).

A highly relevant development in the field of quantum technology with a view to national security is the promise of the quantum computer.[16] It is expected that quantum computers can be used as a digital weapon to break current cryptographic standards. This means that encrypting sensitive information using those standards will not be enough (Neumann, 2021). Several (government) services, such as the Tax Administration, use Public Key Infrastructure (PKI). The technology can thus potentially be used to cause disruption or failure of critical processes. It is possible that actors are already storing encrypted communications to decrypt them once a quantum computer with sufficient computing power becomes available (TNO, CWI & AIVD, 2023). It is unclear when the technology will be mature enough to do so. Since some information will remain sensitive for a long period of time and could also damage national security if decrypted by malicious parties in ten, fifteen or twenty years' time, it is important that parties start to implement post-quantum cryptography now, in order to protect this information (AIVD, 2021; TNO, CWI & AIVD, 2023).

In addition, several applications in the military domain are conceivable that could have an impact on operations. Better sensors could greatly improve the effectiveness of radar systems, making it easier to detect enemy vehicles underwater and in the air. Stealth technologies could become less effective as a result (Lele, 2021). In addition, accurate clocks could be developed, enabling navigation in areas where GPS is not available (Reding, 2023). Quantum technology will not only offer new technological improvements and capabilities, but also requires the development of new (military) strategies, tactics, policies and threat assessments (Krelina, 2021).

The above developments also highlight the relevance of quantum technology in terms of strategic dependencies. For instance, in 2023, the European Commission identified quantum technology as one of the strategic focus areas for the upcoming European Economic Security Strategy. This strategy (still under development) aspires to provide a common framework for strategic autonomy by promoting competitiveness, protecting against risks that involve high-risk strategic dependencies and cooperating with partners (European Commission, 2023a). In addition, the European Commission has selected quantum technology as one of four technology areas (alongside advanced semiconductors, AI and biotechnology) considered most likely to carry the most sensitive and immediate risks in terms of undesired knowledge and technology transfer. Member states are advised to carry out a joint risk assessment for these technology areas (European Commission, 2023b). At the same time, unilateral export controls have also recently been imposed in areas including quantum technology[17], despite efforts within the EU to take such measures jointly. This not only creates the risk of a 'patchwork' of export-restrictive measures within the EU, but also of fragmentation of the common market within the EU (European Commission, 2024).

B.4 Robotics and autonomous systems (RAS)

Robots are unmanned systems that can perform tasks in the air, on the ground, on or under water autonomously. Robots are used to take over dull, dirty or dangerous tasks from humans, but also offer important offensive and defensive capabilities in areas such as intelligence gathering and the use of weapons. To perform these tasks, robots are equipped with control technology and

[16] See also the threat theme of cyber threats (A.9).

[17] For example in Spain in May 2023 (Ministerio de Industria, 2023) and in France in February 2024 (Haeck, 2024)

sensors (such as cameras, thermometers and light sensors). RAS technology is aimed at developing methods, tools and resources in the areas of mechanical structure, remote control and autonomous operation (Bronkhorst, 2020). Autonomy means that a system can act independently in an unexpected and uncertain situation, whereby human supervision and monitoring ensure that the autonomous systems stay within the imposed boundaries in all phases of development (design, implementation, evaluation and adaptation) (Reding, 2023; Elands, 2023). The functionality of autonomous systems is based on three pillars: a world model, intelligence (reasoning ability) and a task (goal function). Sensors play an important role in collecting information about the environment and about the functioning of the system itself, which serve to check the information against the world model.

A key driver in the further development of RAS are advances in AI, and thus the further development of autonomy in unmanned systems. An example of increasing autonomy can be seen in the concept of swarming (swarms of unmanned systems), where systems collaborate (Bronkhorst, 2020). Such swarms of systems have a potentially disruptive impact on the battlefield, for example because they can saturate (air) defence systems. The increase of autonomy in unmanned systems, and with it the concern about whether one can still control these systems, has been a long-time worry for the West, among others. This is true especially with regard to the development of Lethal Autonomous Weapon Systems (LAWS) (Rathenau Institute, 2021). International legal agreements have so far failed to materialise, but the technology continues to develop, also because such autonomous weapon systems can make use of developments in AI and civilian applications of autonomy (Reding, 2023). As discussed earlier for Artificial Intelligence, Western countries emphasise the need for meaningful human control. However, potential adversaries will have different legal and ethical frameworks regarding the development, application and deployment of AI systems for military use (Government of the Netherlands, 2023).

In recent conflicts, autonomous systems have been frequently deployed. Autonomous systems have played and still play an important role in the conflicts in Nagorno-Karabakh, Syria, Gaza and Ukraine (Detsch, 2021; Williams, 2023; Pol, 2022). Both Ukrainian and Russian armed forces use unmanned systems for (supporting) military operations in the air, on the ground and at sea. The systems are used to damage critical infrastructure, disrupt enemy supply lines, carry out surveillance and evacuation missions in hostile areas and destroy vehicles and personnel (Vos, 2023). Although the use of unmanned systems (drones) has a great impact on the battlefield, the drones deployed in the war in Ukraine are mostly controlled by human operators, are small and do not operate in a networked structure or only to a very limited extent. At the same time, parties do make innovative use of commercial, low-cost systems (often for single use) that can be adapted for military purposes (Pettyjohn, 2024). Drones are used to attack targets (military and equipment), for example, but primarily play an important role in intelligence gathering and surveillance (Pettyjohn, 2024). Due to the increased use of unmanned systems, counter-drone capabilities are taking off as well (think of nets, electronic warfare, digital attacks on software and more) (Reding, 2023; Pettyjohn, 2024).

B.5 Photonics technology

Photonics technology focuses on the generation, transport and detection of light waves and light particles, also known as photons. Photonics is similar to electronics, but instead of electrons, photons are used to transport information (Photondelta, 2024; Van Bree, 2023; Government of the Netherlands, 2023a). Photonics has very broad application possibilities within, among others, the following areas: manufacturing industry (e.g. production machines with lasers and 3D display technology), health (such as diagnostics and monitoring using light), agrifood sector (think of optical sensors for food safety and precision agriculture), semiconductors (e.g. for making chips using light), ICT (such as fibre optics and satellite communication), and energy and the environment (e.g. measuring particulate matter using optical sensors) (Parlementaire Monitor, 2018). The technology is used in numerous 'high-tech' products, not only in consumer products such as displays, cameras, phones, internet connections, solar panels and lighting (also in greenhouses, for example), but also in specific military products such as night vision goggles or various types of sensors for security applications. Photonics is also an important enabler for the further development of other technology areas, such as quantum technology and AI (PhotonicsNL, 2020; Government of the Netherlands, 2023a; 2024).

In the context of national security, we see a number of relevant developments. One of the most important developments in the field of photonics are communication applications. Particularly relevant are fibre optic networks and optical (satellite) communication, where information is sent over long distances via light. Given the relatively secure and robust connection via light signals, the application is highly relevant for the defence and security domain (Government of the Netherlands, 2024). Photonics technology is also important in the military domain for the further development of (optical) lasers, among other things (Reding, 2023). The UK has recently conducted a successful test with a laser directed-energy weapon, for example. Such weapons can hit targets with an intense

beam of light, disabling them or inflicting major damage (Optics.org, 2024).

An emerging subfield of photonics technology is integrated photonics. This involves the application of optical systems in the chip industry (Photonic Integrated Circuits, PICs). Photonic chips promise to be a more (energy) efficient future alternative to current electronic chips (Government of the Netherlands, 2023b).

Technologies used to produce very small semiconductor components (Extreme Ultraviolet Lithography (EUV) and optical metrology) are also subfields of photonics (Government of the Netherlands, 2024). Machines (such as those of ASML) apply patterns to a chip that form processor or memory elements. As mentioned earlier, the semiconductor industry is an important application area of photonics, especially in the Netherlands. In general, photonics companies within the EU experience challenges in the supply chain. These challenges involve not only shortages in materials, but also in intermediate products and machines, for which these companies are dependent upon suppliers outside the EU (Government of the Netherlands, 2023b). At the same time, export measures for the semiconductor industry reflect the geopolitical tensions between the US and China, among others, with China in particular also being dependent upon Western companies such as ASML.

B.6 Energy technology

Energy technology is a broad field that includes a range of technologies for the production, storage, transportation and use of energy, such as technologies to harness natural energy sources (fossil fuels, nuclear power and renewable energy sources) (Bronkhorst, 2020). The area is rapidly evolving due to the transition from the use of fossil energy to renewable energy. Because the energy transition affects many sectors of society, it attracts a lot of attention.

Developments in nuclear energy, renewable energy sources and sustainable fuels (such as biofuels and hydrogen) are particularly relevant (Reding, 2023). Second-generation biofuels such as cellulose, algae and waste oils are used for the production of, for example, bioethanol, but CO_2 and hydrogen (see also A.10 Threats to critical infrastructure) as raw materials for chemical technology are also emerging (COGEM, 2023). An important starting point is that technological advancements like these should not compete for materials with food production (COGEM, 2023). With the growing reliance on renewable energy and the increasing electrification of society, robust and reliable electricity storage (such as batteries, but also flywheels) becomes increasingly important (Reding, 2023).

Electricity storage is essential to accommodate peak electricity supply and demand, and so is decentralisation in order to create networks that are independent of each other. In section A.10 Threats to critical infrastructure, a more detailed explanation is given of the challenges surrounding the energy transition in relation to critical infrastructure. In the military domain, the supply of fuel is currently one of the critical issues for operational continuity. This is partly because weapon systems require more energy (e.g. laser applications). Electricity storage is therefore also becoming increasingly important in this context (Ministry of Defence, 2023).

In addition, technological developments with regard to energy transmission (such as micro grids for the built environment), heat networks and other ways to promote flexibility in the energy system are important, especially when it concerns a stable electricity grid (Government of the Netherlands, 2023a; Reding, 2023). At the same time it is crucial within critical infrastructure, for instance, to pay attention to the 'intermediate phase'. This is the stage when new technologies for the energy transition have not yet been developed to the fullest but are already being implemented alongside existing infrastructure and technology. In this phase it should be ensured that new and existing technologies can be linked, while guaranteeing the continuity of electricity supply (TenneT, 2023).

It should be noted that Dutch and European strategic autonomy is limited when it comes to the further development of energy technologies. On the one hand, the energy supply itself is used as a strategic weapon by, for instance, Russia. On the other hand, there is dependence in the area of the actual development of and research into renewable energy sources, especially on China, which has itself set the goal of being carbon neutral by 2060 (Government of the Netherlands, 2024). In addition to such investments, China is also dominant in the value chain of rare earths that are crucial for battery technology, for example (Government of the Netherlands, 2023a). Apart from investments in emerging technologies such as sodium ion, which require fewer critical raw materials, the Nationale Technologiestrategie states, among other things, that we should "strive for a sustainable and resilient supply chain for critical raw materials to minimise potential risks and promote the energy transition in a reliable and stable manner". (Government of the Netherlands, 2024, p.81). A key initiative in response to the finding that the EU is highly dependent on other countries for critical raw materials is the EU's Critical Raw Materials Act (2023/0079) (European Commission, 2023). This regulation includes a set of actions to ensure that the EU has and maintains access to a secure, diversified, affordable and sustainable supply of critical raw materials. Investigations are also

ongoing into recycling (of wind turbine blades, for example (TNO, 2024)) as a possible (partial) solution to the shortage of materials (Pommeret, 2022).

B.7 Biotechnology

Biotechnology is a technology that uses living organisms, cells or their components to develop new products. Thanks to developments in sequencing (determining the base order in genetic material), gene editing (making highly specific changes to the genome)[18] and genetic modification (adaptation of genetic material in a way that is not possible in nature), combined with the further development of technologies such as information technology and automation, biotechnology is on the rise. This makes it possible to apply biotechnology on an ever-larger scale (COGEM, 2023). The technology is used, for example, to improve crops (such as plant or seed breeding), in healthcare (such as fighting diseases), and for industrial applications (such as replacing environmentally harmful substances with biological materials) (Government of the Netherlands, 2024). A colour classification of the application areas of biotechnology is often used: industrial applications (white), agriculture and food (green), medical and health (red), and maritime (blue) (Van Bree, 2023).

In the context of national security, this technology area also has both civilian and military applications and is thus dual-use in nature. For instance, developments in synthetic biology allow very precise modifications to existing organisms or even the creation of entirely new organisms. Synthetic biology gained prominence with the rapid development of a COVID-19 vaccine (GCHQ, 2022). The techniques used for vaccine development can also be used to (re)create a virus (Van Weerd, 2021). Developments in precision health, using knowledge of DNA (for the purpose of personalised treatment of diseases) (COGEM, 2023; Reding, 2023), also have potentially malicious applications. For example, biological weapons could be developed that target people with specific genetic characteristics, and genetic information could be abused to identify and discriminate against ethnic groups on the basis of race. It is therefore essential to (digitally) secure databases where DNA codes are stored[19] (Luca, 2023). Government databases such as the UK Biobank[20] are crucial for training algorithms on anonymised data, for example, in order to conduct research into underlying causes of certain diseases. However, this also makes them a target of criminals and other malicious parties (Alder, 2023; Kuntz, 2024). In late 2023, for example, the company 23andMe was targeted in a massive data breach, in which data from almost seven million users was stolen. Cybercriminals gained access to certain personal data, such as family trees, year of birth and geographical location, by using login details that were exposed in previous hacks (McCallum, 2023; The Guardian, 2024).

Biotechnology applications can be used for human enhancement, but not all human enhancement techniques are biotechnology in the sense that (components of) cells or living organisms are used. Human enhancement revolves around improving people's physical, cognitive, physiological, sensory or social functions (Reding, 2023). However, apart from the ethical and legal frameworks, research into human genetic modification and gene therapy is still at an early stage because they are highly complex processes. Moreover, at the moment the most gains can be made in the field of training or other external, relatively simple interventions (Van Weerd, 2021). In this context, it is relevant to mention the recent developments around Neuralink, Elon Musk's company that is focused on neurotechnology and the development of brain-computer interfaces (BCIs, brain implants). Such BCIs are designed to control a computer using thoughts, making them a form of human enhancement. However, the first applications are envisaged for people who are paralysed. Creating links with, for instance, AI to make people think faster is something for a very distant future. The company claims to have succeeded in inserting a BCI into a human being for the first time in February 2024, providing only very limited additional information about the patient in question (Guarino, 2024).

The EU has stricter regulations on biotechnology than, for instance, China, given the political and social emphasis on ethical considerations with regard to genetic modification (Government of the Netherlands, 2024). At the same time, the technology continues to develop. This carries the risk that at some point Europe will be confronted with technological applications in the defence and security domain without having developed the appropriate countermeasures.

[18] Gene editing (making highly specific changes to the genome) has taken off since the application of the CRISPR-Cas9 system (Clustered regularly interspaced short palindromic repeats (CRISPR) associated protein) over 10 years ago. This makes it relatively easy to create a break at a specific site in the DNA and modify the genome at that site (COGEM, 2023)

[19] Also think of companies offering online services to research genealogy based on genetic material.

[20] See *https://www.ukbiobank.ac.uk/* for more information on the UK Biobank.

Section C
Methodology

A number of methodical steps were followed to arrive at the National Security Trend Analysis.

Step 1: listing of developments outlined in the NRA
The Trend Analysis discusses new developments since the drafting of the National Risk Assessment (NRA) and the status of those already included in the NRA. Therefore, the first step in the analysis involves listing all the developments included in the NRA for each of the threat themes. These threat themes are:

- Infectious diseases;
- Climate and natural disasters;
- Major accidents;
- Social polarisation, extremism and terrorism;
- Foreign subversion of the democratic constitutional system (*including organised crime*);
- International and military threats;
- Economic threats;
- Cyber threats;
- Threats to critical infrastructure.

Step 2: two-track literature scan
Subsequently, a comprehensive literature scan was performed along two tracks. On the one hand, it concerned a scan from the perspective of the threat themes discussed in the NRA.[21] This means that a search was done for relevant developments from the perspective of infectious diseases, for example. This search focused both on the status of developments already included in the NRA and on new developments. On the other hand, a scan was performed from the perspective of more autonomous developments in the social, technological, ecological, economical and (international) political (STEEP) domains. When these two tracks are combined, a complementary picture of developments relevant to national security emerges (see step 3). The organisations within the ANV created several scan teams that looked at a number of topics (threat themes or autonomous developments). Whenever possible, a match was made with the expertise of the organisations in question.

In the literature scan, different types of sources were consulted. These included academic literature, grey literature in the form of reports from governments and (inter)national organisations, as well as news reports. Only new developments that have occurred since the first quarter of 2022 when the NRA analysis was performed, or about which more information has become available since then or which have manifested themselves differently than previously expected, were included in the literature scan. The Trend Analysis includes publications that were published up to and including 31 May 2024. In terms of time horizon, the primary focus is on developments that will be significant for the remaining duration of the Security Strategy for the Kingdom of the Netherlands, up to and including 2029. For a number of more long-term developments, such as those regarding climate change, we have deviated from this limit, especially since these and other movements also have longer lead times in terms of possible measures and policies. The findings from the literature scan were supplemented and validated through in-depth interviews with content experts. For the interpretation and retrieval of developments for the Caribbean part of the Kingdom, a separate session was organised with representatives of the countries and public bodies.

Step 3: exchanging information on developments
Whereas the scan for developments was designed based on the individual threat themes and developments in the broader domains, an explicit function of the Trend Analysis is also to provide insight into the possible connections between them. Therefore, the next step was to exchange information about the developments for the various topics scanned. For each of the developments identified, we assessed whether they might also apply to another threat theme or autonomous development. In order to do so,

[21] The NRA contains nine threat themes. However, the Trend Analysis looks at ten themes. The reason for this is that the topic of organised crime was included in the NRA in an umbrella theme, but is presented separately in the Trend Analysis. This is to match the way in which organised crime has been included in the Security Strategy.

a work session was organised with all scan teams, at which the following two questions were asked:

- Which developments from threat theme X potentially affect threat theme Y and should also be included as developments within this theme?
- Which findings from the perspective of the five autonomous developments are relevant to the individual threat themes and should also be included as developments within those themes?

The step resulted in a more complete and integral picture of the relevant developments for each threat theme and autonomous development.

Step 4: summary and integral overview of developments (what's new?)

Based on the findings from the previous steps, we also created a summary and integral overview of developments. This mainly looked at developments that may have broad implications for multiple threats, for example, and that may also interact extensively with other developments. This overview focuses mainly on the question *'what's new?'* and is designed along the lines of the STEEP domains, as also used in the literature scan. The objective of the overview is not only to highlight some of the key findings from the previous steps, but also to pay particular attention to cross-connections.

Step 5: interpretation of implications – strategic insights and consequences for the security assessment

The fifth step involves interpreting the implications of all developments considered. This interpretation takes place at three different levels of abstraction. First of all, for each threat theme the possible consequences of related developments for the threat assessment of the relevant theme as outlined in the NRA are indicated. This interpretation is mainly based on the implications of developments for the six national security interests compared to the 2022 analysis, where applicable also focusing on the expected frequency of the threat(s) in question. However, it is important to stress that the Trend Analysis is not a risk assessment. This means that no explicit statement is made about changes in impact and likelihood scores for the various threat scenarios presented in the NRA. Second, an interpretation of the broader developments as viewed from the STEEP domains is provided in a similar manner. It focuses primarily on the implications for national security (interests) in general and the threats for which the broader developments may be relevant. Third, an interpretation of the consequences at a more strategic level of abstraction is provided. In this case, the primary question is which dynamics we see when we compare the developments from the Trend Analysis. This interpretation adopts more of a systems perspective, building on the overviews created in step four. It also includes a look at possible questions and challenges for further strategy development.

Difference with previous ANV horizon scans

The approach of the Trend Analysis 2024 differs in several respects from previous, similar ANV products such as the 2018, 2019 and 2020 horizon scans. For instance, this edition puts greater emphasis on both the implications and coherence of the various developments. This translates, among other things, into an overview with insights at the strategic level. At the same, this Trend Analysis also pays more attention to developments (and their implications) from the perspective of the various threat themes. This partly stems from another difference, which is that the Trend Analysis, unlike its predecessors, is explicitly linked to other analysis and strategy documents. These are the NRA on the one hand and the Security Strategy on the other. Furthermore, the creation of the Trend Analysis involved more structured and frequent consultation with the clients for whom it was made. For this purpose, a steering committee was formed, which also included representatives from the Caribbean part of the Kingdom. Finally, the way in which the findings are presented is also different from many of the other ANV products. Instead of organising the report in the same order as the analytical steps described above, the main report highlights the more strategic and overarching findings.

Section D
The National Network of Safety and Security Analysts

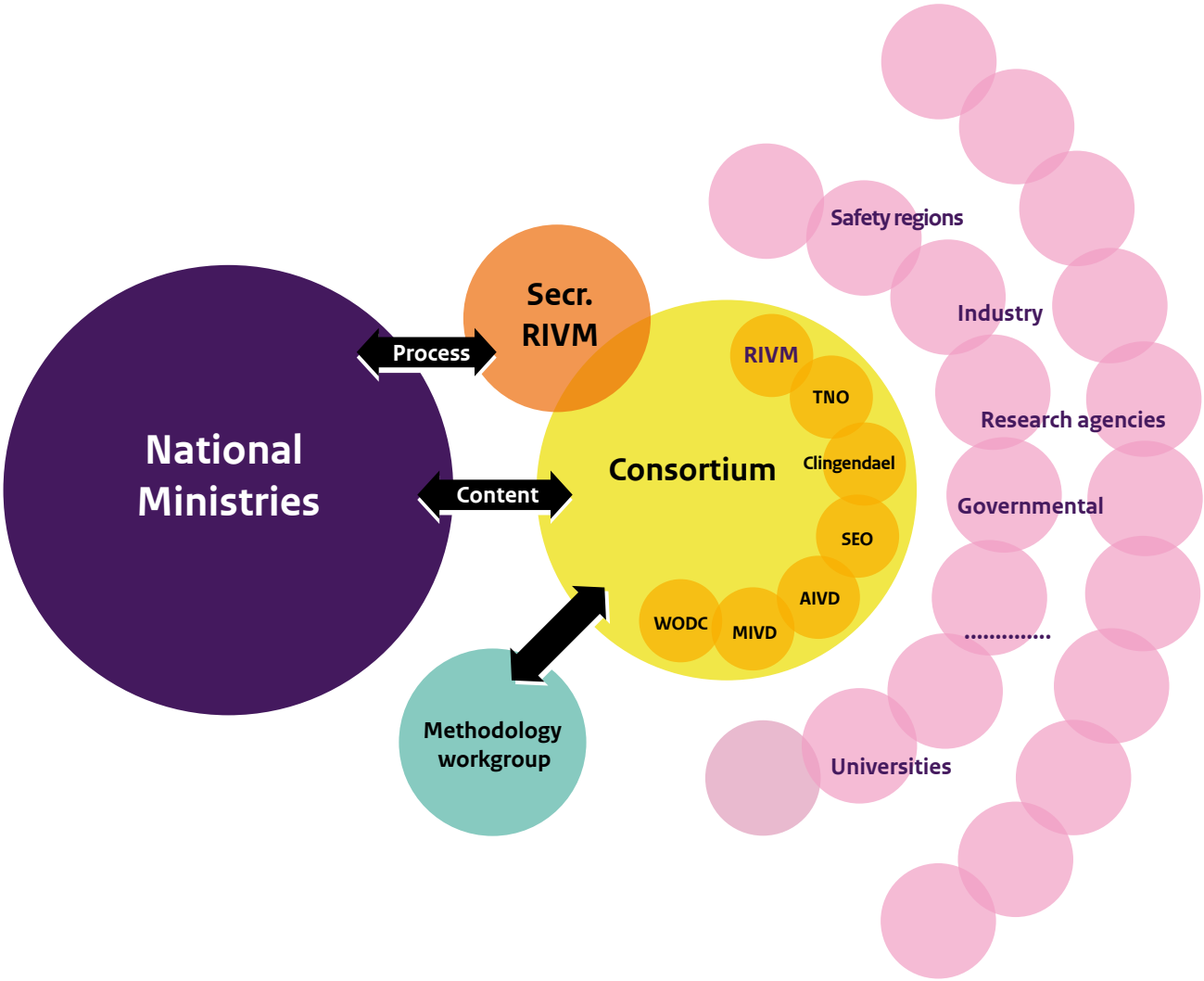
The National Network of Safety and Security Analysts (ANV) is a knowledge network that was established in 2010. At the request of the Ministry of Justice and Security, the network has since then prepared national risk assessments and other in-depth analysis studies in the area of national security on behalf of the former National Security Steering Group (Stuurgroep Nationale Veiligheid, SNV). The ANV compiled the National Security Profile in 2016 and the 2019 and 2022 National Risk Assessments.

The ANV consists of a permanent core of seven organisations surrounded by a network (the 'ring') of organisations, such as knowledge institutions, research agencies, civil services, safety regions, (essential) businesses and consultancy firms, which are engaged in the production of analyses and in-depth studies, depending on the knowledge requirements. The permanent core consists of:

- The National Institute for Public Health and the Environment (RIVM)
- The Netherlands Organisation for Applied Scientific Research TNO
- The Netherlands Institute of International Relations 'Clingendael'
- SEO Amsterdam Economics
- The General Intelligence and Security Service (AIVD)
- The Military Intelligence and Security Service (MIVD)
- Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC)

These organisations possess wide-ranging, multidisciplinary expertise and therefore collectively span the National Security work field. This structure guarantees the all-hazard approach of ANV products as well as the uniformity of the methodology and cross-disciplinary analysis. Monitoring and further development of the methodology used by the ANV is in the hands of a working group dedicated to that purpose. The seven core organisations, united in the Consortium, share responsibility for the quality of the contents of the NRA and other products. Specific, supplementary expertise is provided by the other organisations in the network. The organisations in the core and the ring ensure that experts and analysts are made available to sit on working groups, which undertake the various activities in continuously varying compositions. There is also a supporting secretariat (the ANV Secretariat) made up of a general secretary and project support personnel, who provide process management, progress monitoring and support for the creation of the different products. The ANV Secretariat acts as the fixed point of contact for the principal and is housed within the RIVM. The organisational structure of the National Network of Safety and Security Analysts is shown in the following figure.

Figure 1. Network structure of the ANV



References

Introduction

ANV (National Network of Safety and Security Analysts). 2022. *Rijksbrede Risicoanalyse Nationale Veiligheid – Hoofdrapport.* Available at: *https://www.rivm.nl/nationale-veiligheid*

A.1 Climate and natural disasters

Academische Werkplaats Gezonde Leefomgeving (June 2023). *Wie houdt het hoofd koel?* Available at: *https://www.awgl.nl/images/projecten/2023/230710%20Onderzoeksrapport%20Wie%20houdt%20het%20hoofd%20koel.pdf*

Central Bank of Curaçao and Sint Maarten (December 2023). *Economic bulletin. Winds of Change: Adapting to Climate Change*. December 2023. Available at: *https://cdn.centralbank.cw/media/economic_bulletins_2023/20231213_economic_bulletin_december_2023.pdf*

European Environment Agency (EEA) (2022). *Climate change as a threat to health and well-being in Europe: focus on heat and infectious diseases*. EEA Report No 07/2022. Available at: *https://www.eea.europa.eu/publications/climate-change-impacts-on-health*

Government of the Netherlands (2024). *Afbouw gaswinning Groningen.* Consulted on 19 April 2024, available at: *https://www.rijksoverheid.nl/onderwerpen/gaswinning-in-groningen/afbouw-gaswinning-groningen*

KNMI (Royal Netherlands Meteorological Institute). (9 October 2023). KNMI'23-klimaatscenario's voor Nederland. Available at: *https://www.knmi.nl/research/publications/knmi-23-klimaatscenario-s-voor-nederland*

KNMI (Royal Netherlands Meteorological Institute). (2 January 2024). *Jaaroverzicht aardbevingen.* Consulted on 10 August 2023, available at: *https://www.knmi.nl/over-het- knmi/nieuws/jaaroverzicht-aardbevingen-2023*

NIPV (Netherlands Institute for Public Safety). (23 January 2023). *Natuurbrandsignaal '23.* Consulted on 9 October 2023, available at: *https://nipv.nl/natuurbrandsignaal-23-meer-onbeheersbare-natuurbranden-met-grotere-impact-op-samenleving/*

NOS (9 November 2022). Bonaire kampt met hevige regenval, straten overstroomd. *NOS Nieuws.* Consulted on 6 March 2024, available at: *https://nos.nl/artikel/2451698-bonaire-kampt-met-hevige-regenval-straten-overstroomd*

Nu.nl (2023). Nederlands klimaat wordt extremer: nattere winters, drogere en hetere zomers. *Nu.nl.* Consulted on 6 March 2024, available at: *https://www.nu.nl/klimaat/6284004/nederlands-klimaat-wordt-extremer-nattere-winter-maar-veel-drogere-en-hetere-zomer.html*

OECD (2023), *Taming Wildfires in the Context of Climate Change*, OECD Publishing, Paris. Available at: *https://doi.org/10.1787/dd00c367-en*

PBL (Netherlands Environmental Assessment Agency). (2024). *Klimaatrisico's in Nederland; De huidige stand van zaken.* The Hague: PBL (Netherlands Environmental Assessment Agency). Available at: *https://www.pbl.nl/system/files/document/2024-05/pbl-2024-klimaatrisicos-in-nederland-5359.pdf*

RIVM (National Institute for Public Health and the Environment). (31 May 2021). *Klimaatverandering leidt nu al tot meer sterfte door hitte.* Consulted on 9 November 2023, available at: *https://www.rivm.nl/nieuws/klimaatverandering-leidt-nu-al-tot-meer-sterfte-door-hitte*

Stamper, M. (8 June 2023). 'Eilanders moeten anders gaan denken over klimaatverandering'. *Caribisch Netwerk.* Consulted on 6 March 2024, available at: *https://caribischnetwerk.ntr.nl/2023/06/08/eilanders-moeten-anders-gaan-denken-over-klimaatverandering/*

United Nations. (18 July 2023). *Health risks on the rise as heatwave intensifies across Europe: WMO.* Consulted on 9 November 2023, available at: *https://news.un.org/en/story/2023/07/1138802*

A.2 Infectious diseases

Carter, S. et al., (30 October 2023). *The Convergence of Artificial Intelligence and the Life Sciences.* NTI bio. Available at: *https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_Executive-Summary_FINAL.pdf*

Kaiser, J. (17 March 2023). Growing number of high-security pathogen labs around world raises concerns. ScienceInsider. Available at: *https://www.science.org/content/article/growing-number-high-security-pathogen-labs-around-world-raises-concerns*

NOS. (15 March 2024). Vijf vragen over de dalende vaccinatiegraad. NOS Nieuws. Available at: *https://nos.nl/artikel/2512871-vijf-vragen-over-de-dalende-vaccinatiegraad*

RIVM (National Institute for Public Health and the Environment). *Infectieziekten.* Consulted on 14 March 2024, available at: *https://www.rivm.nl/klimaat-en-gezondheid/infectieziekten*
RIVM (National Institute for Public Health and the Environment). (29 June 2023). Vaccinatiegraad en jaarverslag Rijksvaccinatieprogramma Nederland 2022. Available at: *https://www.rivm.nl/bibliotheek/rapporten/2023-0031.pdf*
RIVM (National Institute for Public Health and the Environment). (20 December 2023). Staat van infectieziekten in Nederland, 2022. Available at: *https://www.rivm.nl/bibliotheek/rapporten/2023-0396.pdf*

A.3 Major accidents

ANVS (Authority for Nuclear Safety and Radiation Protection). (26 March 2023). Veiligheid kerncentrales Oekraïne. Available at: *https://www.autoriteitnvs.nl/actueel/nieuws/2022/02/25/situatie-in-oekraine*
AVIV. (23 March 2023). Rapport toetsing realisatiecijfers vervoer gevaarlijke stoffen over het spoor aan de risicoplafonds Basisnet. Gasunie. Waterstofnetwerk Nederland. Available at: *https://www.gasunie.nl/projecten/waterstofnetwerk-nederland*
Gasunie. (30 May 2024) *Waterstofnetwerk Nederland.* Available at: *https://www.gasunie.nl/projecten/waterstofnetwerk-nederland*
Geelen, L.M.J. et al. (22 September 2023). De bijdrage van Tata Steel Nederland aan de gezondheidsrisico's van omwonenden en de kwaliteit van hun leefomgeving. doi: 10.21945/RIVM-2023-0171
Porthos. CO_2-reductie door opslag onder de Noordzee. Available at: *https://www.porthosco2.nl/*
RIVM (National Institute for Public Health and the Environment). (30 May 2024a). RIVM houdt nucleaire situatie in Oekraïne in de gaten. Available at: *https://www.rivm.nl/straling-en-radioactiviteit/stralingsincidenten-en-kernongevallen/oekraine*
RIVM (National Institute for Public Health and the Environment). (30 May 2024b). *Verkenning Chemours en Westerschelde.* Available at: *https://www.rivm.nl/industrie/onderzoeken/verkenning-chemours-westerschelde*

A.4 Social polarisation, extremism & terrorism

Algemeen Dagblad (AD). (4 October 2022). Vertrouwen boeren in overheid is helemaal weg: ' Ze weten niet waar ze over praten'. Available at: *https://www.ad.nl/binnenland/vertrouwen-boeren-in-overheid-is-helemaal-weg-ze-weten-niet-waar-ze-over-praten~a1196e8d/?referrer=https%3A%2F%2Fwww.google.com%2F*
AIVD (General Intelligence and Security Service). (17 April 2023). AIVD-jaarverslag 2022. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022*
AIVD (General Intelligence and Security Service), Netherlands Police & NCTV (National Coordinator for Counterterrorism and Security). (9 April 2024). Met de rug naar de samenleving: Een analyse van de soevereinenbeweging. Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2024/04/09/tk-bijlage-24401640-fenomeenanalyse-soevereinen*
CBS (Statistics Netherlands). (9 May 2023). *Minste vertrouwen in Tweede Kamer in 10 jaar tijd.* Available at: *https://www.cbs.nl/nl-nl/nieuws/2023/19/minste-vertrouwen-in-tweede-kamer-in-10-jaar-tijd*
Dutch Media Authority. (14 June 2023). *Digital News Report Nederland 2023*. Available at: *https://www.cvdm.nl/wp-content/uploads/2023/06/CvdM-DigitalNewsReport-2023.pdf*
Macaskill, A., Holden, M., Marsh, S. (24 November 2023). Gaza war increases risk of Islamist attacks in Europe, security officials say. Reuters. Available at: *https://www.reuters.com/world/europe/gaza-war-increases-risk-islamist-attacks-europe-security-officials-say-2023-11-24/*
Movisie. (November 2023). Themadossier Israel-Palestina. Available at: *https://www.movisie.nl/artikel/israel-palestina-hoe-blijven-we-nederland-verbinding*
Mulder, J. (14 June 2023). Jongere haalt nieuws steeds meer van sociale media zoals TikTok, maar vertrouwt die minder. *Trouw.* Available at: *https://www.trouw.nl/binnenland/jongere-haalt-nieuws-steeds-meer-van-sociale-media-zoals-tiktok-maar-vertrouwt-die-minder~b3fc37ed/?referrer=https://www.google.com/*
NCTV (National Coordinator for Counterterrorism and Security). (2023a). Dreigingsbeeld Terrorisme Nederland December 2023. Available at: *https://www.nctv.nl/onderwerpen/dtn*
NCTV (National Coordinator for Counterterrorism and Security). (2023b). Dreigingsbeeld Terrorisme Nederland 58. Available at: *https://www.nctv.nl/documenten/publicaties/2023/05/30/dreigingsbeeld-terrorisme-nederland-58*
NCTV (National Coordinator for Counterterrorism and Security). (12 December 2023). Dreigingsbeeld Terrorisme Nederland. Available at: *https://www.nctv.nl/onderwerpen/dtn*
Reuters. (24 November 2023a). Gaza war increases risk of Islamist attacks in Europe, security officials Say. *Reuters.* Available at: *https://www.reuters.com/world/europe/*
Reuters. (14 December 2023b) Seven arrested in Germany, Denmark, the Netherlands over suspected terrorism plots. Available at: *https://www.reuters.com/world/europe/copenhagen-police-danish-intelligence-make-arrests-suspicion-preparations-attack-2023-12-14/*

RIVM (National Institute for Public Health and the Environment). (26 September 2022). Rijksbrede Risicoanalyse 2022. Available at: *https://www.nctv.nl/documenten/publicaties/2022/09/26/rijksbrede-risicoanalyse-nationale-veiligheid*

A.5 Foreign subversion of the democratic constitutional system

AIVD (General Intelligence and Security Service). (2023). AIVD-jaarverslag 2022. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022*

AIVD (General Intelligence and Security Service). (2024a). *AIVD-jaarverslag 2023*. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

AIVD (General Intelligence and Security Service). (2024b). Strafbaarstelling van moderne spionagevormen. Available at: *https://www.aivd.nl/onderwerpen/spionage/strafbaarstelling-van-moderne-spionagevormen*

Albertini, A. (7 November 2023). Etoiles de David taguées à Paris : la piste d'une opération d'ingérence russe privilégiée. Le Monde. Available at: *https://www.lemonde.fr/societe/article/2023/11/07/pochoirs-d-etoiles-de-david-a-paris-la-piste-d-une-operation-d-ingerence-russe-privilegiee_6198775_3224.html*

AWTI (Advisory Council for Science, Technology and Innovation). (28 November 2022). Advies: Kennis in conflict - veiligheid en vrijheid in balans. Available at: *https://www.awti.nl/documenten/adviezen/2022/11/29/index*

Bischoff, K. (30 May 2023). AI tools in hybrid warfare - A double-edged sword. Risk Intelligence. Available at: *https://www.riskintelligence.eu/background-and-guides/ai-tools-in-hybrid-warfare-a-double-edged-sword*

Bolle, J. (18 February 2024). In Den Haag botste de lange arm van het Eritrese regime met de vuist van de oppositie – en niet voor het eerst. De Volkskrant. Available at: *https://www.volkskrant.nl/binnenland/in-den-haag-botste-de-lange-arm-van-het-eritrese-regime-met-de-vuist-van-de-oppositie-en-niet-voor-het-eerst~b110f345/European Commission. (2023). Critical Raw Materials Act. Available at: https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en*

European Commission. (2024). EU Chips Act. Available at: *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en*

Government of the Netherlands. (28 February 2022). Strafbaarstelling spionage gemoderniseerd. Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2022/02/28/strafbaarstelling-spionage-gemoderniseerd*

Houtkamp, C., Drost, N. (2023). *Oekraïense en Russische gemeenschappen in Nederland.* Clingendael Institute. Available at: *https://www.clingendael.org/sites/default/files/202305/Oekra%C3%AFense%20en%20Russische%20gemeenschappen%20in%20Nederland.pdf*

Kingston, T. (4 January 2024). European Navies try to Keep up in Cat-and-Mouse Game of Seabed Warfare. *Defense News*. Available at: *https://www.defensenews.com/global/europe/2024/01/04/european-navies-try-to-keep-up-in-cat-and-mouse-game-of-seabed-warfare/*

Martin, M. (12 March 2024). Houthi attacks in Red Sea threaten internet infrastructure. Deutsche Welle. Available at: *https://www.dw.com/en/houthi-attacks-in-red-sea-threaten-internet-infrastructure*

Ministry of Economic Affairs and Climate Policy. (2023). Wet veiligheidstoets op investeringen, fusies en overnames. Available at: *https://www.bureautoetsinginvesteringen.nl/het-stelsel-van-toetsen/wet-veiligheidstoets-investeringen-fusies-en-overnames*

MIVD (Military Intelligence and Security Service). (19 April 2023). MIVD Openbaar Jaarverslag 2022. Available at: *https://open.overheid.nl/documenten/ronl-fe92eb9796cac86ecf33c8fdd97167cd1543df8a/pdf*

NOS. (18 February 2024). *Waarom voor- en tegenstanders van het Eritrese regime met elkaar botsen.* Available at: *https://nos.nl/artikel/2509365-waarom-voor-en-tegenstanders-van-het-eritrese-regime-met-elkaar-botsen*

Okano-Heijmans, M. (18 January 2023). Ontkoppelen is niet de oplossing voor ons probleem met China. Clingendael. Available at: *https://spectator.clingendael.org/nl/publicatie/ontkoppelen-niet-de-oplossing-voor-ons-probleem-met-china*

Ramdharie, S. (12 February 2024). Europese landen waarschuwen voor grote Russische desinformatie-campagne. De Volkskrant. Available at: *https://www.volkskrant.nl/nieuws-achtergrond/europese-landen-waarschuwen-voor-grote-russische-desinformatie-campagne~ba31a7f7/*

Scott, M. (10 March 2022). As war in Ukraine evolves, so do disinformation tactics. Politico. Available at: *https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/*

A.6 Organised crime

Ministry of Justice and Security. (2023). *Voortgangsrapportage aanpak georganiseerde criminaliteit.*

NCTV (National Coordinator for Counterterrorism and Security). (3 July 2023). *Cybersecuritybeeld Nederland 2023.* Available at: *https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023*

Netherlands Police. (2023). *Mogelijke verdubbeling explosie-incidenten.* Available at: *https://www.politie.nl/nieuws/2023/juli/16/mogelijke-verdubbeling-explosie-incidenten.html*

NOS. (22 March 2024). Dit jaar al 250 vuurwerkaanslagen ondanks maatregelen. *NOS*. Available at: *https://nos.nl/artikel/2513720-dit-jaar-al-250-vuurwerkaanslagen-ondanks-maatregelen*

UK National Cyber Security Centre. (March 2023). *ChatGPT and large language models: what's the risk?* Available at: *https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk*

Van Nierop, L. (26 May 2023). Als de oorlog in Oekraïne voorbij is, gaan de westerse wapens zwerven. *NRC*. Available at: *https://www.nrc.nl/nieuws/2023/05/26/als-de-oorlog-in-oekraine-voorbij-is-gaan-de-westerse-wapens-zwerven-a4165707*

WODC (Research and Documentation Centre). (28 December 2023). *Update liquidaties 2022*. Available at: *https://repository.wodc.nl/handle/20.500.12832/3328;*

WODC (Research and Documentation Centre). (30 December 2021). *2e verkennende studie liquidaties*. Available at: *https://repository.wodc.nl/handle/20.500.12832/3136*

A.7 International and military threats

Al Hussein, M. (16 January 2024). *The Gaza War May Radicalize the Gulf*. Carnegie Endowment for International Peace. Available at: *https://carnegieendowment.org/sada?lang=en*

Al Jazeera. (29 August 2023). Taiwan warns of surge in tensions as Chinese fighter jets cross median line. *Al Jazeera*. Available at: *https://www.aljazeera.com/news/2023/8/29/taiwan-warns-of-surge-in-tensions-as-chinese-fighter-jets-cross-median-line*

Ayres, A. (21 June 2023). India Is Not a U.S. Ally–and Has Never Wanted to Be. *Time Magazine*. Available at: *https://time.com/6288459/india-ally-us-modi-biden-visit/*

Bugos, S. et al. (November 2023). Russia Withdraws Ratification of Nuclear Test Ban Treaty. *Arms Control Association*.

Clingendael Institute. (2024). *Strategische Monitor 2023: Barsten en Blokken*. Available at: *https://www.clingendael.org/publication/strategische-monitor-2023-barsten-en-blokken*

Diwan, I., Alaya, H., Meddeb, H. (23 January 2024). *The Buildup to a Crisis: Current Tensions and Future Scenarios for Tunisia*. Malcolm H. Kerr Carnegie Middle East Centre. Available at: *https://carnegieendowment.org/research/2024/01/the-buildup-to-a-crisis-current-tensions-and-future-scenarios-for-tunisia?lang=en&center=middle-east*

Dolzikova, D. (1 March 2023). China's imports of Russian uranium spark fear of new arms race. *RUSI*. Available at: *https://www.bloomberg.com/news/articles/2023-03-01/china-nuclear-trade-with-russia-risks-tipping-military-balance*

European Parliament. (21 November 2023). *European defence industry reinforcement through common procurement act (EDIRPA)*. Available at: *https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739294*

Hirsh, M. (11 April 2023). How AI Will Revolutionize Warfare. *Foreign Policy*. Available at: *https://foreignpolicy.com/2023/04/11/ai-arms-race-artificial-intelligence-chatgpt-military-technology/*

Kumagai, S. (July 2023). India-Russia Economic Ties Are Strengthening Rapidly - Especially in Terms of Crude Oil Trade. *Japan Research Institute*.

Landgraf, W. et al. (18 January 2024). "A frozen conflict boils over, Nagorno-Karabakh in 2023 and future implications", *Foreign Policy Research Institute*. Available at: *https://www.fpri.org/article/2024/01/a-frozen-conflict-boils-over-nagorno-karabakh-in-2023-and-future-implications/*

Marcetic, B. (20 December 2023). In Gaza, the next generation of radicalization begins. *Responsible Statecraft*. Available at: *https://responsiblestatecraft.org/israel-hamas-war-counterterrorism/*

Pincus, W. (21 March 2023). The Hypersonic Arms Race is Heating Up. *The Cipher Brief*. Available at: *https://www.thecipherbrief.com/column_article/the-hypersonic-arms-race-is-heating-up*

Reuters. (November 2023a). Recent coups in West and Central Africa. *Reuters*. Available at: *https://www.reuters.com/world/africa/recent-coups-west-central-africa-2023-08-30/*

Reuters. (December 2023b). Iran undoes slowdown in enrichment of uranium to near weapons-grade -IAEA. *Reuters*. Available at: *https://www.reuters.com/world/middle-east/iran-undoes-slowdown-enrichment-uranium-near-weapons-grade-iaea-2023-12-26/*

Reuters. (18 January 2024). US urges discussions with China on practical nuclear risk reduction steps. *Reuters*. Available at: *https://www.reuters.com/world/us-urges-discussions-with-china-practical-nuclear-risk-reduction-steps-2024-01-18/*

Wall, C., Wegge, N. (2023). *The Russian Arctic Threat: Consequences of the Ukraine War*. Centre for Strategic and International Studies. Available at: *https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230125_Wall_RussianArcticThreat_0.pdf*

Williams, H. (23 February 2023). Russia Suspends New START and Increases Nuclear Risks. *Centre for Strategic and International Studies*. Available at: *https://www.csis.org/analysis/russia-suspends-new-start-and-increases-nuclear-risks*

A.8 Economic threats

AIVD (General Intelligence and Security Service). (23 April 2024). *AIVD-jaarverslag 2023*. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

AFM (Dutch Authority for the Financial Markets). (2024). *Digital Operational Resilience Act (DORA)*. Available at: *https://www.afm.nl/nl-nl/sector/themas/digitalisering/dora*

ASML. (8 March 2023). *Statement regarding additional export controls*. Available at: *https://www.asml.com/en/news/press-releases/2023/statement-regarding-additional-export-controls*

ASML. (1 January 2024). *Statement regarding partial revocation export license*. Available at: *https://www.asml.com/en/news/press-releases/2023/statement-regarding-partial-revocation-export-license*

De Nederlandsche Bank. (21 August 2023a). *FSC: "Nederlandse economie en financiële instellingen tonen zich weerbaar, maar risico's voor de financiële stabiliteit blijven hoog"*. Available at: *https://www.dnb.nl/algemeen-nieuws/persbericht-2023/fsc-nederlandse-economie-en-financiele-instellingen-tonen-zich-weerbaar-maar-risico-s-voor-de-financiele-stabiliteit-blijven-hoog/*

De Nederlandsche Bank. (9 October 2023b). *Risico's voor financiële stabiliteit nemen toe door snel gestegen rentes.* Available at: *https://www.dnb.nl/algemeen-nieuws/persbericht-2023/risico-s-voor-financiele-stabiliteit-nemen-toe-door-snel-gestegen-rentes/*

European Commission. (2023). *Temporary Crisis and Transition Framework*. Available at: *https://competition-policy.ec.europa.eu/state-aid/temporary-crisis-and-transition-framework_en*

European Commission. (31 May 2024). *Trade defence investigations*. Available at: *https://tron.trade.ec.europa.eu/investigations/ongoing*

Evofenedex. (4 April 2023). *Veel minder nachtvluchten op Schiphol bedreiging voor luchtvracht.* Available at: *https://www.evofenedex.nl/actualiteiten/veel-minder-nachtvluchten-op-schiphol-bedreiging-voor-luchtvracht*

Government of the Netherlands. (25 June 2021). *Nationale veiligheidstoets op investeringen, fusies en overnames.* Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2021/06/25/nationale-veiligheidstoets-op-investeringen-fusies-en-overnames*

Government of the Netherlands. (22 July 2022). *Nieuwe Europese richtlijn moet veiligheid verhogen.* Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2022/07/22/nieuwe-europese-richtlijn-moet-veiligheid-verhogen*

Government of the Netherlands. (10 February 2023a). *Nederland niet meer afhankelijk van energie uit Rusland.* Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2023/02/10/nederland-niet-meer-afhankelijk-van-energie-uit-rusland*

Government of the Netherlands. (31 May 2023b). *Kabinet versterkt economische weerbaarheid kennisintensief bedrijfsleven.* Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2023/05/31/kabinet-versterkt-economische-weerbaarheid-kennisintensief-bedrijfsleven*

Government of the Netherlands. (n.d.-a). *Nederlands hulp voor Oekraïne.* Available at: *https://www.rijksoverheid.nl/onderwerpen/oorlog-in-oekraine/nederlandse-hulp-voor-oekraine*

Government of the Netherlands. (2024). *Aanpak stikstofuitstoot verminderen.* Available at: *https://www.rijksoverheid.nl/onderwerpen/aanpak-stikstof-natuur-water-en-klimaat/aanpak-stikstofuitstoot-verminderen*

ING. (19 October 2023). *Extreme weather is making major trade routes less reliable, and it's only going to get worse.* Available at: *https://think.ing.com/articles/extreme-weather-makes-major-trade-routes-less-reliable/*

Jumelet, P. (1 November 2023). Capaciteit Panamakanaal wegens recorddroogte nog drastischer omlaag. *Nieuwsblad Transport.* Available at: *https://www.nt.nl/scheepvaart/2023/11/01/capaciteit-panamakanaal-wegens-recorddroogte-nog-drastischer-omlaag/?gdpr=deny*

Koenis, C. (2023). Hoe de oorlog tussen Israël en Hamas ook de wereldeconomie raakt. *RTL Nieuws.* Available at: *https://www.rtl.nl/economie/artikel/5415250/oorlog-israel-hamas-wereldeconomie-olie-gas-kunstmest?redirect=rtlnieuws*

Kompeer, J., Schellevis, J. (23 August 2023). 'Babyboomerbruggen' toe aan groot onderhoud, files en kosten verwacht. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2394865-babyboomerbruggen-toe-aan-groot-onderhoud-files-en-kosten-verwacht*

Ministry of Defence. (18 April 2024). *Jaarverslag MIVD 2023.* Available at: *https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023*

Ministry of Defence. (n.d.). *Militaire steun aan Oekraïne.* Available at: *https://www.defensie.nl/onderwerpen/oostflank-navo-gebied/militaire-steun-aan-oekraine*

Ministry of Finance (2023). *Miljoenennota 2024 – 2.2.4 Oekraïne.* Available at: *https://www.rijksfinancien.nl/miljoenennota/2024/2153111*

NOS. (19 April 2023a). Nieuwe aanwijzingen voor Russische sabotage op zeebodem. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2471999-nieuwe-aanwijzingen-voor-russische-sabotage-op-zeebodem*

NOS. (1 September 2023b). Ruzie over krimp Schiphol loopt hoog op, VS dreigt met sancties. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2488777-ruzie-over-krimp-schiphol-loopt-hoog-op-vs-dreigt-met-sancties*

ProRail. (31 August 2023). *Meer spoorwerk overdag en doordeweeks.* Available at: *https://www.prorail.nl/nieuws/meer-spoorwerk-overdag-en-doordeweeks*

Rooijers, E. (26 February 2024). Wachtlijsten stroomnet staan vol met 'zombieaanvragen'. *Financieel Dagblad.* Available at: *https://fd.nl/bedrijfsleven/1508521/wachtlijsten-stroomnet-staan-vol-met-zombieaanvragen*

Van der Boon, V., Gras, A. (2 April 2024). Tientallen bedrijven krijgen al geen drinkwater, nieuwbouwwijken volgen. *Financieel Dagblad.* Available at: *https://fd.nl/economie/1512002/tientallen-bedrijven-krijgen-al-geen-drinkwater-nieuwbouwwijken-volgen*

Van der Boon, V., Kakebeeke, P., Sie, P. (24 April 2024). Vooral in Zuid- en Oost-Nederland gaan klappen vallen door de mestcrisis. *Financieel Dagblad*. Available at: *https://fd.nl/politiek/1514612/vooral-in-zuid-en-oost-nederland-gaan-klappen-vallen-door-de-mestcrisis*

Van der Maas, R. (6 February 2023). Personeelstekort speelt wegvervoer ook in 2023 parten. *Nieuwsblad Transport*. Available at: *https://www.nt.nl/wegvervoer/2023/02/06/personeelstekort-speelt-wegvervoer-ook-in-2023-parten/?gdpr=accept*

Vestergaard, R. (3 December 2023). Nieuwe bedrijfsaansluiting op riool niet langer zeker. *Financieel Dagblad*. Available at: *https://fd.nl/bedrijfsleven/1498179/nieuwe-bedrijfsaansluiting-op-riool-niet-langer-zeker*

A.9 Cyber threats

AIVD (General Intelligence and Security Service). (4 April 2023). *Het PQC-migratie handboek*. Available at: *https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-handboek*

Cary, D., Del Rosso, K. (6 September 2023). Sleight of hand: How China weaponizes software vulnerabilities. *Atlantic Council*. Available at: *https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/*

CISA (U.S. Cybersecurity and Infrastructure Security Agency). (2024). PRC *State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Available at: *https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf*

Cyber Risk. (2024). The European Cyber Resilience Act (CRA). Available at: *https://european-cyber-resilience-act.com/*

ENISA. (11 November 2022). *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*. Available at: *https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030*

ENISA. (19 October 2023). *ENISA Threat Landscape 2023*. Available at: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023*

European Parliament. (9 December 2023). *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI*. Available at: *https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai*

European Space Agency. (7 February 2024). How ESA ensures cybersecurity in space. Available at: *https://www.esa.int/About_Us/Cyber_resilience_at_ESA/How_ESA_ensures_cybersecurity_in_space*

Galle, A. (January 2022). Drinking from the Fetid Well: Data Poisoning and Machine Learning. *U.S. Naval Institute (USNI)*. Available at: *https://www.usni.org/magazines/proceedings/2022/january/drinking-fetid-well-data-poisoning-and-machine-learning*

Government of the Netherlands. (17 October 2023). *Agenda Digitale Open Strategische Autonomie*. Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Hofmans, T. (31 January 2024). SIDN wil domein-registratiesysteem naar AWS verplaatsen. *Tweakers*. Available at: *https://tweakers.net/nieuws/218152/sidn-wil-domeinregistratiesysteem-naar-aws-verplaatsen.html*

iBestuur. (21 November 2023). Privacyzorgen rond eIDAS-wetgeving van de baan. *iBestuur* Available at: *https://ibestuur.nl/artikel/privacyzorgen-rond-eidas-wetgeving-van-de-baan/*

Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A., Gausen, A. (December 2023). *The rapid rise of Generative AI. Centre for Emerging Technology and Security (CETAS)*. Available at: *https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai*

Kaczmarek, S. (5 February 2024). *We Need Cybersecurity in Space to Protect Satellites*. Scientific American. Available at: *https://www.scientificamerican.com/article/we-need-cybersecurity-in-space-to-protect-satellites/*

Krasodomski, A., Buschser, M. (14 March 2024). *The EU's new AI Act could have global impact*. Chatham House. Available at: *https://www.chathamhouse.org/2024/03/eus-new-ai-act-could-have-global-impact*

Lohn., A., Knack, A., Burke, A., Jackson, K. (2023). *Autonomous Cyber Defense: A Roadmap from Lab to Ops*. CSET & CETAS. Available at: *https://cset.georgetown.edu/wp-content/uploads/Autonomous-Cyber-Defense-1.pdf*

Manky, D. (23 March 2023). The Latest Intel on Wipers. *FortiGuard Labs*. Available at: *https://www.fortinet.com/blog/threat-research/intel-on-wiper-malware*

Ministry of Defence. (18 April 2024). *Jaarverslag MIVD 2023*. Available at: *https://www.defensie.nl/downloads/jaarverslagen/2024/04/18/jaarverslag-mivd-2023*

NCSC (National Cyber Security Centre). (21 February 2023). *Vier cybersecuritylessen uit één jaar oorlog in Oekraïne*. Available at: *https://www.ncsc.nl/documenten/publicaties/2023/februari/21/vier-cybersecuritylessen-uit-een-jaar-oorlog-in-oekraine*

NCSC (National Cyber Security Centre. (2024). DDos – Wat kun je zelf doen?. Available at: *https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ddos*

NCSC (National Cyber Security Centre). (24 January 2024). *The near-term impact of AI on the cyber threat*. Available at: *https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat*

NCTV (National Coordinator for Counterterrorism and Security). (4 July 2022). *Cybersecuritybeeld Nederland 2022*. Available at: *https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022*

NCTV (National Coordinator for Counterterrorism and Security). (3 July 2022b). *Cybersecuritybeeld Nederland 2022*. Available at: *https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022*

NCTV (National Coordinator for Counterterrorism and Security). (3 July 2023). *Cybersecuritybeeld Nederland 2023*. Available at: *https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023*

NCTV (National Coordinator for Counterterrorism and Security), AIVD (General Intelligence and Security Service). (9 February 2024). *Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT*. Available at: *https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/6/mivd-aivd-advisory-coathanger-tlp-clear/TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER.pdf*

NIST (National Institute of standards and Technology). (2024). *Cybersecurity for the Space Domain*. Available at: *https://www.nccoe.nist.gov/cybersecurity-space-domain*

NOS. (17 April 2024). BabyTV opnieuw gehackt: allerkleinsten kijken kwartier naar Russische propaganda. *NOS*. Available at: *https://nos.nl/artikel/2517151-babytv-opnieuw-gehackt-allerkleinsten-kijken-kwartier-naar-russische-propaganda*

Portbase. (1 October 2018). *Portbase is met cloudgang klaar voor de toekomst.* Available at: *https://www.portbase.com/portbase-is-met-cloudgang-klaar-voor-de-toekomst/*

Schellevis, J. (1 February 2024). Onrust over gedeeltelijke verhuizing .nl-domeinen naar het Amerikaanse Amazon. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2507035-onrust-over-gedeeltelijke-verhuizing-nl-domeinen-naar-het-amerikaanse-amazon*

Van Sant, S., Goujard, C. (23 November 2022). *European Parliament website hit by cyberattack after Russian terrorism vote. POLITICO*. Available at: *https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/#:~:text=The%20attack%20on%20the%20European,with%20links%20to%20Russia%20indeed*

Vincent, J. (2 November 2017). Google's AI thinks this turtle looks like a gun, which is a problem. *The Verge*. Available at: *https://www.theverge.com/2017/11/2/16597276/google-ai-image-attacks-adversarial-turtle-rifle-3d-printed*

A.10 Threats to critical infrastructure

AIVD (General Intelligence and Security Service). (17 April 2023). *AIVD-jaarverslag 2022*. Available at: *https://www.aivd.nl/documenten/jaarverslagen/*

AIVD (General Intelligence and Security Service). (2024a). *AIVD-jaarverslag 2023*. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

ANV (National Network of Safety and Security Analysts). (26 September 2022). *Themarapportage Bedreiging Vitale Infrastructuur.* Available at: *https://www.nctv.nl/documenten/publicaties/2022/09/26/themarapportage-bedreiging-vitale-infrastructuur-2022*

Argyroudis, S. A., Mitoulis, S. A., Hofer, L., Zanini, M. A., Tubaldi, E., & Frangopol, D. M. (2020). Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. *Science of the Total Environment*. Available at: *https://doi.org/10.1016/j.scitotenv.2020.136854*

European Parliament. (20 July 2023). *Future Shocks 2023: Anticipating and weathering the next storms*. Available at: *https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)751428*

Gasunie. (Juli 2023). *Halfjaarbericht 2023*. Available at: *https://www.publicatiesgasunie.nl/halfjaarbericht-2023*

Geudens, P., Kramer, O. Drinkwaterstatistieken 2022. *Vewin.* Available at: *https://www.vewin.nl/SiteCollectionDocuments/Publicaties/Cijfers/Vewin-Drinkwaterstatistieken-2022-NL-WEB.pdf*

Government of the Netherlands. (11 June 2018). *Structuurvisie Ondergrond.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2018/06/11/structuurvisie-ondergrond*

Government of the Netherlands. (21 November 2022). *Eindrapport IKUS-II Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/03/07/bijlage-2-rapport-ikus-ii-november-2022-inventarisatie-kwetsbaarheden-uitval-satellietnavigatie* pdf (overheid.nl)

Government of the Netherlands. (2023a). *Kabinet zet in op energieopslag.* Available at: *https://www.rijksoverheid.nl/actueel/nieuws/2023/06/07/kabinet-zet-in-op-energieopslag*

Government of the Netherlands. (1 December 2023b). *Nationaal Plan Energiesysteem.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/12/01/nationaal-plan-energiesysteem*

Government of the Netherlands. (2024). *Probleemanalyse Congestie in het laagspanningsnet.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2024/01/22/bijlage-2-probleemanalyse-congestie-in-het-laagspanningsnet*

Huizinga, L. (19 December 2022). The Far-Right's Fascination with the U.S. Electric Grid. *UNICORN RIOT*. Available at: *https://unicornriot.ninja/2022/the-far-right-fascination-with-the-electric-grid/*

ILT (Human Environment and Transport Inspectorate). (2024). *Drinkwater steeds schaarser: provincie neem verantwoordelijkheid.* Available at: *https://www.ilent.nl/documenten/leefomgeving-en-wonen/drinkwater/drinkwater/signaalrapportages/*

Ministry of Defence. (2023). *Roadmap energietransitie operationeel materieel.* Available at: *https://www.defensie.nl/downloads/publicaties/2023/01/31/roadmap-energietransitie-materieel*

Ministry of Defence – Government Offices of Sweden. (19 October 2023). *Damaged telecommunications cable between Sweden and Estonia*. Available at: *https://www.government.se/articles/2023/10/damaged-telecommunications-cable-between-sweden-and-estonia/*

NCTV (National Coordinator for Counterterrorism and Security) (a). *Wat zijn de CER- en NIS2-richtlijnen?*. Available at: *https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen/wat-zijn-de-cer-en-nis2-richtlijnen*

NCTV (National Coordinator for Counterterrorism and Security) (b). *CER- en NIS2-richtlijnen?*. Available at: *https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen 161*

NOS. (9 November 2022). Bonaire kampt met hevige regenval, straten overstroomd. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2451698-bonaire-kampt-met-hevige-regenval-straten-overstroomd*

NOS. (19 July 2023a). Vier doden in Kroatië en Slovenië door noodweer. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2483455-vier-doden-in-kroatie-en-slovenie-door-noodweer*

NOS. (13 November 2023b). Tienduizenden getroffen door aanhoudende overstromingen Noord-Frankrijk. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2497714-tienduizenden-getroffen-door-aanhoudende-overstromingen-noord-frankrijk*

NOS. (12 March 2024). Tesla-fabriek bij Berlijn weer aangesloten op stroomnet na brandstichting. *NOS Nieuws.* Available at: *https://nos.nl/artikel/2512432-tesla-fabriek-bij-berlijn-weer-aangesloten-op-stroomnet-na-brandstichting*

PBL (Netherlands Environmental Assessment Agency). (2024). *Klimaatrisico's in Nederland;* De huidige stand van zaken. The Hague: PBL (Netherlands Environmental Assessment Agency). Available at: *https://www.pbl.nl/system/files/document/2024-05/pbl-2024-klimaatrisicos-in-nederland-5359.pdf*

Price, J. (1 December 2023). A year after the Moore County power grid attacks, questions and challenges remain. *WUNC*. Available at: *https://www.wunc.org/news/2023-12-01/a-year-after-the-moore-county-power-grid-attacks-questions-and-challenges-remain*

RDI (Dutch Auhtority for Digital Infrastructure). (2023). *Toekomstverkenning: de Trendradar.* Available at: *https://www.rdi.nl/onderwerpen/onderzoek-en-ontwikkelingen/trendradar*

TenneT. (14 March 2023). *Integrated Annual Report 2022*. Available at: *https://tennet-drupal.s3.eu-central-1.amazonaws.com/default/2023-11/TenneT_IAR_2022.pdf*

TenneT. (2024). Flexibel elektriciteitsverbruik. Available at: *https://www.tennet.eu/nl/flexibel-elektriciteitsverbruik*

TNO (Netherlands Organisation for Applied Scientific Research). (20 March 2023). *Transport gevaarlijke stoffen vraagt nu om nieuw veiligheidsbeleid.* Available at: *https://www.tno.nl/nl/newsroom/2023/03/transport-gevaarlijke-stoffen/#:~:text=Het%20transport%20van%20gevaarlijke%20stoffen,op%20welke%20plek%20als%20eerste*

Van Leerdam, R., Rook, J., Riemer, L., Van der Aa, N. (3 April 2023). *Waterbeschikbaarheid voor de bereiding van drinkwater tot 2030 - knelpunten en oplossingsrichtingen.* RIVM. Available at: *https://www.rivm.nl/publicaties/waterbeschikbaarheid-voor-bereiding-van-drinkwater-tot-2030*

Vuilleumier, P., Kerkdijk, R. (20 March 2023). Telco security Landscape 2023. ETIS. Available at: *https://www.etis.org/sites/default/files/content-files/ETIS-Papers/telco_sec_landscape_2023_published.pdf*

Wells, E. M., Boden, M., Tseytlin, I., & Linkov, I. (2022). Modeling critical infrastructure resilience under compounding threats: A systematic literature review. *Progress in Disaster Science*. Available at: *https://doi.org/10.1016/j.pdisas.2022.100244*

Section B Technology assessment

ANV (National Network of Safety and Security Analysts). (27 January 2020). AI in de context van Nationale Veiligheid. *TNO*. Available at: *https://www.rivm.nl/nationale-veiligheid*

Bronkhorst, A. et al. (2020). *Defensie technologie verkenning 2020. TNO*.

COGEM (The Netherlands Commission on Genetic Modification), Health Council of the Netherlands, *Trendanalyse biotechnologie 2023. Tijd voor een integrale visie* (Bilthoven: March 2023), 3.

Government of the Netherlands. (2023b). *Besluit toepassingsbereik sensitieve technologie.* Available at: *https://wetten.overheid.nl/BWBR0048201/2023-06-01*

Government of the Netherlands. (19 January 2024). *Nationale Technologiestrategie.* Available at: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Photondelta. (13 February 2024). *Annual Review 2023*. Available at: *https://www.photondelta.com/downloads/*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

US Department of Defence. (2020). *Joint Publication 3-14 Space Operations*. Available at: *https://irp.fas.org/doddir/dod/jp3_14.pdf*

Van Bree, T. et al. (March 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Available at: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.1 Artificial Intelligence

AIVD (General Intelligence and Security Service). (2024). *AIVD-jaarverslag 2023*. Available at: *https://www.aivd.nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023*

ANV (National Network of Safety and Security Analysts). (27 January 2020). AI in de context van Nationale Veiligheid. *TNO*. Available at: *https://www.rivm.nl/nationale-veiligheid*

Galle, A. (January 2022). Drinking from the Fetid Well: Data Poisoning and Machine Learning. *U.S. Naval Institute (USNI)*. Available at: *https://www.usni.org/magazines/proceedings/2022/january/drinking-fetid-well-data-poisoning-and-machine-learning*

Gonzalez, S., Kant, M., Miikkulainen, R. (2024). Evolving GAN formulations for higher-quality image synthesis. *Artificial Intelligence in the Age of Neural Networks and Brain Computing*. Available at: *https://www.sciencedirect.com/science/article/abs/pii/B9780323961042000142*

Government of the Netherlands. (21 November 2022). *Eindrapport IKUS-II Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/03/07/bijlage-2-rapport-ikus-ii-november-2022-inventarisatie-kwetsbaarheden-uitval-satellietnavigatie* pdf (overheid.nl)

Government of the Netherlands. (2023a). Defensie Strategie Data Science en AI 2023-2027. Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/05/31/defensie-strategie-data-science-en-artificiele-intelligentie-2023-2027*

Government of the Netherlands. (17 October 2023b). *Agenda Digitale Open Strategische Autonomie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Government of the Netherlands. (19 January 2024). *Nationale Technologiestrategie.* Available at: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Hazell, J. (2023). Spear Phishing With Large Language Models *[2305.06972] arXiv*. Available at: *https://doi.org/10.48550/arXiv.2305.06972*

Heijnen, M., Schoonderwoerd, T., Neerincx, M., van der Waa, J., Kester, L., van Diggelen, J., Elands., P. (2024). "*A Socio-Technical Feedback Loop for Responsible Military AI Life-Cycles from Governance to Operation*," DOI: 10.1201/9781003410379-3

Janjeva, A., Harris, A., Mercer, S., Kasprzyk, A., Gausen, A. (December 2023). The rapid rise of Generative AI. *Centre for Emerging Technology and Security (CETAS)*. Available at: *https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai*

Nurkin, T., Konaev, M. (25 May 2022). Eye-to-Eye-in-AI. *Atlantic Council*. Available at: *https://www.atlanticcouncil.org/in-depth-research-reports/report/eye-to-eye-in-ai/*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Taddeo, M., Ziosi, M., Tsamados, A., Gilli, L., Kurapati, S. (September 2022). AI for National Security: the Predictability Problem. *Centre for Emerging Technology and Security (CETAS)*. Available at: *https://cetas.turing.ac.uk/publications/artificial-intelligence-national-security-predictability-problem*

Van Bree, T. et al. (March 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Available at: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.2 Space technology

Ben-Itzhak, S. (11 January 2022). Companies are commercializing outer space. Do government programs still matter?. *The Washington Post*. Available at: *https://www.washingtonpost.com/politics/2022/01/11/companies-are-commercializing-outer-space-do-government-programs-still-matter/*

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Centre of Excellence. (21 November 2022). *Eindrapport IKUS-II*. Available at: *https://open.overheid.nl/documenten/ronl-e7e61227b3dd72448fb767b7d0ed1c779552d421/pdf*

Defense Advanced Research Projects Agency. (17 February 2024). *DARPA Launch Challenge (Archived)*. Available at: *https://www.darpa.mil/news-events/darpa-launch-challenge*

ENISA. (11 November 2022). *Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!*. Available at: *https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030*

Goguichvli, S., Linenberger, A., & Gillette, A. (1 October 2021). The Global Legal Landscape of Space: Who Writes the Rules on the Final Frontier. *Wilson Center*. Available at: *https://www.wilsoncenter.org/article/global-legal-landscape-space-who-writes-rules-final-frontier*

Lillis, K. (17 February 2024). *Exclusive: Russia attempting to develop nuclear space weapon to destroy satellites with massive energy wave, sources familiar with intel say*. CNN. Available at: *https://edition.cnn.com/2024/02/16/politics/russia-nuclear-space-weapon-intelligence/index.html*

Miller, C., Scott, M., Bender, B. (9 June 2022). UkraineX: How Elon Musk's space satellites changed the war on the ground. *POLITICO*. Available at: *https://www.politico.com/news/2022/06/09/elon-musk-spacex-starlink-ukraine-00038039*

NATO. (2024) *NATO's Approach to Space*. Available at: *https://www.act.nato.int/our-work/network-community/natos-approach-to-space/*

NSO (Netherlands Space Office). (20 October 2022). *NSO Advies voor het ruimtevaartbeleid 2023-2025.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2022/10/20/nso-advies-voor-het-ruimtevaartbeleid-2023-2025*

OECD. (15 September 2022). *Earth's Orbits at Risk: The Economics of Space Sustainability*. Available at: *https://www.oecd-ilibrary.org/science-and-technology/earth-s-orbits-at-risk_16543990-en*

Projectteam Statelijke Dreigingen. (9 November 2021). Eindrapport state-of-the-art onderzoek Statelijke Dreigingen. *Ministerie van Defensie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2021/11/09/tk-bijlage-wodc-rapport-state-of-the-art-statelijke-dreigingen-fase-1*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Secure World Foundation. (2024). *Global Counterspace Capabilities Report*. Available at: *https://swfound.org/counterspace/*

Starling, C. (15 February 2024). *Russian nuclear anti-satellite weapons would require a firm US response, not hysteria*. Atlantic Council. Available at: *https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-nuclear-anti-satellite-weapons-would-require-a-firm-us-response-not-hysteria/*

UK Office of the Chief Scientific Adviser for National Security, Government Communications Headquarters (GCHQ), National Crime Agency. *Joint Emerging Technology Trends: JETT Report 2022*.

US Department of Defence. (2020). Joint Publication 3-14 Space Operations. Available at: *https://irp.fas.org/doddir/dod/jp3_14.pdf*

Wall, M. (14 July 2022). Kessler Syndrome and the space debris problem. *Space*. Available at: *https://www.space.com/kessler-syndrome-space-debris*

Wayenburg, B. (15 February 2024). *Wat zou dat betekenen, een kernwapen in de ruimte?* NRC. Available at: *https://www.nrc.nl/nieuws/2024/02/15/een-kernwapen-in-de-ruimte*

You, G. H. (19 May 2022). Outer Space Security & Governance. *Foreign Policy*. Available at: *https://foreignpolicy.com/2022/05/19/outer-space-security-international-governance/*

B.3 Quantum technology

AIVD (General Intelligence and Security Service). (23 September 2021). *Bereid je voor op de dreiging van quantumcomputers.* Available at: *https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers*

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

European Commission. (20 June 2023a). *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL* ON "EUROPEAN ECONOMIC SECURITY STRATEGY". Available at: *eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020*

European Commission. (3 October 2023b). *Recommendation on critical technology areas*. Available at: *https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4735*

European Commission. (2024). *White Paper on Export Controls*. Available at: *https://policy.trade.ec.europa.eu/news/commission-publishes-new-guidelines-annual-report-dual-use-export-controls-2024-01-25_en*

Haeck, P. (27 February 2024). *Europe is ring-fencing the next critical tech: Quantum*. Politico. Available at: *https://www.politico.eu/article/how-europe-ring-fencing-quantum-computing-technology-defense/*

Krelina, M. (6 November 2021). Quantum technology for military applications. *EPJ Quantum Technology*. Available at: *https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-021-00113-y#citeas*

Lele, A. (2021). Quantum Technologies and Military Strategy. *Springer*. Available at: *https://doi.org/10.1007/978-3-030-72721-5*

Ministerio de Industria, Comercio y Turismo. (2023). *Disposición 12785 del BOE núm. 129 de 2023*. Available at: *https://www.boe.es/boe/dias/2023/05/31/pdfs/BOE-A-2023-12785.pdf*

Neumann, N., Van Heesch, M., Philipson, F., Smallegange, A. (2021). Quantum Computing for Military y Applications. *2021 International Conference on Military Communication and Information Systems (ICMCIS)*. Available at: *https://ieeexplore.ieee.org/document/9486419*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

TNO (Netherlands Organisation for Applied Scientific Research), CWI, AIVD (General Intelligence and Security Service). (December 2023). *Het PQC-migratie handboek, richtlijnen voor het migreren naar post-quantumcryptografie.* Available at: *https://www.tno.nl/nl/newsroom/2023/04/pqc-migratie-handboek/*

Van Bree, T. et al. (March 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Available at: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.4 Robotics and autonomous systems

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

Detsch, J. (30 March 2021). The U.S. Army Is Using the Nagorno-Karabakh Conflict to Study Drone Warfare. *Foreign Policy*. Available at: *https://foreignpolicy.com/2021/03/30/army-pentagon-nagorno-karabakh-drones/*

Elands, P., Heijnen, M. & Werkhoven, P. (2023). Operationalization of meaningful human control for military AI. TNO.

Government of the Netherlands. (17 October 2023). *Agenda Digitale Open Strategische Autonomie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Pettyjohn, S. (8 February 2024). Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine. *CNAS*. Available at: *https://www.cnas.org/publications/reports/evolution-not-revolution*

Pol, A., Zwijnenburg, W. (October 2022). A Laboratory of Drone Warfare. *PAX*. Available at: *https://paxforpeace.nl/wp-content/uploads/sites/2/import/2022-11/PAX_Syria_A%20Laboratory%20of%20Drone%20Warfare_2022.pdf*

Rathenau Instituut. (4 January 2021). *Killer robots. Waarom internationale afspraken nodig zijn.* Available at: *https://www.rathenau.nl/nl/digitalisering/killer-robots-waarom-internationale-afspraken-nodig-zijn*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Vos, L. (2023). The use of technology and its implications in the Ukraine war. *TNO*.

Williams, D., Al-Mughrabi, N. (23 October 2023). Israel carries out limited raids in Gaza, Hamas launches drones. *Reuters*. Available at: *https://www.reuters.com/world/middle-east/israel-mounts-limited-gaza-ground-raids-puts-hostage-number-222-2023-10-23/*

B.5 Photonics technology

Government of the Netherlands. (2023a). *Besluit toepassingsbereik sensitieve technologie.* Available at: *https://wetten.overheid.nl/BWBR0048201/2023-06-01*

Government of the Netherlands. (17 October 2023b). *Agenda Digitale Open Strategische Autonomie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Government of the Netherlands. (19 January 2024). *Nationale Technologiestrategie.* Available at: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Optics.org. (23 January 2024). *Military laser DragonFire achieves first successful test firing*. Available at: *https://optics.org/news/15/1/30#:~:text=During%20a%20trial%20at%20the,a%20weapon%20against%20aerial%20targets*

Ministry of Defence. (2023). *Roadmap energietransitie operationeel materieel.* Available at: *https://www.defensie.nl/downloads/publicaties/2023/01/31/roadmap-energietransitie-materieel*

Parlementaire Monitor. (17 July 2018). *Nationale Agenda Fotonica (bijlage bij 33009 ,nr.64).* Available at: *https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkq4lwat43ym Parlementaire monitor*

Photondelta. (13 February 2024). *Annual Review 2023.* Available at: *https://www.photondelta.com/downloads/*

PhotonicsNL. (2022). Photonics roadmap. Available at: *https://photonicsnl.com/*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

Van Bree, T. et al. (March 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Available at: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

B.6 Energy technology

Bronkhorst, A. et al. (2020). Defensie technologie verkenning 2020. *TNO*.

COGEM (The Netherlands Commission on Genetic Modification), Health Council of the Netherlands. (2023). Trendanalyse biotechnologie 2023, Tijd voor een integrale visie. *COGEM*. Available at: *https://open.overheid.nl/documenten/ronl-0cc88c42d7d145c61dfe8a7ed66f9e71db88b021/pdf*

European Commission. (16 March 2023). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020.* Available at: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0160*

European Union. *Strategic Energy Technology Plan*. Available at: *https://energy.ec.europa.eu/topics/research-and-technology/strategic-energy-technology-plan_en#related-links*

Government of the Netherlands. (1 December 2023a). *Nationaal Plan Energiesysteem.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/12/01/nationaal-plan-energiesysteem*

Government of the Netherlands. (17 October 2023b). *Agenda Digitale Open Strategische Autonomie.* Available at: *https://www.rijksoverheid.nl/documenten/rapporten/2023/10/17/bijlage-agenda-dosa-tgpdfa*

Government of the Netherlands. (19 January 2024). Nationale Technologiestrategie. Available at: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Pommeret, A., Ricci, F., Schubert, K. (2022). Critical raw materials for the energy transition. *European Economic Review*, 141. Doi: *https://doi.org/10.1016/j.euroecorev.2021.103991*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

TenneT. (14 March 2023). *Integrated Annual Report 2022*. Available at: *https://tennet-drupal.s3.eu-central-1.amazonaws.com/default/2023-11/TenneT_IAR_2022.pdf*

TNO (Netherlands Organisation for Applied Scientific Research). (31 May 2024). *Nieuwe ontwikkeling in recycling windturbinebladen*. Available at: *https://www.tno.nl/nl/duurzaam/hernieuwbare-elektriciteit/windparken-zee/duurzaam-ontwerp-windturbines-circulair/recycling-windturbinebladen/*

B.7 Biotechnology

Alder, S. (2 November 2023). Why Do Criminals Target Medical Records? The HIPAA Journal. Available at: *https://www.hipaajournal.com/why-do-criminals-target-medical-records/*

COGEM (The Netherlands Commission on Genetic Modification), Health Council of the Netherlands. (2023). Trendanalyse biotechnologie 2023, Tijd voor een integrale visie. *COGEM*. Available at: *https://open.overheid.nl/documenten/ronl-0cc88c42d7d145c61dfe8a7ed66f9e71db88b021/pdf*

Government of the Netherlands. (19 January 2024). Nationale Technologiestrategie. Available at: *https://www.rijksoverheid.nl/documenten/beleidsnotas/2024/01/19/de-nationale-technologiestrategie*

Guarino, B. (30 January 2024). Elon Musk's Neuralink Has Implanted Its First Chip in a Human Brain. What's Next?. *Scientific American*. Available at: *https://www.scientificamerican.com/article/elon-musks-neuralink-has-implanted-its-first-chip-in-a-human-brain-whats-next/*

Kuntz, K. (1 May 2024). Biotech Matters: Problems with Life Science Databases in the United States. CNAS. Available at: *https://www.cnas.org/publications/reports/biotech-matters-problems-with-life-science-databases-in-the-united-states*

Luca, J. (15 October 2023). DNA Hacking: How Hackers Can Access and Manipulate Your Genetic Data. *Medium*. Available at: *https://medium.com/@rmndrathna4/dna-hacking-how-hackers-can-access-and-manipulate-your-genetic-data*

McCallum, S., Tidy, J. (5 December 2023). 23andMe: Profiles of 6.9 million people hacked. BBC. Available at: *https://www.bbc.com/news/technology-67624182*

Reding, D. et al. (March 2023). Tech Trends report 2023-2043. *NATO Science & Technology Organization*. Available at: *https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol2.pdf*

The Guardian. (15 February 2024). Hackers got nearly 7 million people's data from 23andMe. The firm blamed users in 'very dumb' move. Available at: *https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response*

UK Office of the Chief Scientific Adviser for National Security, Government Communications Headquarters (GCHQ), National Crime Agency, *Joint Emerging Technology Trends: JETT Report 2022*

Van Bree, T. et al. (March 2023). Herijking Sleuteltechnologieën 2023. *TNO/NWO*. Available at: *https://www.tno.nl/nl/newsroom/2023/04/nieuwe-lijst-44-sleuteltechnologieen/*

Van Weerd, C., Lassche, D. (October 2021). National Security Implications of Quantum Technology and Biotechnology. *TNO/HCSS*. Available at: *https://hcss.nl/wp-content/uploads/2021/11/Strategic-Alert-Quantum-Technology-HCSS-TNO-2021-2.pdf*

Government of the Netherlands

Published by:

The National Institute for Public Health and the Environment (RIVM)
The Netherlands Organisation for Applied Scientific Research (TNO)
The Netherlands Institute of International Relations 'Clingendael' (Clingendael)
SEO Amsterdam Economics (SEO)
The General Intelligence and Security Service (AIVD)
The Military Intelligence and Security Service (MIVD)
Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC)

October 2024

015738