National Risk Assessment of the Kingdom of the Netherlands 2022

National Network of Safety and Security Analysts

National Risk Assessment of the Kingdom of the Netherlands 2022

National Network of Safety and Security Analysts

Publication details

The National Risk Assessment of the Kingdom of the Netherlands 2022 has been compiled by the National Network of Safety and Security Analysts at the request of the National Coordinator for Security and Counterterrorism (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: L. Gooijer (leendert.gooijer@rivm.nl)

Contents

Foreword

This National Risk Assessment (NRA) describes threats that could disrupt Dutch society. Potential threats are identified and the risk they pose for national security is assessed in terms of both consequences and likelihood. The overview of the various threats and their associated risks can assist in the development of the National Security Strategy (NSS), as this requires insight into the main national security risks for the Kingdom of the Netherlands in the years ahead. The National Risk Assessment may be used as input for this strategy, as well as for resilience assessments and crisis management.

The NRA is not the first risk analysis published by the National Network of Safety and Security Analysts (ANV). The ANV issued annual national risk assessments (*Nationale Risicobeoordeling*, NRB) up until 2014, which used scenarios to analyse a number of threats. In 2016 and 2019 respectively, the National Risk Profile (*Nationaal Veiligheidsprofiel*, NVP) and National Risk Assessment (*Geïntegreerde risicoanalyse*, GRA) were published. Each of these assessments includes an all-hazard overview of the main risks for national security.

The NRA builds on the knowledge and experience gained in the context of these previous assessments. Alongside this, key modifications and additions have been introduced, such as revisions of existing scenarios, the selection and analysis of new scenarios, a discussion of latent threats and a more prominent place for digitisation and internationalisation in our methodology.

The development and assessment of scenarios continues to be the main basis of our approach to the NRA. The 60+ scenarios included in the NRA were assessed in a large number of experts meetings, during which experts for the relevant theme assessed the impact and likelihood of the scenarios presented here. We would like to take this opportunity to thank the experts involved for their contributions to these sessions and their help in shaping the scenarios under consideration. A special feature of these expert meetings was that most of them took place online. This is because they were held in January and February 2022, during the COVID-19 pandemic.

It is worth pointing out that some of the threats discussed in the NRA did in fact take place while the assessment was under preparation. As stated earlier, the NRA expert sessions took place in the midst of the COVID-19 pandemic, as did the analyses preceding these sessions. In the summer of 2021 there was also widespread flooding in Limburg, Belgium and Germany, and in 2022 the Netherlands is facing an outbreak of avian influenza. During the recording of the outcomes of the NRA there was also the Russian invasion of Ukraine and at the time of writing of this foreword (late June 2022), the Dutch policy regarding nitrogen emissions had sparked protests across the Netherlands.[1]

[1] The invasion by Russia and the war in Ukraine occurred after the expert sessions for this risk assessment were held (January/February 2022) and as a result these events were not explicitly discussed. However, this type of threat was specifically considered (including in a scenario that looks at the temporary occupation of an EU member state) and Russian assertiveness is part of the context of multiple thematic reports, in particular the reports on international and military threats. See also the afterword.

These events illustrate that risk analyses such as the NRA are not merely a theoretical exercise but that threats and their associated risks can indeed materialise. This fact underlines the importance of risk assessments and the periodic implementation of such assessments, in particular for strengthening national security.[2]

As stated, the NRA was carried out by the National Network of Safety and Security Analysts. This is a knowledge network that has been analysing risks and threats to national security since 2011. The ANV consists of a permanent core of seven organisations (RIVM, TNO, Instituut Clingendael, SEO, AIVD, MIVD, WODC) and a wider network or organisations that includes knowledge institutions, safety regions and other civil services, businesses and research agencies.[3]

In addition to this NRA main report, there is a separate report containing a risk assessment for the Caribbean part of the Netherlands, as well as nine thematic reports that deal with the individual threat themes in greater detail.

[2] This is also highlighted in the lessons learned and recommendations by the Dutch Safety Board (Onderzoeksraad voor Veiligheid) regarding the response to the COVID-19 crisis. See: Dutch Safety Board, 2022. Aanpak coronacrisis (Response to the COVID-19 crisis). Deel 1: tot september 2020 (Part 1: the period up to September 2020). This report also takes an in-depth look at the pandemic scenario previously prepared by the ANV (page 98/99).

[3] A more detailed description of the ANV is included in Annex 1.

Summary

Introduction

The National Risk Assessment (NRA) provides an overview of a wide range of threats that have the potential to cause disruption in the Netherlands. The assessment does not only discuss the characteristics of a threat but also its associated risk. The outcomes of the NRA are used as input in the National Security Strategy and other instruments. The translation of the NRA into strategy or policy does, however, require certain choices to be made. This is because the analysis distinguishes between threats with a large impact on society, threats with a high likelihood of occurrence and threats that feature a combination of both. Selecting the type of threat on which to focus from a policy perspective is not within the scope of the NRA. This choice is possibly complicated by the fact that the assessment also reveals connecting links, interdependencies and overarching topics that will require a more holistic approach.

Framework of the risk assessment

The threats included in the NRA are analysed based on the six national security interests. When one or more of the six national security interests are seriously affected, society faces disruption and there is potential for a threat to have a detrimental impact on Dutch national security. The six national security interests are: (i) territorial security, (ii) physical safety, (iii) economic security, (iv) ecological security, (v) social and political stability, and (vi) the international legal order and stability. These interests can be affected by a wide variety of threats. For this reason the NRA uses an all hazard approach, considering both intentional (*security*) and non-intentional (*safety*) threats that may originate both domestically as abroad.

The risks belonging to the various threats were made explicit by way of scenarios. The likelihood and security of these were subsequently assessed in expert sessions using a fixed methodology. Both axes use a five-point scale, ranging from 'very unlikely' to 'very likely', and from 'limited' to 'catastrophic'. The fact that the same assessment method is applied across the different scenarios makes the associated risks comparable. In this way, the National Risk Assessment applies a comparative perspective to a wide range of risks.

In total more than 60 scenarios were created across nine overarching threat themes:

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

All of the above threat themes were analysed individually and each theme is discussed in a dedicated thematic report. In addition to the scenarios, the thematic reports also address relevant developments and latent threats. The theme-specific outcomes can be used to delve deeper into specific threats and their associated risks, and can assist in producing resilience assessments and reinforcing crisis management. The results for the nine threat themes were subsequently collated and provide the basis for the overall results of the NRA.

Results of the risk assessment seen through three lenses

Different perspectives can be chosen when considering what threats will present the greatest risk to Dutch national security in the years ahead.

Greatest likelihood

Looking at the threats that have the highest likelihood, it is striking that there is a relatively high number of scenarios that are deemed 'very likely' (this is the highest likelihood rating according to the method used). Among these are scenarios from various themes, encompassing both safety threats (wildfires, flu epidemic) and security threats (hybrid operations, disruption to international trade, collateral damage of cyber attacks). In light of the relatively high likelihood that these types of threats will occur, it is key to put in place mechanisms for mitigating their impact.

Greatest impact

For a large number of scenarios, the expected impact has been rated 'serious' or higher. Zooming in on threats with the two highest impact ratings ('very serious' and 'catastrophic'), we once again see a mix of safety and security threats, from both internal and external sources. Physical threats under the climate and natural disasters and Infectious diseases themes – i.e. flooding from the sea and a new pandemic similar to COVID-19 – are expected to have the greatest impact. Both scenarios will have a major, catastrophic impact on multiple national security interests.

Once again, ensuring resilience against these types of threats will be key as this will ultimately reduce the chance of a catastrophic impact. As an example, consider the long-term measures already in place to protect the Netherlands against flooding from the sea.

Combination of impact and likelihood

Lastly we can consider threats characterised by both a relatively large impact and likelihood. This type of threat is found in many of the threat themes. Looking at the nine scenarios that rank highest in terms of the combination of impact and likelihood, the Climate and natural disasters theme in particular is well represented. This theme covers a number of scenarios that belong to the category extreme weather category, namely scenarios on the heat/drought and a hurricane. The hurricane scenario represents one of the greatest risks to the Caribbean part of the Kingdom of the Netherlands. Another scenario that ranks high for both impact and likelihood is a wildfire. Climate change is a key driver for the various risks addressed in the Climate and natural disasters threat theme.

The infectious diseases theme also includes multiple scenarios that have high ratings in terms of impact as well as likelihood. Both a flu epidemic and a pandemic similar to COVID-19 can lead to a large number of fatalities and patients (causing severe pressure on the healthcare sector) and may lead to a severe impact on the economy and society (depending on the circumstances and possible containment measures).

Within the economic threats theme, the two scenarios found amongst the top nine for impact and likelihood are predominantly illustrations of the risks associated with dependency. These risks could materialise as soon as there is a threat of shortages of certain goods or if tensions arise between the actors involved. The specific scenarios involved here are those relating to trade disruption as a result of production issues abroad and the import of, or difficulty in importing, fossil-based energy.

Finally, the top nine also features the themes foreign subversion of the democratic constitutional system (scenario hybrid operations by Russia, using various instruments) and cyber threats (scenario attack on a cloud service provider). The assessment shows that it is not always possible to determine precisely what effects a cyber threat may have, which gives rise to a certain level of unpredictability.

Although the above themes contain the highest ranking scenarios when impact and likelihood are combined, other themes can still be relevant from this perspective. Within the theme international and military threats this applies to potential instability on the borders of the European Union and the Kingdom of the Netherlands. This includes events such as the collapse of the Venezuelan state or tensions in the Balkans. The same perspective highlights social polarisation within the social polarisation, extremism and terrorism theme and a blackout on the power grid within the disruptions to critical infrastructure theme. In other words, the combined perspective of impact and likelihood results in a broad spectrum of threats.

Applying of the results

The three above perspectives on interpreting risks can also be used to support the follow-up to the NRA:

- If a threat has a *high likelihood*, it seems sensible for society to make preparations and check whether it is sufficiently resilient. Examples of threats include wildfires, terrorist attacks by a lone actor and the collateral damage of a cyber attack.
- Regarding threats that could have the *greatest impact* on national security, an obvious choice would be to minimise the risk that these might materialise. In this context, the question naturally arises as to what possibilities are at our disposal to minimise that risk (or keep it as low as possible), and whether additional investments would be proportional to the security gains made.
- When determining priorities from a risk-oriented perspective, threats with a relatively *great impact and a high likelihood* can be used as a guide. Further analysis of the relevant threats can provide insight into whether risk reduction measures are best focused on the aspect of likelihood or impact.
- Analysing the specific consequences of a particular threat makes it possible to produce a concrete resilience analysis and use the results to strengthen crisis management. In relation to threats that can result in a high number of casualties for instance, this could include checking how the required medical assistance would or could be made available. In this way, it becomes possible to establish a direct link between risk analyses and resilience assessments.

Interdependencies and overarching conclusions

This risk assessment not only offers the opportunity to directly look into specific risks, but also highlights a large number of connections and interdependencies between the various risks that must be taken into account. Examples include the interconnectedness and dependencies between vital processes and digitisation (with the dependency between electricity supply and telecoms being particularly pertinent), and between economic and international developments.

In addition to this, the assessment has brought a number of overarching topics to the fore. These are: *climate change*, *the energy transitions*, *tensions in society* and *hybrid threats*. Within these topics, multiple developments that are relevant to national security converge. Climate change, for example, is a driver that will increase the impact and likelihood of a range of threats. This is to say that the effects of climate change are not restricted to the theme of climate and natural disasters (which includes an increased probability of extreme weather events that could amongst others affect vital infrastructure), but can also include an aggravation of both social and international tensions. In relation to the energy transition, there are multiple issues at play, including greater dependency and pressure on the electricity grid as well as a greater dependency on energy sources, materials, technology and (foreign) actors. Both intentional (security) and non-intentional (safety) threats can heighten tensions in society. Tensions could arise in connection with the challenges posed by climate change and the energy transition but they may equally be the result of actions by extremist or state actors. State actors may also seek to create or exacerbate such tensions as part of a hybrid threat. Hybrid threats concern state actors purposefully deploying various instruments that are below the threshold of armed conflict and which do not necessarily entail a severe impact on national security in themselves, but that could undermine national security when seen as a whole. This includes setting up misinformation campaigns and carrying out cyber attacks. Hybrid threats are therefore not restricted to a specific type of action or a specific type of threat.

A holistic analysis of the above overarching topics can be carried out from the perspective of resilience and crisis management. The connecting links and interdependencies create a certain level of unpredictability with regard to the consequences that will arise if a risk materialises. This requires a more holistic approach that allows issues to be treated as a complex system.

Concluding remarks

The NRA considers a large number of threats and their associated risks. Although it is true that some of these threats have not occurred in the Netherlands for some considerable time or are considered unlikely or very unlikely to emerge in future, others have indeed already materialised. For others still, estimates are that they are likely to arise (or arise again) as challenges for our society in the years ahead. It is emphasised that the threat assessment presented in the NRA is not static but can evolve as a result of social, international, technological and other developments. It is key for our society to be aware of and keep up to date with the set of threats that could undermine our national security, for example by conducting periodic analyses such those included in the NRA. This will provide tools for the creation of a resilient Kingdom of the Netherlands.

1. Introduction

1.1 The framework of the National Risk Assessment

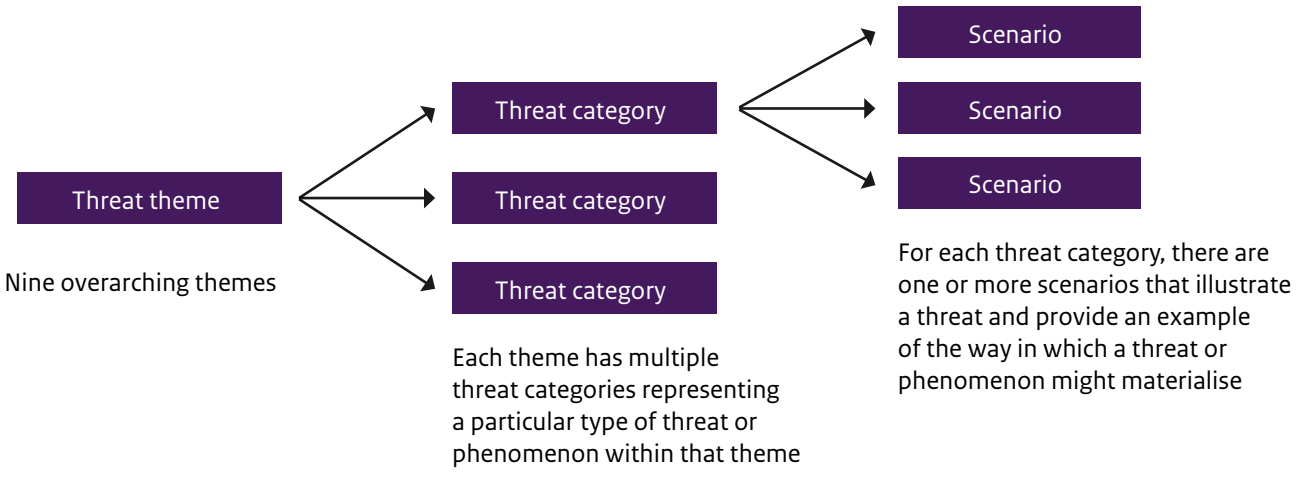
The document before you contains the main report on the 2022 National Risk Assessment (NRA), as prepared by the National Network of Safety and Security Analysts (ANV). This assessment provides an overview of a wide range of threats that can disrupt our society and their associated risks. A large number of threats have been identified and subsequently analysed in terms of impact and likelihood by wat of specific scenarios, in order to provide an understanding of the risks that they entail. The results of the NRA are used as input for the National Security Strategy. This main report is a synthesis of nine underlying NRA thematic reports prepared by the ANV.

An all-hazard approach was adopted in light of the widely varying nature of threats that could undermine national security. Both intentional (security) and non-intentional (safety) threats are considered, originating both domestically and abroad. To assist in determining the impact and likelihood of sometimes rather abstract threats, these treats were translated into one or more specific scenarios. More than 60 such scenarios have been elaborated, across a total of nine overarching threat themes:

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

Each of the nine threat themes has been subdivided into various threat categories, each of which consists of a number of related scenarios. The climate and natural disasters theme, for example, comprises the flooding, earthquakes, extreme weather and wildfires risk categories. The category flooding contains a number of different scenarios, such as flooding from the sea or from a river. The following figure shows how themes, categories and scenarios relate to each other. A full list of threat themes and categories has been included in Annex 2.

Figure 1 Relationship between themes, categories and scenarios



All scenarios were assessed in the same manner, based on the national security methodology developed by the ANV. This method is based on six national security interests, which are used to determine the consequences of a threat for society. The six interests cover territorial security, physical safety and ecological security, as well as social and political stability and the international legal order and international stability. Descriptions of the national security interests are provided in the following table. See Annex 2 for a more detailed description of the approach and methodology used by the ANV.

Table 1 National security interests

The six national security interests	
Territorial security	The unimpeded functioning of the Netherlands and its EU and NATO allies as independent states in the widest sense, or their territorial integrity in a narrow sense.
Physical safety	The unimpeded functioning of people in the Netherlands and their surroundings.
Economic security	The unimpeded functioning of the Netherlands as an effective and efficient economy.
Ecological security	The unimpeded continued existence of the natural living environment in and around the Netherlands.
Social and political stability	The unimpeded continued existence of a social climate in which individuals can function without disruption and groups of people enjoy living together within the benefits of the Dutch democratic constitutional system and values shared therein.
International legal order and stability	The proper functioning of the international system of norms and agreements aimed at promoting international peace and security, including human rights, and effective multilateral institutions and international regimes, as well as the proper functioning of states bordering the Kingdom of the Netherlands and in direct vicinity of the European Union.

National security is at stake when one or more national security interests are threatened to the extent that society is or could be disrupted.

Compared to previous analyses carried out by the ANV, such as the 2016 National Security Profile and the 2019 National Risk Assessment, aspects of the national security interests, their translation to impact criteria and the associated analyses were adapted and expanded for the purpose of the NRA. For example, aspects related to digitisation and internationalisation were given a more prominent place in the methodology.

The scope of the current risk assessment is also wider than that of previous editions. Threats for the entire Kingdom of the Netherlands are examined, including for the Caribbean part of the Kingdom.

A further addition is the inclusion of latent threats. Alongside threats that were analysed in the 60+ standard scenarios that focus on the coming five years, this assessment also looks at threats or developments developing at a slower pace and that could become relevant over the longer term (10-20 years) in particular. This creates a picture of topics that may not be relevant for another 10-20 years but which may already require action to be taken now. In addition to latent threats, the NRA features a number of wild card scenarios that stretch the limits of what is seen as conceivable threats. Both the latent threats and the wildcards have been described in qualitative terms. They are used as a complement to the risks that were analysed and assessed in terms of impact and likelihood in expert sessions with the help of scenarios. A number of latent threats are revisited in chapter 13, which discusses selected overarching topics in the context of the NRA. More information on the wildcards can be found in the individual thematic reports.

Annex 2 provides a more detailed description of the adopted approach and methodology within the NRA.

1.2 Aim and scope

The purpose of this risk assessment is to provide an overview of risks relevant to the national security of the Kingdom of Netherlands, thus allowing reasoned choices to be made in relation to priority setting and reviews to be carried out into what level of resilience is present and required. The NRA itself does not prioritise threats but acts as input for priority setting in the National Security Strategy (NSS). [4]

1.3 Reading guide

This report has several sections. Section I discusses the main results of the risk assessment for each of the threat themes. Chapters 2-10, which make up this section, cover the following threat themes:

- Chapter 2: Climate and natural disasters;
- Chapter 3: Infectious diseases;
- Chapter 4: Major accidents;
- Chapter 5: Social polarisation, extremism and terrorism;
- Chapter 6: Foreign subversion of the democratic constitutional system;
- Chapter 7: International and military threats;
- Chapter 8: Economic threats;
- Chapter 9: Cyber threats;
- Chapter 10: Threats to critical infrastructure.

Alongside a qualitative description of the key results, each of these chapters also provides a risk matrix for the relevant theme.[5] This plots the scenarios analysed in the context of the theme along the axes of impact and likelihood. Chapter 11 subsequently discusses risks for the Caribbean part of the Kingdom. All of the threat themes and the Caribbean part of the Kingdom are also addressed in separate thematic reports. These take a more in-depth look at developments relevant to the specific theme, the scenarios developed by the ANV and the anticipated consequences and likelihood of these scenarios. This main report summarises the key outcomes and observations made in the relevant thematic report for each of the above themes.

Section II discusses the overall results of the NRA, as well as the connecting links between the various threat themes and the wider threat landscape in the area of national security. Chapter 12 presents the overall results of the NRA in a risk matrix that plots all the analysed scenarios along the axes of impact and likelihood. This matrix is then used to present, discuss and interpret the results. Chapter 13 discusses a number of overarching topics that were mentioned in multiple threat themes, whereas chapter 14 reflects on the threat landscape for national security as a complex system.

The third and final section of this report contains the final conclusions of the risk assessment (chapter 15), which set out a number of possible avenues for the follow-up to the results of the NRA. The annexes not only offer further information on the ANV and the national security methodology applied by the network, but also provide an overview of all the threat themes and corresponding categories.

[4] As stated previously, this assessment covers the whole of the Kingdom of the Netherlands, including the Caribbean part. This might prompt the question whether the term 'national security' would perhaps better be replaced by an alternative such as 'territory-wide security'. However, a decision was made to use 'national security' here, since this is the more common term.

[5] References for the definitions used in the thematic chapters and elsewhere can be found in the underlying thematic reports.

SECTION I:
Outcomes by threat theme

This section of the NRA main report presents an overview of the main results for each of the nine threat themes and the analysis relating to the Caribbean part of the Kingdom. For additional information, please see the underlying thematic reports created by the ANV.

2. Climate and natural disasters

As part of the climate and natural disasters theme, four different types of climate and natural disasters that could affect national security have been analysed. These are: floods, extreme weather events, wildfires and earthquakes. The corresponding scenarios deal with possible disasters caused by natural phenomena.[6] The focus is on climate and natural disasters occurring in the Netherlands that in turn generate effects within the Netherlands, although the theme also addresses hurricanes that may occur in the Caribbean part of the Kingdom. Impact and likelihood assessments have taken place for a total of eight scenarios. The figure below shows these scenarios in a comparative perspective.

Figure 2 Risk matrix – climate and natural disasters

Catastrophic		• Flooding from the sea			
Very serious	• Induced earthquake		• River flood	• Hurricane • Heat/drought	
Serious			• Snow storm		• Wildfires
Substantial			• Naturally occurring earthquake		
Limited					
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**

[6] Earthquakes can be the result of natural phenomena or may be induced by humans. Both types have been considered here. It is noted that induced earthquakes are the result of human activities rather than natural phenomena. However, in light of the fact that the scenario still involves forces of nature, this threat is also dealt with under natural disasters.

It is noteworthy that both the impact and the likelihood of the scenarios vary widely. Impact in general is relatively high, which is mainly due to the physical size of the areas that might be hit by climate and natural disasters. The fact that phenomena such as a flood, hurricane (Caribbean part) or extreme heat and drought can affect large areas means that territories or ecological systems can suffer widespread damage, that the number of casualties can be significant, that a serious lack of basic needs can occur and that day-to-day activities may become disrupted in an extensive area. The size of the affected areas also means that, as a result of choices made during the recovery period, residents in one area might come to feel that they are worse off than individuals in other areas. This could give rise to feelings of anger and incomprehension among affected individuals.

What is striking is that climate and natural disasters have a very broad impact. Almost all national security interests can be affected by them. The national security interests that can potentially be affected are territorial security, physical safety, economic and ecological security, and socio-political stability. The international legal order is the only national security interest that would not be affected by climate and natural disasters. The impact is greatest in relation to physical safety. This interest includes criteria relating to fatalities, casualties and chronically ill patients, and a lack of basic needs. All three criteria can be severely hit by climate and natural disasters. The high impact scores for the number of people affected by serious injuries and chronic illness are particularly striking. On the one hand, this involves individuals who receive a direct injury from falling debris during an earthquake, hypothermia during a flood or similar events. On the other hand, disasters may lead to mental health issues such as depression, anxiety or post-traumatic stress disorder, both in and outside of the affected area. This too will affect national security if this were to occur on a large scale.

Climate and natural disasters are closely linked with vital societal processes. Virtually all types of climate and natural disasters can disrupt vital processes such as the provision of power, gas, potable water and telecommunication services. This not only applies to the area suffering from the direct impact of an event. Cascade effects can also cause vital processes to fail in other areas. Loss of vital processes causes disruption to daily life and could result in a lack of basic necessities.

There is also a strong link with economic threats. Various types of climate and natural disasters could for example threaten the Netherlands' role as a key logistical hub by rendering certain transport modes temporarily unavailable. This would restrict the transport of goods from and to the hinterland, causing a rise in transport costs, loss of prosperity and shortages of specific products.

As indicated, the likelihood of the scenarios also varies widely. Some threats already occur with a degree of regularity, yet their impact has so far remained relatively limited. In spite of this, it is quite conceivable that their impact may increase and that the threat will indeed take on the scope of a disaster. This can be illustrated by wildfires. Uncontrollable wildfires occur on average once every year. The intensive use of natural areas means the risk of casualties is high. If multiple wildfires were to occur simultaneously, an additional challenge arises in how to allocate fire-fighting capabilities. Add to this that hardly any control measures are put in place to reduce the risk. Experts therefore believe that the question is not if but when an uncontrollable wildfire with serious consequences will occur.

The scenario looking at an induced earthquake is seen as very unlikely. This conclusion is based on the combination of the various elements in this scenario – a major earthquake resulting in serious consequences such as casualties and building collapse. This does not alter the fact that induced earthquakes, albeit with a magnitude smaller than that used in the scenario, occur with some regularity in the Netherlands, particularly in Groningen. Although these earthquakes have a significant impact in the affected area, they do not result in fatalities or the collapse of buildings.

This assessment focuses on threats that may affect the Kingdom of the Netherlands in the next five years. However, in order to create a picture of slowly emerging threats, a review was also carried out into developments that could result in threats over the longer term (in 10 to 20 years) or which influence the impact and likelihood in a way that means threats could undermine national security more quickly or more severely over time.

Climate change is a major development that will heighten the impact and likelihood of virtually all threat categories, with the exception of earthquakes. This will be discussed in greater detail in Chapter 13. Aside from climate change, the impact of the threat categories is also influenced by both economic growth and demographic developments in the Netherlands. Economic and population growth increases the potential impact of flooding, wildfires and earthquakes in areas that are susceptible to these threats. Not only will the economic damage be greater, the number of potential casualties will be higher too. The ongoing investments in homes and infrastructure in the lowest parts of the Netherlands in relation to sea level can serve as an example of this. The long lifecycle of this type of investment means they are certain to see the long-term effects of climate change. Another fact is that society is becoming increasingly vulnerable to climate and natural disasters such as extreme weather events and earthquakes.

In addition to this, there are upcoming technological advances that may bring benefits as well as threats in the context of climate and natural disasters. An example of this is geoengineering, which involves large-scale interventions in our climate to counteract global warming and its effects. A number of countries already use geoengineering techniques, for example to combat extreme heat or create rainfall, and intend to make more frequent use of these. The long-term side-effects of geoengineering for our climate, environment and ecosystems are not known and could carry high risks as they might in fact cause extreme weather events or result in depletion of the ozone layer. In intentional and unintentional ways, the use of geoengineering may also generate geopolitical tension. When global climate policy fails, the probability increases that various countries will turn to geoengineering in order to combat the effects of climate change.

3. Infectious diseases

Within the infectious diseases theme a distinction is made between four different threat categories:

- Human infectious diseases and zoonoses;
- Animal and plant diseases;
- Antimicrobial resistance (AMR);
- Food crises.

The distinction between the first two threat categories is predominantly based on the mode of transmission between humans, animals and plants. Human infectious diseases entail transmission from human to human, whereas zoonoses involve transmission from animals to humans. The spread can then continue among humans, as illustrated by the COVID-19 pandemic. The Animal and plant diseases category does not involve transmission to humans. The AMR and Food crises threat categories have been reviewed separately, due to the different nature of these types of threats and as a result of the fact that there are other factors at play in addition to the link to infectious diseases. No scenarios were created for these two categories. Both AMR and food crises are considered latent threats. The scenarios that were analysed within the infectious diseases theme are shown in the risk matrix below.

Figure 3 Risk matrix – Infectious diseases

Catastrophic			• Pandemic caused by a respiratory virus transmissible from human to human		
Very serious			• Flu pandemic		
Serious					• Flu epidemic
Substantial				• Outbreak of foot and mouth disease among cows	
Limited			• Outbreak of a zoonotic variant of avian flu		
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**

Human infectious diseases and zoonoses

What is striking first and foremost in the matrix is the high likelihood of a flu epidemic. This is based on the fact that a flu epidemic takes place on almost a yearly basis, caused by existing variants of influenza viruses. A pandemic is less likely but would have a major impact on national security. The analysis also shows that a pandemic caused by a new respiratory virus transmissible among humans will have a more severe impact than a flu pandemic. The pandemic caused by a new respiratory virus transmissible among humans is based on the COVID-19 pandemic. The origin of the pathogen could be a zoonosis that is transmissible to humans.

The impact of human infectious diseases is mainly seen in terms of the number of fatalities and people getting sick. In case of a severe pandemic, another visible effect is a lack of acute healthcare. Costs are also high and may result in the highest impact category possible for this impact criterium in case of far-reaching measures to combat a pandemic. A final observation is that the scenarios involving a pandemic result in widespread disruption to daily life as a result of (work) absences due to illness and/or measures such as lockdowns. This can potentially lead to societal effects such as social polarisation, diminishing solidarity and rioting. These are certainly conceivable in the scenario that deals with an outbreak of a new respiratory virus transmissible between humans. Here there is a link with the social polarisation, extremism and terrorism theme, which highlights the topic of a lack of trust in government agencies.

The rate of spread primarily depends on whether the pathogen is transmissible among humans, on whether the pathogen can spread via the air or direct contact and on response times. In this regard it is clear, in no small part due to the COVID-19 pandemic, that globalisation (including tourism) is a factor that amplifies the global spread of pathogens.

In order to minimise response times, it is key to devote particular attention to the rapid detection of a pathogen and the adequate identification and recognition of potential signs of an epidemic. Especially with regard to the detection and identification of potential outbreaks of pathogens, the past few years have seen a number of favourable developments. Increasingly advanced molecular techniques are used in combination with bioinformatics to run faster and more accurate diagnoses that make it possible to determine the nature and scope of an outbreak. In addition to this, a holistic early warning system is in place that covers both human infectious diseases and infectious diseases in animals (the One Health approach). This system was also used during the COVID-19 pandemic.

The global outbreak of COVID-19 has exposed vulnerabilities with regard to known response-related issues. Examples include the availability of specialist care (specifically intensive care and ventilators) and options for separate treatment (quarantine) that may be required in the event of a new pandemic. There is also reduced control of the security of supply and availability of personal protective equipment and vaccines, since production is in the hands of a small number of international players in a global market. Yet the urgent need to develop vaccines against SARS-Cov-2 variants has also strengthened global cooperation between business and academia. The COVID-19 pandemic has also illustrated that tensions can arise within society and debate can be generated around topics like vaccines. Debates such as these could potentially be intentionally fuelled by the actions of foreign actors. In this respect, there is also to the possible use of misinformation as part of hybrid threats (see also Chapter 6).

Animal and plant diseases

Recent outbreaks of variants of avian flu (bird flu) have shown that robust preparation for and implementation of a national response is and remains necessary. The decision was made to restrict the analysis of this topic to a scenario for animal diseases and assess this scenario in terms of its likelihood and impact on national security. The reason for this is that plant diseases will not immediately affect national security.

The analysis found that there is a relatively high probability that an outbreak of an animal disease such as swine fever, foot and mouth disease or (non-zoonotic) bird flu will occur in the next few years. In terms of impact, the assessment shows that a great number of criteria will be affected and the overall impact would be substantial. In this context, the greatest effects are seen in terms of financial losses and societal impact. Here, it is clear that the consequences of this type of animal disease would have a significant impact on individuals and businesses in the relevant industry. This is further illustrated by the estimated number of individuals suffering from mental health issues and the impact on daily life. Moreover, expressions of anger and frustrations may manifest in the form of violence and intimidation as response to possible (containment) measures. Feelings of injustice may lead to animosity and social polarisation, which once again provides a link to the theme of social polarisation, extremism and terrorism.

Antimicrobial resistance

Although the issue of AMR does not pose a threat to national security at this time or in the years ahead, the increase of resistance across the globe means AMR should still be considered a ‘silent assassin’ and should therefore continue to be subject to close monitoring.

One of the most worrisome developments in the Netherlands is carbapenem resistance (CRE), because it renders potential bacterial infections difficult or impossible to treat. Prevention of CRE is the subject of close monitoring and all efforts are made to prevent its spread, including by means of screening, early detection and adequate measures to tackle incidental cases and outbreaks. The One Health approach, which involves taking a holistic view of all aspects of human health in relation to animal health and the environment, remains key in this regard.

Food crises

Large-scale food crises are an infrequent occurrence and, based on the previous assessment, the view is that the impact would be limited if a crisis were to occur. This leads to the conclusion that although adequate continued attention to food security is key, incidents and crises in relation to food do not pose a threat to national security. This is not expected to change in the years ahead.

Food scarcity is addressed under the topic of climate change in the thematic report on climate and natural disasters. Climate change, and also international conflicts, may lead to food scarcity in parts of the world, which could cause a rise in food prices and new migratory flows.

4. Major accidents

The major accidents theme address the risks of unintentional radiation accidents, chemical accidents and transport accidents. Under the radiation accidents and chemical accidents categories, the consequences and likelihood of four scenarios have been analysed (two scenarios for each category). The matrix below shows these scenarios in a comparative perspective.

Figure 4 Risk matrix - major accidents

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious					
Serious	• Borssele nuclear plant • Train disaster with flash fire				
Substantial	• Radiation accident in Europe • Failure of an ammonia storage tank				
Limited					

When looking at the risk diagram, the first thing one notices is the fact that all scenarios elaborated for this theme have a low likelihood (the rating is 'very unlikely'). The purpose of elaborating highly unlikely scenarios is to check if and to what extent the major accidents theme can have an impact on national security or whether the theme is predominantly relevant at a local or regional level.

The risk categories within the theme have a broad impact. Most of the national security interests are affected, with the impact being relatively often characterised as substantial or serious and occasionally as very serious. The impact on national security is mainly seen in terms of physical safety, economic and territorial security, and socio-political stability. In brief, these incidents would mainly result in casualties, financial losses and a disruption of daily life.

However, it is important to qualify these conclusions and make a distinction between radiation accidents on the one hand and chemical accidents on the other. For example, an accident at a nuclear plant will not lead to any direct fatalities as a result of radiation exposure. The opposite is true for chemical accidents, where fire, explosions or toxic clouds could result in casualties as well as fatalities. This raises the question of whether several hundred individuals requiring acute healthcare might result in issues in terms of available capacity.

In the case of radiation accidents, a small number of deaths is possible if panic takes hold when the surrounding areas are evacuated. People may also become ill (including mental health issues) and fall victim to the event after some time has elapsed, for example if people succumb to cancer developed as a result of radiation exposure.

The impact of radiation accidents is also partially linked to mitigation measures that are put in place. A prohibition on the grazing of livestock following a major radiation accident would result in financial losses for the agricultural industry. Such a measure could also be taken if a major accident were to occur at a plant elsewhere in Europe and the resulting cloud of radioactive material reaches the Netherlands due to unfavourable winds. Lastly, there will be serious implications for residents in the vicinity of a plant in case they are forced to evacuate and remain elsewhere for an extended period of time.

Both chemical accidents and radiation accidents could conceivably start a societal debate on the accident itself, operations at the plant in question and any measures taken. This debate could for example focus on the use nuclear energy or the transport of hazardous substances by rail. In addition to debate, a major incident could prompt expressions of anger and other emotions amongst citizens and also threats or instances of intimidation towards people seen as responsible.

As with chemical accidents, transport accidents may lead to a large number of casualties and fatalities, in particular when the accident involves a means of transport capable of carrying a large number of passengers, such as an airplane or a cruise ship. Fortunately, the likelihood of such an accident is (once again) low. Transport accidents may also result in cascade effects that could for example disrupt the role of the Netherlands as a key logistical hub or other vital processes. This links back to the economic threats and threats to critical infrastructure themes.

In a more indirect sense, there are also links to a number of intentional threats within the major accidents theme. One of the scenarios examined as part of the cyber threats theme deals with a cyber attack during which a business in the chemical industry is targeted and a hazardous substance is deliberately released. Although the likelihood of such a scenario is relatively low, it is estimated to be more likely than its unintentional counterpart. The intentional use of CBRN agents is considered in the international and military threats theme.

Finally, the radiation, chemical and transport accidents categories have connections with the subject of energy transition. A potential debate on nuclear energy following an accident at a nuclear power plant has been mentioned above and is something that may also become relevant in relation to the energy transition process. Moreover, substances such as hydrogen may take on an important role in the energy transition. This role comes with risks that must be taken into account. Transport accidents could lead to cascade effects that affect the energy system, for example if a shipping accident were to cause damage to a wind farm. In addition to the aspects briefly raised here, the energy transition has multiple facets that are relevant for national security. This is discussed in greater detail in chapter 13.

5. Social polarisation, extremism and terrorism

The social polarisation, extremism and terrorism theme has four separate threat categories – social polarisation, non-violent extremism, violent extremism and terrorism. Social polarisation refers to an increase in the 'us-versus-them' way of thinking in society and a situation in which groups are increasingly opposed to one other, giving rise to internal tensions. In some instances, social polarisation can contribute to a breeding ground for radicalisation. As groups experience more divisions between them and increasingly begin to see each other as adversaries, the opinions held by each group can develop into radical views. Extremism refers to the active pursuit of and/or support for drastic changes in society that may pose a danger to the democratic rule of law or the continued existence thereof, including through the possible use of undemocratic methods that could undermine the functioning of the democratic rule of law. Extremists may seek to achieve their goals by either violent or non-violent means. Lastly, terrorism is the threat, preparation or perpetration of ideologically motivated severe violence against humans or acts aimed at disrupting the fabric of society, with a view to bringing about social changes, instilling fear among the population or influencing the political decision-making process. All four categories in some way concern themselves with the structure and components of the Dutch democratic legal order and a possible reordering thereof. As social polarisation progresses to terrorism, the accompanying level of violence increases.[7]

Groups engaged in extremist or terrorist activities may belong to a wide range of movements or ideologies, including right-wing extremism, anti-government extremism, left-wing extremism and radical Islam. For each of these movements and associated groups, aspects such as the appeal of a movement and the potential for violence by a specific group is influenced by domestic and international developments. The thematic report on social polarisation, extremism and terrorism discusses relevant developments for a number of these movements and the topic of social polarisation in greater detail.

Spread across the four threat categories, ten scenarios have been analysed in terms of their impact and likelihood. The matrix below shows these scenarios in a comparative perspective.

[7] Compared with previous risk assessments carried out by the ANV, such as the 2016 National Security Profile and the 2019 National Risk Assessment, a relatively high number of scenarios were elaborated for this theme. The decision to develop a larger set of scenarios was taken in light of the fact that a number of topics within the social polarisation, extremism and terrorism theme have gained in prominence over the past years. The aim here is to reflect the diversity of threats within this theme.

Figure 5 Risk matrix – social polarisation, extremism and terrorism

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious					
Serious		• Multiple terrorist attacks • Infiltration of public administration	• Assault on and hostage-taking in parliament	• Social polarisation surrounding conspiracy theories	
Substantial			• Attack on pride event • Escalation of violence by right-wing extremists • Anarcho-extremism • Subversive enclaves	• Anti-government extremism	
Limited					• Lone actor

In general, it is striking that the scenarios developed for this theme have a relatively high rating in terms of likelihood. Eight out of ten scenarios are rated as 'somewhat likely' or higher, with the scenario on a lone actor even being rated 'very likely'. It is however important to point out that the consequences of this scenario are limited, especially when compared to the other scenarios in the terrorism category.

All scenarios have an impact on socio-political stability. The scenarios for the social polarisation, non-violent extremism and violent extremism categories in particular show the highest impact scores in relation to this national security interest, primarily for the subversion of the democratic constitutional system and societal impact criteria. These criteria also have major importance for the consequences of scenarios within the Terrorism category. However, as the extent of an attack and the intensity of violence used increase, physical safety emerges as the national security interest that is affected most severely in this category. As regards the majority of the scenarios within the other categories, casualties and fatalities cannot be ruled out but numbers will remain limited.

A closer look at the consequences of the various scenarios for the democratic constitutional system reveals multiple scenarios where the rights and freedoms of citizens or groups of citizens are undermined, for example through discrimination, exclusion, threats and, in some instances, physical violence. Many of the scenarios also reference a negative effect on (perceived) security among politicians, public administrators or government officials. However, threats, intimidation and, in some instances, physical violence do not only affect the individual that is targeted. They also have a ripple effect on the people surrounding this individual, such as family members and co-workers. This applies as much to citizens being subjected to exclusion, intimidation or similar as it does to individuals employed at institutions linked to the democratic constitutional system that become victim of threats. Politicians feel less able to speak out on certain topics out of fear they too will become victims of intimidating home visits, and prospective or current local councillors and members of the municipal council may quit out of fear for their own safety and that of their families. Put differently, ideologically motivated abuse or home visits do not only

affect the targeted official, administrator or politician but their professional group as a whole. The same reasoning also applies to citizens who suffer an erosion of their rights and freedoms. Discrimination or intimidation of individuals has repercussions for the sense of security and perceived freedom of the wider population group these individuals are part of. The extent of such repercussions depends in part on the gravity and the duration of these events.

A further factor that is important in this regard is the extent to which society – and therefore the democratic constitutional system and the overarching legal order – is resilient to the events described in the scenarios in this thematic report. Relevant questions include whether there is sufficient capacity to support or provide security for individuals who are being targeted by extremists' threats and the possibilities for the early detection of future terrorist attacks. Two scenarios within this theme – infiltration of public administration and multiple terrorist attacks – show a positive deviation in respect of their likelihood. For both cases, the analysis revealed that resilience sits at a level that allows the likelihood of these events to be downgraded to rating B (unlikely). Resilience, however, is not a given. For these scenarios too, it will be key to maintain vigilance with regard to the level of resilience. It will also be important to examine more closely how resilience can be increased for the type of events in the other eight scenarios covered in this theme.

The fact that the NRA is split into nine different themes does not mean to say there are no links between them. Consider social polarisation for instance, which may arise in connection with a wide range of topics that have been included in one of the other thematic reports, such as issues relating to the climate and international cooperation. It should be evident that tensions around these and other topics could ultimately also lead to manifestations of extremism or terrorism. Aggravating social polarisation and extremism can also be part of a deliberate strategy by state actors to destabilise Dutch society, for example in the context of hybrid operations. Such subversion by state actors is covered in the foreign subversion of the democratic constitutional system theme.

6. Foreign subversion of the democratic constitutional system

The foreign subversion of the democratic constitutional system theme comprises four threat categories – foreign influencing (hybrid threats), espionage, foreign interference and organised crime. Each of these categories will be discussed individually.[8] The following risk matrix presents an overview of all the scenarios developed for this theme along the axes of likelihood and impact.

Figure 6 Risk matrix – foreign subversion of the democratic constitutional system

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious					
Serious			• Criminal violence towards media and government • Foreign interference diaspora communities	• (Covert) influencing by China	• Hybrid operations by Russia - exploiting societal debate (migration)
Substantial				• Cyber espionage targeted at public authorities • Organised crime throughout the Netherlands • Traditional state espionage • Criminal interference in business	
Limited					

[8] The reason for the individual treatment of the two categories within the NRA this is that there are relatively large differences between them.

Foreign influencing (hybrid threats)

Foreign governments and other actors engage in a range of activities that can exert influence on other nation states in a variety of ways. These activities do not necessarily need to be directly aimed at the Kingdom of the Netherlands or its allies in order to have a detrimental impact on Dutch national security. Foreign influencing is undesirable for national security as it may gradually act to undermine the Dutch democratic constitutional system. Different forms of influencing or subversion can be captured under the term 'hybrid threats'.

In light of the fact that hybrid campaigns are often carried out by state actors (sometimes with the help of non-state actors such as criminal organisations), hybrid threats can be considered part of the overarching concept 'state threats': *forceful, subversive, misleading or covert activities by or on behalf of state actors that are below the threshold of armed conflict and which may harm the national security interests of the Netherlands through a combination of the objectives pursued, means used and resulting effects.*

Hybrid threats are often latent threats as they do not always manifest themselves in a single event or occurrence (such as a ransomware attack). What this means is that a typical hybrid threat consists of many different types of activities that do not necessarily affect national security in themselves. It is in fact in the interest of a hybrid actor to covertly influence another state and its citizens for as long as possible, without being caught for illegal activities. Consider economic investment and cultural exchange programmes for instance. These are not illegal in themselves and initially revolve around economic or other benefits. However, these instruments may also become vehicles for foreign influencing or subversion, with the cumulative effect of such legal activities in the long term possibly being that a state becomes heavily dependent upon another state. The latter then has the power to exert not only economic but also political influence within the former state. In other words, hybrid threats are a 'slow burn' because influence is built slowly and under the radar, until a point of no return is reached and a state has unintentionally become dependent on another state in a wide range of ways.

Hybrid threats are the perfect example of a topic that cannot be captured in a single-focus scenario (dealing with a single phenomenon), as they are typically threats that develop over the longer term and the impact of which is also not seen until later on. For this reason, hybrid threats have been included as an overarching topic in chapter 13, which highlights links with other themes that that contain individual phenomena that can also very conceivably be part of a larger hybrid threat. It is vitally important to always approach specific threats from a holistic perspective. While it is clearly important to be able to mitigate individual events (e.g. a cyber attack), it is more pertinent still to remain aware of the bigger picture in those instances and look for connections between events (*connecting the dots*). Something that would initially appear to be a stand-alone event may take on a completely different guise when it is found to be part of a larger whole, something that will also have an impact on the government response.

Espionage

Espionage is the covert gathering of intelligence relating to the political or economic situation in a country. The aim may also be to steal trade secrets or personal data, or acquire knowledge on specific technologies. The Netherlands is an attractive target for espionage by other countries. Our country is a member of the North Atlantic Treaty Organisation (NATO) and the European Union (EU), and has access to interesting information. Our country is also host to numerous international organisations, including the Organisation for the Prohibition of Chemical Weapons (OPCW) and the International Criminal Court (ICC). In addition to this, there is a wealth of knowledge and high-performance technology to be found in Dutch knowledge and educational institutions as well as in the corporate sector.

Espionage may be carried out in a traditional manner, by approaching individuals who can then be used to gain access to information. To this end, agents of foreign secret services are always on the lookout for interesting people (sources) such as government officials, military personnel, scientists, senior executives and journalists. In addition, there is extensive digital espionage nowadays. Online or cyber espionage is the stealing, whether undetected or otherwise, of information by penetrating digital systems. This involves the breaching of information systems, which has a significant impact on the integrity of digital infrastructure. Parties engaged in espionage may use information acquired through traditional or cyber espionage to enhance the competitive position of their domestic economy, strengthen their armed forces or exert influence on processes and decision-making within international institutions, depending on the nature of that information. All of this may be detrimental to the position and interests of the Netherlands. Cyber espionage can be deployed alongside other hybrid tools in order to undermine the functioning of state actors or to achieve various other purposes. Cyber espionage may also be deployed in order to steal valuable information, such as technological information or trade secrets. It is of course possible for traditional and digital forms of espionage to be deployed in tandem with each other.

Espionage is considered to be a serious threat to the Netherlands and its allies. States such as Russia and China

have major geopolitical ambitions and therefore seek information that enables them to modernise their armed forces, reinforce their economies or influence political decision-making in the West. Simultaneously, attempts at digital espionage by foreign state actors aimed at Dutch ministries have led to an increase in attention and wariness for the threat that cyber espionage can pose. Something that is also reflected in an increased concern regarding the use of technology provided by foreign suppliers and the possibility that the hardware or software in question could have 'backdoors' that may enable foreign intelligence services to gain unwarranted access. Another topic that has attracted increasing attention in recent times is espionage and sabotage targeted at underwater infrastructure, such as subsea cables. At the start of 2022, the Ministry of Justice and Security submitted a legislative proposal for consultation that aims to modernise the penalisation of espionage. This could help to improve future possibilities for tackling 'novel' forms of espionage (such as cyber espionage) for various purposes.

As part of the NRA, scenarios for both traditional and digital espionage have been composed. Although these scenarios and for that matter the threat category as a whole could be said to encompass relatively small-scale incidents, such as the bribing of a single defence staff member, the consequences could nevertheless be severe and affect national security. Furthermore, espionage is a phenomenon that has a relatively high likelihood of occurrence. The specific national interest that will be affected the most is highly dependent on the type of information that is acquired by means of espionage as well as the intended target. In practice, it is not always straightforward to identify the impact of (cyber) espionage on national security, typically because there is a degree of uncertainty as to who has acquired what information and the end to which the actor intends to use that information. There is for example concern regarding the economic impact of espionage but these economic consequences are in turn difficult to define.

This is because actors engaging in espionage may choose to withhold crucial information acquired until an opportune moment arises for them to deploy it. The precise moment and the context within which the information is used will significantly determine the ultimate consequences for the Dutch economy and other national security interests. If, for example, a store-and-forward strategy is used in order to leverage crucial information during international negotiations, the effects may even include harm to the international legal order (through the influencing of multilateral decision-making processes). As a result, geopolitical developments also provide an important context in relation to both the likelihood and the impact of an information breach.

Foreign interference

Foreign interference relates to interference by state actors that may lead to a severe disruption and malfunctioning of the democratic legal order and open society. Foreign interference may undermine the integrity of Dutch public administration if the independence of parliament or the judiciary becomes compromised or if doubt arises as regards the fairness and anonymity of elections. Foreign subversion also has the potential to undermine the stability of society if acceptance in regards to different population groups comes under pressure. This threat category focuses on foreign interference aimed at diaspora communities in the Netherlands, for example by seeking to widen cultural differences between these communities and other Dutch citizens, and tracing or intimidating political opponents.

Foreign interference aimed at diaspora communities is often a gradual process and activities are often conducted in secrecy. The dividing lines within the affected diaspora communities are often deepened at a gradual pace. The interfering state will then actuate those dividing lines at a time opportune to it, for example when it wishes to mobilise members of the diaspora community for elections in their country of origin. This type of foreign interference may take on many guises and can vary from the previously mentioned electoral mobilisation of large groups of voters to the intimidation or even assassination of members of the opposition residing in the Netherlands. It is therefore difficult to arrive at an unequivocal assessment of the impact of foreign interference aimed at diaspora communities.

The type of foreign interference that is often most visible to the general public is that aimed at electoral mobilisation. This will affect Dutch social and political stability in particular. Large groups of Dutch citizens are brought into direct opposition vis-à-vis each other, stirred up by a foreign power.

Organised crime

Crime occurs in varying forms and degrees within Dutch society. Whereas a large number of offences committed in the Netherlands will not have any relevance for national security, the opposite is true for activities that can be designated as organised crime.[9] The term organised crime

[9] A term often used instead of organised crime is 'subversive crime'. By definition, subversive crime implies that the relevant criminal act in some way or another harms (subverts) the Dutch political or social system. By contrast, organised crime is a more neutral, overarching term. Although organised crime largely covers the same criminal activities as subversive crime, it does not qualify the effect on society. Since national security looks at a wide range of effects of a threat, and not just the impact on the democratic constitutional system, the ANV has chosen to use the term 'organised crime'.

is applicable when three conditions are met:

- Crimes in question are serious offences, such as (large-scale) fraud, violent crime and drug-related crime, committed in a systematic manner.
- These crimes are committed by groups that are primarily pursuing illegal gains. The offences must therefore be carried out by a group and be aimed at acquiring things such as power, money or status. This is in contrast to perpetrators acting individually or crimes committed in the context of a relationship.
- Criminals are able to shield their crimes in a reasonably effective manner, for example by using facilitators in legitimate society. These are people whose position in a legitimate industries means they can provide facilitating services to criminals, with varying degrees of intent and coercion. Examples include real estate brokers and people working for car rental companies or in the financial sector who assist a buyer, tenant or client in concealing their true identity or the origin of their financial means.

In the Netherlands, groups of criminals engaging in organised crime are regularly referred to using the term *Crimineel Samenwerkingsverband (CSV)* or 'criminal partnerships'. These organised crime groups carry out a wide range of activities that can potentially constitute organised crime, including human trafficking, cybercrime, fraud and property crime. Dutch criminals are also key international players in the trafficking and manufacture of narcotic drugs. The Netherlands is a key hub for the cocaine trade and (to a lesser extent) the heroine trade, in part due to its geographical position, good infrastructure, the presence of diaspora communities and access to the required knowhow. There is also large-scale domestic production of primarily cannabis and synthetic drugs, predominantly for export. With a view to shielding and facilitating these activities, criminals not do only engage in money laundering their illicit gains but will also seek to influence others, for example by way of bribery, infiltration, threats or physical violence. These efforts to exert influence may be targeted at other criminals, the perpetrators' direct social environment, individuals employed in private sectors of interest for criminals, or civil servants and public administrators.

In general, organised crime remains relatively invisible to the larger Dutch society. This is because most criminals will specifically aim to keep a low profile and shield their activities. At the same time, prominent incidents that lift this veil of secrecy take place with some regularity, including assassinations in public spaces. Organised crime exerts its influence both through these eye-catching incidents as well as through its permanent, latent presence. Organised crime can occur throughout the Netherlands and harm a broad spectrum of groups and sectors. The fact that organised crime is to a degree latent in nature means its dynamics are difficult to capture in a relatively brief, covering a handful of pages. The three scenarios developed as part of the NRA are therefore primarily intended to raise of awareness the topic in the context of national security and provide an overview of the possible consequences of manifestations of organised crime.

Organised crime can have an impact on a relatively high number of national security interests, which serves to illustrate the many ways in which organised crime can influence society. The highest impact scores are predominantly related to the violation of the democratic constitutional system. This can for the most part be attributed to criminal threats towards government officials, as well as possible breaches of integrity and a possible loss of confidence among the general public in regard to the government's capacity to fight organised crime. At the same time, the scenarios covering organised crime are characterised by a high likelihood.

Furthermore, the organised crime threat category does not exist in isolation. There is a strong link between organised crime and the cyber threats theme. Criminals do not only happily exploit technological advances such as the wide availability of end-to-end encryption services for their own ends, they also engage in cybercrime. A well-known example of this is performing ransomware attacks, where malware might be used to gain and then block access to a system for its users. Payment is then demanded in return for restoring that access. An example of such a ransomware scenario is discussed in greater detail in the thematic report on cyber threats. Criminal activities may furthermore be carried out under the direction of state actors, for instance as part of hybrid operations. This phenomenon is referred to as 'crime as a service'.

The development of organised crime depends on the current and future resilience of society. The activities and success of parties engaged in organised crime in part depend on their social environment. Individuals who have confidence in the police and public authorities and that are able to successfully participate in society, are less easily tempted to facilitate or become involved with organised crime. By contrast, facilitating or engaging in criminal activities will more readily be considered if individuals have no socio-economic prospects and have negative experiences with the authorities. In recent years, politicians and public administrators have once again begun to pay more attention to (the importance of) preventing organised crime. This has led to more financial resources being made available by the central government for the combating of organised crime while awareness has also increased among local and other authorities. Multiple national initiatives have been set up that aim to coordinate

and align the tackling of subversive or organised crime. These include the Ministerial Committee for Combating Subversion *(Ministeriële Commissie Aanpak Ondermijning, MCAO)* and the 'programmatic DG' at the Ministry of Justice and Security. This heightened focus and awareness can help to increase resilience against organised crime, although the contribution made will depend on how structural this attention will turn out to be. There is a danger that after increased political and administrative focus, organised crime, in part due to its relative invisibility, is put on the back burner in favour of policy areas such as the climate, healthcare and housing. The coming years will reveal whether the additional focus on and investment in relation to organised crime have been adequately safeguarded and is producing the desired effect.

General reflection

Despite the substantive differences between the four threat categories considered within this theme, it is possible to identify a number of connecting links. The first is the violation or subversion of the democratic constitutional system. In this respect, the threats covered within the theme show a high degree of similarity. The Dutch democratic constitutional system can be negatively affected by activities undertaken by both state actors and non-state criminal actors. Both types of actors are motivated by a desire to realise their own goals, with a negative impact on Dutch society as a result.[10] State actors and the threat they pose constitute a second connecting link for at least three out of four of the threat categories. The wider concept of state threats covers hybrid threats and (digital) espionage, as well as foreign subversion of diaspora communities.[11] The analyses carried out in respect of this theme reaffirm that a number of the threats covered by this broader concept can harm the democratic constitutional system. In a number of instances, organised crime can also be considered a state threat. This applies when criminals operate under the direction of a state actor, who could for example instruct them to carry out a ransomware attack.

A final connecting link is the importance of technological advancements and the digitisation of society for each of the threat categories considered here. Technological advancements for example permit criminal actors to better shield their communications by using apps that automatically encrypt messages. The fact that some aspects of daily life are increasingly conducted online, such as banking, making purchases and communicating with others, also creates opportunities for criminal actors in the area of scams, the sale of narcotics and cybercrime.[12] For their part, state actors have more and more options at their disposal for the (online) monitoring of diaspora communities residing in the Netherlands. Moreover, widespread access to and use of social media platforms and messaging services also facilitate the deployment of misinformation campaigns in the context of hybrid operations. Another effect of digitisation is that networks, systems and process automation become increasingly interwoven. This creates vulnerabilities that state actors may seek to exploit when carrying out hybrid operations, such as offensive cyber operations for the purpose of sabotage or espionage. At the same time, the creation of a 5G network with nationwide coverage and the roll-out of other new technology require hardware and software that may be sourced from foreign suppliers. Although this is not an issue in itself, there are countries that will deliberately include vulnerabilities in their products which they can later use to acquire sensitive information. As society increasingly moves online and technological advancements continue to emerge, it is key to monitor what vulnerabilities this may entail and what the impact on the democratic constitutional system might be if actors with malicious intent decide to exploit those vulnerabilities.

[10] It is evident that activities of non-state, extremist actors may also result in a violation of the democratic constitutional system. This is discussed in the thematic report on social polarisation, extremism and terrorism.

[11] The concept of state threats refers to forceful, undermining, misleading or covert activities by or on behalf of state actors that are below the threshold of armed conflict and which may harm the national security interests of the Netherlands through a combination of the objectives pursued, means used and resulting effects.

[12] The phenomenon of cybercrime is dealt with in greater detail in the thematic report on cyber threats.

7. International and military threats

The international and military threats theme considers four threat categories: (i) fragility in the vicinity of the Netherlands and/or the EU, (ii) pressure on multilateral security institutions, (iii) armed conflict between centres of power, and (iv) proliferation of weapons of mass destruction. In the final assessment, six of the twelve scenarios assessed in terms of their likelihood and impact on national security have a relatively high impact rating concerning the national security interest international legal order and stability. These scenarios are: IS seizes power in Morocco; deployment of nuclear weapons in the Iran and Saudi Arabia conflict; collapse of the Venezuelan state; reunification of China and Taiwan; temporary occupation of an EU Member State (Finland); and the disintegration of NATO.

Figure 7 Risk matrix – international and military threats

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious	• IS seizes power in Morocco • Deployment of nuclear weapons in the Iran and Saudi Arabia conflict	• Reunification of China and Taiwan • Temporary occupation of an EU Member State	• Collapse of the Venezuelan state • Disintegration of NATO		
Serious			• Crisis in the South China Sea • Rift within the EU	• Break-up of Bosnia-Herzegovina	
Substantial		• Terrorist attack using a biological weapon	• Disintegration of the OSCE	• Innovation of nuclear delivery systems	
Limited					

Mounting geopolitical tensions between various great powers threaten our national security as well as the security and stability of our surroundings. The Russian invasion of Ukraine at the beginning of 2022 is an example of the growing military threat, resulting in a renewed threat of armed conflict for European borders. International tensions are also on the rise further away from Europe, including in South East and East Asia. Here, China is increasingly asserting itself as the economic, political and military powerhouse of the future. These geopolitical tensions are illustrated by the annual rise in military spending around the globe. Even though a direct threat to the borders of the Netherlands is unlikely, there is nevertheless an increasing risk that the Netherlands could become involved in international and military crises, for example as a result of Treaty obligations under Article 5 of the NATO Treaty and Article 42(7) of the EU Treaty for example.

In addition, a race has begun to gain control over unexplored regions (the Artic, the seas and space) that could create new hotbeds of conflict. Conflicts and fragility on surrounding Europe also create a power vacuum that allows extremists, terrorist groups and organised crime to operate without impunity, put the relevant regions under pressure and become a threat to our national security and trade routes. When this situation contributes to high, uncontrolled and irregular migration, our public space can be influenced and social stability can come under significant pressure. What is more, state actors who are able to influence migration flows do not hesitate to use them as a tool to pressure us.

All of this marks a new era of international and military threats, in which both state and non-state actors increasingly turn to hybrid methods and techniques. This includes the combined use of economic, military and other instruments that blur the line between war and peace and which can range from the influencing of public opinion by means of misinformation and propaganda as well as conducting cyber attacks and espionage to blackmail, sabotage and attacks using CBRN agents. These hybrid attacks target an opponent's vulnerabilities, are ambiguous in nature and involve a conscious effort to remain below detection thresholds, thus making it difficult to attribute the attacks in question. Another aim of hybrid attacks is to erode our capabilities by weakening our democratic constitutional system as well as undermining cohesion and solidarity within society, the EU and NATO.

A rule-based, functional international legal order is crucial to our national security interests. Its multilateral framework helps to reduce the unpredictability of the changing nature of international relations and prevents conflict and instability. However, the mounting geopolitical tensions between the great powers are placing this multilateral system under significant pressure. These tensions can take on a range of forms, varying from the use of a veto within the UN Security Council to the withdrawal from international conventions and treaties. The disruption of international cooperation in areas such as free trade, security, non-proliferation and climate action has a direct impact on our economy and our international position, and also directly affects Dutch citizens abroad. In today's globalised world, the reach of our Kingdom does not stop at its physical borders. Dutch citizens, businesses and our diplomatic missions, consular posts, posted military and posted civil personnel in particular run the risk of becoming caught up in violent actions and combat operations.

The EU, NATO, OSCE and UN are not immune to the pressures exerted on the international system. On the one hand there are certain states that actively attempt to undermine the cohesion and capabilities of these organisations through a wide array of hybrid actions. On the other hand there are members who are turning away from multilateralism. The fact that certain EU Member States are specifically calling into question the basic principles and values underpinning the European integration project, including the democratic constitutional system, undermines not only the international influence of the EU but also the same foundations that are crucial to our prosperity, the protection of our safety and respect for personal and public values. Organised and coordinated strategies to manipulate opinions through the mass dissemination of fake news and misuse of the algorithms integral to the current working and programming of social media, have a growing impact and can destabilise societies by influencing public opinion or democratic processes such as elections.

Another major risk are weapons of mass destruction. The past years have seen an increase in threats involving the use chemical, biological, radiological or nuclear (CBRN) agents. Against the backdrop of increasing geopolitical tensions, regional arms races are taking place and nation states feel less and less bound by multilateral arms control agreements. A further threat lies in the inclusion in weapon systems of technological advancements that reduce reaction times and increase unpredictability. Advances in biological science bring potentially dangerous applications within reach, including for non-state actors. An attack using CBRN agents requires specific knowledge but this barrier is lowered as a result of increased access to information (via the internet). There are also regular calls from terrorist organisations or extremists to carry out attacks using CBRN agents.

Seen through the lens of the six national security interests, the threats within the international legal order and stability theme receive relatively high ratings in respect to the

national security interest covering the proper functioning international legal order and stability. A further, overarching observation is that this international order is currently undergoing great change. The post-war era in which the international state system and power relations were dominated by the United States definitely appears to be over. We now see an increasing number of challenges to the US from a surging China and a revisionist, revanchist Russia. The international order is also highly complex in nature due to continued international cooperation in a number of areas. As a result, some aspects of the multilateral world order are retained while other elements of this same world order have come under considerable pressure. In a wide range of areas, changing coalitions work with and against each other. These international relations generate a high level of uncertainty and contribute to a deterioration of the international and military security situation.

8. Economic threats

Economic threats arise in many ways and can vary widely in scope, from trade contraction, financial crises, shortages of strategic commodities such as fossil-based energy and key raw materials, to extensive industrial espionage and other forms of interference in Dutch industry. These scenarios may have a considerable or even high impact in the short term. In the longer term, there is the possibility of risk accumulation.

The Economic threats theme focuses on five threat categories:

- Threats to the Netherlands' role as an important logistical hub
- Contraction or distortion of international trade
- Foreign interference in industry
- Strategic dependencies
- Destabilisation of the financial system

The scenarios within each of these threat categories affect our national security. However, they do so in different ways, to different degrees and are subject to different levels of likelihood. This is summarised in the risk matrix below.[13]

Figure 8 Risk matrix - economic threats

Catastrophic					
Very serious			• Systemic actor in the finance sector facing great difficulty	• Import of fossil-based energy	
Serious		• Trade war involving Europe • Disruption of payments • Foreign state acquiring a minority interest in a major telecommunications provider			• Trade disruption due to production issues abroad
Substantial		• New European debt crisis	• Foreign regulation of tech companies	• Adjustment of the value of financial assets as a result of expectations not being realised	
Limited				• Shortages of key raw materials • Covert acquisition of an unlisted company whose products include dual-use goods	• Foreign venture capital investment in health and biotech start-ups
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**

[13] The matrix uses abbreviated titles for some of the scenarios.

Impact on economic security

The impact on economic security is measured by the extent to which the scenarios result in a cost to the public or private sector and the extent to which the vitality of the Dutch economy is compromised (measured as increases in unemployment and national debt).

The impact on economic security is relatively high in scenarios that strike at the heart of the economy. This is seen in almost every threat category. For a small and open economy like the Netherlands, a distortion of international trade or a contraction of global trade carries a high cost, which in turn has an impact on employment and public finances. The same is true for major macro-financial shocks in the destabilisation of the financial system category. This effect is relatively independent of the origin of the shock itself. Our economic security will be affected by both domestic and foreign shocks. Both disruptions of production as well as trade disputes will cause trade to contract and the macroeconomy will suffer in case of a shock to major actors within the system in either the financial or sovereign debt markets.

For scenarios that describe a threat to the logistical hub function of the Netherlands, the link between the eventual degree of economic damages and the origin of the disruption varies. As a general rule, Dutch prosperity is responsive to disruptions of this function, but not all disruptions have an equal impact. In order to accurately reflect the origin of the disruption, the scenarios in relation to the logistical hub function were incorporated in the thematic reports on international and military threats and natural disasters. A disruption of our logistical hub function that effectively leads to a contraction of global trade (as in the case of a reunification of China and Taiwan, see the thematic report on international and military threats) comes with a high economic cost. This is less so in the event of a temporary and more localised disruption as a result of interruptions in inland shipping during extreme weather (as in the case of extreme heat/drought, see the thematic report on climate and natural disasters).

In relative terms, the impact on economic security is generally less severe in the scenarios that deal with foreign interference in industry and strategic dependencies, although the import of fossil fuel scenario is an exception to this. Foreign interference in industry can, but does not by definition, result in costs. Any such costs are also lower when compared with major macro-economic shocks. Another observation is that the vitality of the Dutch economy is only at stake in rare instances. Strategic dependencies have associated costs, in particular the dependency on fossil energy imports should these suffer disruption, but over a longer, five-year term the impact on economic vitality is limited.

Impact on other security interests

Risks to our national security may still be present even where costs are low or the impact on the vitality of the Dutch economy is limited. This is because the scenarios will often also affect other national security interests. The costs of a disruption to payment systems are relatively modest, but societal effects are nevertheless severe because of harm to the integrity of digital infrastructure and a disruption of daily life. A dependency on fossil-based energy may cause citizens to experience a lack of the basic need for (affordable) energy. Trade wars are accompanied by international and political fall-out and cause harm to the rule-based international financial-economic system. A reduction in trade as a result of production issues abroad may result in shortages of essential goods such as medicines. Espionage following a takeover in the telecommunications sector is a violation of the integrity of the Dutch digital infrastructure. Many instances in which economic threats do not affect economic security still pose risks to our national security, potentially via another security interest.

The economy as an endogenous system, the role of policy and the build-up of latent threats

A number of scenarios only have a limited direct impact on the economic security interest, especially where the vitality of the Dutch economy is used as a reference. This holds true in particular for the foreign interference in industry and strategic dependencies threat categories. In the scenario dealing with foreign acquisition of Dutch start-ups, the economic consequences are limited, mainly because the direct 'economic loss' over the medium term is virtually zero. Start-ups are typically small enterprises that do not generate a large turnover yet and have an uncertain future. As a result, the cost associated with a loss of Dutch ownership and control is limited, as is the impact on the vitality of the Dutch economy in the event that knowledge and (human) capital are moved abroad. Similar considerations apply to the scenario that looks at a foreign takeover of an innovative battery manufacturer.

This limited effect on the impact indicators does not necessarily mean that this type of threats lacks relevance in relation to a long-term strategy for Dutch (economic) security. Over the longer term, a continued outflow of high-value economic activity to other countries by way of foreign takeovers may be harmful to the vitality of the Dutch economy. This is, however, not set in stone since assessing potential long-term damage to the vitality of the economy is complex. The outflow of knowledge to other countries or the future development of dependencies may create the necessary conditions for events that can in fact harm our national security, for instance because those conditions permit a foreign actor to build up a position of political, economic or strategic military power. However, the effect

of this type of outflow of knowledge is uncertain and takes place over a long period of time, which makes both its impact and likelihood difficult to estimate.

A further point of attention with regard to economic risks is that the economy often acts like an endogenous system. Under pressure of economic stimuli, actors often pursue efficient outcomes within the context of policy frameworks. Resulting, unintended consequences may contribute to the build-up of risks within the financial system, mounting pressure on the multilateral system for rule-based international trade, the development of dependencies and other facilitation of the strategic position of foreign actors. The emphasis here is on the unintentional aspect, in the sense that costs or risks gradually develop alongside the original policy aim of creating benefits. Transactions that are efficient in economic terms take place because the private benefits exceed the costs. However, these decisions typically do not take account of external effects, such as risks to national security. The reason for this is that although each transaction has no or little impact on national security in itself, a tangible security risk may yet arise as the cumulative effect of a large number of transactions. This means that so-called no-regret options in policy are likely few and far between. In respect of dependencies for example, each dependency will be beneficial in some ways and disadvantageous in other ways. Indeed, in global value chains 'dependency' is the flip side of the benefit of efficiency.

9. Cyber threats

The cyber threats theme considers the impact and likelihood of five scenarios. There are close links between this theme and a number of scenarios from other themes, including the scenario on a ransomware attack on a telecommunications provider (threats to critical infrastructure) and the scenario dealing with cyber espionage targeted at public authorities (foreign subversion of the democratic constitutional system). The matrix below shows all these scenarios in a comparative perspective.

Figure 9 Risk matrix – cyber threats

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious				• Attack on a cloud service provider	
Serious	• Ransomware attack on tele-communications provider				
Substantial		• ICS cyber attack - chemical industry • Ransomware attack in the healthcare sector		• Cyber espionage targeted at public authorities • Misconfiguration at a major internet service provider	• Collateral damage
Limited					

The estimated likelihood varies widely across the scenarios whilst, on the whole, the associated impact remains relatively limited. In this regard, it is important to emphasise that the impact assessments are affected by the fact that it is often extremely difficult to predict the consequences of a disruption to digital systems, networks and services. The 2020 ANV National Security Horizon Scan has previously concluded that, as a result of the interconnectedness and digitisation of society, 'we cannot fully assess the impact of a digital interruption. Data sources and information systems are connected in all sectors of society, but insight into the possible cascade

effects of an outage or into the new avenues of attack these connections create is often lacking' (ANV, 2020). Matters are complicated further still by the ever-changing nature of the digital infrastructure (the complex interaction of IT networks and information systems). This in turn creates further, unexpected dependencies and effects. The latent threats that may arise from technological developments such as AI (advanced AI-driven cyber-attacks) and quantum computing (vulnerabilities in cryptography that undermine the security of protocols and sensitive data as well as additional computational power for malicious parties to carry out automated attacks) illustrate that these dynamics are unlikely to decrease in future.

Another cause of the relatively low impact scores appears to be that the social impact of disruptions are often limited in duration. The importance of digital systems results in a (commercial) motive for providers to resolve issues quickly. In other cases, social impact can be mitigated over time through alternatives or back-up systems while actual recovery efforts are still ongoing. Lastly, the decentralised architecture of the internet and internet services means that many disruptions remain confined to a specific group of users or services. In other words, the effects remain relatively concentrated, even though users or services may be widely (globally) distributed.

Cyber threats give rise to a wide range of effects that touch upon all national security interests and associated impact criteria. This is quite logical since the theme addresses a large variety types of threats which in turn affect a broad spectrum of security interests. A consequence of the wide reach of this theme and its threat categories is that it is difficult to draw general conclusions with regard to the extent and nature of the impact of the underlying phenomena in relation to specific security interests and criteria.

This assessment re-confirms that the digitisation of society (and the economy) not only creates new opportunities and vulnerabilities but that is also a topic that is gaining in strategic, (geo)political importance. The dominant position of major tech companies and the various ways in which states assert themselves in the digital domain create tension between different interests in and views of the digital domain, for instance in relation to the pursuit of digital sovereignty or autonomy by countries and the effects these efforts have on technical developments and innovations. In addition to this, there are developments that put pressure on the governance and principles of the internet and the digital domain, which may in the longer term jeopardise the Dutch interests of an open and digital economy.

10. Threats to critical infrastructure

Critical infrastructure is closely linked to many different threats to national security. The processes that make up the critical infrastructure of the Netherlands are crucial, because any interruption or outage of these processes will quickly result in societal disruption. It therefore follows that the impact of a large number of different threats in part stems from an associated disruption of critical infrastructure. The scenarios discussed as part of this theme illustrate that these threats vary widely. The topics discussed range from terrorist and cyber-attacks as well as disruptive natural phenomena such as floods and wildfires, to technical or human failures and space weather. The impact on critical infrastructure is also addressed in a great number of other threat themes (including climate and natural disasters, cyber threats, foreign subversion and violation of the democratic constitutional system, and economic threats). The figure below contains the risk matrix for the threats to critical infrastructure theme.

Figure 10 Risk matrix – threats to critical infrastructure

	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely
Catastrophic					
Very serious		• Chain effects of a power outage	• River flood		
Serious	• Ransomware attack on tele-communications provider			• Nationwide blackout	• Wildfires
Substantial					
Limited					

The analysis re-affirms that our society is heavily dependent on vital processes and that this is particularly true for vital processes in the energy and telecommunications sectors, in light of the large degree to which society depends on these industries. As is the case for virtually all parts of society, critical infrastructure also increasingly relies on digital systems. At the same time, it is important to realise that these dependencies are dynamic, not static in nature. The complexity of systems and dependencies between systems and processes continue to increase, making it difficult to accurately assess the impact of the events described in the scenarios, given that there are many hidden interdependencies within and between processes. The changeable nature of the use and the continual technological development and innovation of systems and infrastructure also make it challenging to fully keep track of these dependencies.

In the longer term, shortages in the labour market and especially a lack of trained technical specialists, for instance in the area of cybersecurity or with regard to the knowledge and expertise that is required to shape the energy transition, may result in insufficient capacity to maintain critical infrastructure resilience. These shortages are therefore considered to be a latent threat.

A review of the threats with regard to critical infrastructure in the next five years highlights that both state actors and cyber criminals are becoming an ever larger threat to the continuity of vital processes. The key societal function of vital processes makes them an attractive target for malicious actors. It is for this reason that safeguarding the continuity of critical infrastructure is incorporated more and more often in discussions in relation to strategic autonomy and economic security.

At present, the likelihood of deliberate attacks on critical Dutch infrastructure as analysed in this assessment is considered to be relatively low. This can be attributed in part to the preventative and mitigating measures put in place by the providers of vital processes and in part to the capacity and motivation actors would require to carry out such an attack in a targeted and purposeful manner.

When looking at non-intentional threats, the predominant threats to critical infrastructure stem from the effects of climate change and the energy transition. These will become likely and gain in impact in the years ahead. Climate change will give rise to an increase in extreme weather conditions such as extreme rainfall, floods and drought. The likelihood of a disruption to critical infrastructure as a result of natural phenomena such as these will therefore also increase.

Combined with geopolitical developments, the energy transition will encourage efforts regarding further electrification and also bring about changes in the manner in which electricity is generated and distributed. This may cause unexpected effects especially in the transition phase, when there are ongoing changes in infrastructure development.

A final key development is digitisation, which will translate to a continual evolution of the digital infrastructure and dynamic changes in the connections and dependencies between systems. Those changes are not limited to the infrastructure itself but also affect the way infrastructure is used (and therefore society's reliance on it). Due to the COVID-19 pandemic for example, there has been a huge increase in working from home, which has significantly increased the importance of internet access for households and resulted in changes in data flows. The ramifications of these dynamics are that the direct impact and chain effects of an interruption or failure of a vital process are difficult to estimate. It is therefore key that preparations for this type events always allow for the manifestation of unexpected effects.

11. Risks in the Caribbean part of the Kingdom of the Netherlands

As stated, a separate risk assessment was carried out to gain an understanding of the threats that could manifest themselves in the Caribbean part of the Netherlands. The main outcomes of this assessment are presented in this chapter.

Impact on national security

According to the assessment, a number of risks within the climate and natural disasters and international and military threats themes can have a major impact on national security. With regards to natural disasters, hurricanes were found to be the greatest risk (both in terms of likelihood and impact). As was illustrated by hurricane Irma (2017), a hurricane will impact all facets of society on an affected island, primarily disrupting daily life and causing significant economic losses. The hurricane scenario is elaborated in greater detail as part of the climate and natural disasters theme.

The international and military threats theme includes a closer examination of the current social and political situation in Venezuela and a potential escalation thereof. A scenario covering this topic has been developed within the respective threat theme. An escalation as described in the scenario may lead to an increased flow of refugees to the Caribbean part of the Netherlands.

Either scenario will have a major impact. The other themes analysed also point to potential major consequences for the affected country or island if a threat were to materialise. A great number of the themes (including major accidents, terrorism and civil disturbances) identify potential consequences for tourism, the economy and daily life on the islands, especially if infrastructure including transport routes to and from the islands is affected. For a number of other threats (e.g. organised crime), possible consequences include a violation of social and political stability (undermining of the democratic constitutional system).

Local impact and limited capacity

A further observation is that although the impact on national security in accordance with the applied methodology may at times be less relevant to the Kingdom as whole, the local impact may nevertheless be considerable given the small size of the islands. An example of this would be a natural disaster or infectious disease that results in large numbers of individuals requiring medical attention. If these individuals number a few dozen, the applied methodology will not qualify this as a major impact. This is different from the perspective of the island, however, given the limited (medical) capacity for emergency response. The same applies to the reception of large groups of people, for example after a natural disaster in a neighbouring country or an accident involving a cruise ship. Demand will rapidly exceed available reception capacity.

Dependency and vulnerability

A final and related conclusion is the dependency on the outside world as well as the vulnerability of the Caribbean part of the Netherlands. Firstly, its dependency is a given due to the fact that the islands rely on sea and air transport to receive supplies of food and goods, which makes their harbours and airport critical facilities. If these are unavailable or unusable, the consequences will be considerable.

Secondly, a large part of the economy of the Caribbean region depends on tourism. The assessment identifies various threats that can negatively impact on the number of tourist visiting the islands. This dependency therefore also entails a vulnerability, as aptly illustrated by the coronavirus pandemic.

Lastly, the Caribbean part of the Kingdom (in much the same way as the European part of the Netherlands) is heavily dependent on its (critical) infrastructure. Disruptions can have a major impact on the islands, in particular if multiple types of infrastructure are hit at the same time. On top of this, local infrastructure is vulnerable to natural disasters and, as highlighted during the assessment, to cyber threats.

SECTION II: Overall results of the National Risk Assessment

Section II of this report discusses the results of the National Risk Assessment as a whole, alongside a number of connecting links between the various threat themes, a number of overarching topics identified in the assessment and the wider national security landscape.

12. Overall results: risk matrix

As part of the National Risk Assessment, more than 60 scenarios were analysed in terms of their likelihood and impact on national security. The findings of these analyses and the identification of relevant developments, connecting links and overarching insights constitute the key outcomes of the assessment. This chapter discusses the main outcomes of the risk assessment.

12.1 Results of the risk assessment

All the scenarios included in the NRA were developed and assessed using the same methodology. As a result, the NRA makes it possible to put the various threats to Dutch society in a comparative perspective. The insights derived from this can help to inform the prioritisation of threats in policy instruments such as the National Security Strategy. In order to facilitate this comparison, the results are presented in a risk matrix (figure 11).

This matrix is an expanded version of the matrices from the previous, theme-based chapters, which includes all of the 60+ scenarios that were elaborated. The vertical axis reflects the accumulative impact on national security for a particular scenario. This overall impact was calculated based on the impact ratings of a scenario for the six national security interests (see the Annex for an overview of applied the methodology) and is subdivided into six classes ranging from 'limited' to 'catastrophic'. The horizontal axis indicates the likelihood of a scenario. Likelihood has been also subdivided and features five classes ranging from 'very unlikely' to 'very likely'.

Figure 11 Overall risk matrix

Catastrophic		• Flooding from the sea	• Pandemic caused by a virus transmissible from human to human		
Very serious	• IS seizes power in Morocco • Deployment of nuclear weapons in the Iran and Saudi Arabia conflict • Induced earthquake	• Chain effects of a power outage • Reunification of China and Taiwan • Temporary occupation of an EU Member State	• River flood • Flu pandemic • Collapse of the Venezuelan state • Disintegration of NATO • Systemic actor in the finance sector facing great difficulty	• Hurricane • Heat/drought • Import of fossil energy • Attack on a cloud service provider	
Serious	• Borssele nuclear plant • Train disaster with flash fire • Ransomware attack on telecommunications provider	• Trade war involving Europe • Multiple terrorist attacks • Disruption of payments • Foreign state acquiring a stake in a major telecommunications provider • Infiltration of public administration	• Snow storm • Crisis in the South China Sea • Rift within the EU • Criminal violence targeting media and government • Foreign interference diaspora communities • Assault on and hostage-taking in parliament	• Nationwide blackout • (Covert) influencing by China • Social polarisation surrounding conspiracy theories • Break-up of Bosnia-Herzegovina	• Hybrid operations by Russia – exploiting societal debate • Flu epidemic • Trade disruption due to production issues abroad • Wildfires
Substantial	• Radiation accident in Europe • Failure of an ammonia storage tank	• European debt crisis • ICS cyber attack - chemical industry • Ransomware attack in the healthcare sector • Terrorist attack using a bioweapon	• Disintegration of the OSCE • Attack on pride event • Naturally occurring earthquake • Escalation of violence by right-wing extremists • Anarcho-extremism • Foreign regulation of tech companies • Subversive enclaves	• Cyber espionage target at public authorities • Organised crime throughout the Netherlands • Outbreak of foot and mouth disease among cows • Traditional state espionage • Innovation of nuclear delivery systems • Adjustment of the value of financial assets • Misconfiguration at major ISP • Criminal interference in business • Anti-government extremism	• Collateral damage
Limited			• Outbreak of a zoonotic variant of avian flu	• Shortages of key raw materials • Acquisition of a company whose products include dual-use goods	• Lone actor • Foreign venture capital investment in start-ups
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**

When looking at the above matrix, it is important to bear a number of things in mind. The first is that the scenarios shown in the above diagram are primarily intended to illustrate a broader threat category. For example, the scenarios elaborated within the terrorism threat category provide an indication of the different ways in which this threat may manifest itself, but they are not intended to be exhaustive. A more comprehensive picture of the various threats and the associated scenarios included in the matrix can be found in the theme-based chapters of this report and the individual underlying thematic reports.

Second, it is not straightforward to indicate what types of risks constitute the greatest risk to our national security. Is this the threat that has the greatest impact, irrespective of its likelihood of occurrence? Or should the focus in fact be on threats that are very likely to materialise but simultaneously have a relatively limited impact? It might also be equally as necessary to examine the risks that have both a relatively high impact and a relatively high likelihood of occurrence.

The answer to this question depends heavily on one's perspective. The following sections therefore consider the outcomes of the risk matrix from multiple angles. The first of these is the likelihood of occurrence. Our focus then shifts to the impact on national security and we conclude the section by considering the combination of both impact and likelihood. This last perspective is not based on a mathematical approach (in the sense of 'risk equals likelihood x impact'). Instead, we take a qualitative approach based on the types of risks that have both a relatively high impact and a relatively high likelihood of occurrence.

12.2 From a likelihood perspective

The risk matrix allows us to draw a number of general conclusions in respect of likelihood. First of all, it is obvious that the scenarios are distributed across the different classes and that all points on the likelihood scale are represented. Most of the scenarios that are rated 'very unlikely' (left side of the matrix) relate to a physical risk (safety), for example major accidents such as an accident at a nuclear plant or chemical industry as well as natural disasters such as an induced earthquake. In addition to this there are intentional risks (security) that are rated 'unlikely', including a scenario dealing with the deployment of ransomware aimed at the telecommunications sector, as well as scenarios of a more international character (such as the deployment of nuclear weapons outside of the Kingdom of the Netherlands).

Scenarios with a high likelihood are shown on the righthand side of the matrix. A striking aspect is that this half of the matrix contains a high number of scenarios, among which are a relatively large amount of scenarios that have been given the highest likelihood rating ('very likely'). The scenarios once again link back to various themes and encompass both safety threats (wildfires, flu epidemic) as well as security threats (hybrid operations, disruption to international trade, collateral damage of cyber attacks).

A side-by-side comparison of high likelihood ratings with the risk matrix belonging to the 2016 NSP (ANV, 2016) reveals a clear difference and shows that the new assessment includes a relatively high number of scenarios that are rated as 'very likely'. This might lead to the conclusion that, in the opinion of the various experts involved, a number of threats have increased in likelihood over the past years. This statement however needs to be qualified as the high number of 'very likely' scenarios depends on various aspects, including the underlying choices and the number of scenarios elaborated (which is significantly higher than for 2016). Furthermore, the conclusion does not apply to all types of threats either. Even so, the likelihood can in any event be said to have increased for the threat of wildfires. In this regard, it was noted that the question is not so much if but when a fire will occur that affects national security.

A general conclusion from the above is that there is a relatively high probability that events impacting on national security will materialise in the years ahead. This insight can be used to zoom in more closely on resilience in relation to threats with a high likelihood.

12.3 From an impact perspective

For a large number of scenarios, their impact has been rated as 'serious' or higher. This means that all these scenarios will have a detrimental effect on national security. A closer look at the threats with the greatest impact (the ratings 'very serious' and 'catastrophic') reveals that the full range of threat themes is represented once more. The selection again includes safety and security threats from both internal and external sources.

The highest impact rating ('catastrophic') is anticipated in the event of physical threats – i.e. flooding from the sea and a new pandemic similar to COVID-19. Both scenarios will have a major, catastrophic impact on multiple national security interests. Both threats were also at the top of the list in terms of impact in previous risk assessments (ANV, 2016; 2019a). However, there are a number of differences compared to these previous assessments. A different scenario was selected in respect of flooding. Now it is not

the Randstad region that is flooded (Dyke Ring 14) but Flevoland and part of the Northern Netherlands. Such a flood still has a catastrophic impact, but the likelihood rating has moved up a point on the scale ('unlikely'). The pandemic scenario was based on the COVID-19 pandemic, except that the elaborated scenario is somewhat more serious still, for example concerning the availability of vaccines. This variant has a greater overall impact ('catastrophic') than the flu pandemic scenario ('very serious') and has been rated as 'somewhat likely'.

The extent to which society is prepared for the various threats that have a large impact on national security can be explored in greater detail in a resilience assessment. In this context, more detailed insights into the nature of the impact (the specific national security interests or underlying criteria affected) can help to focus resilience and crisis management initiatives. The information provided at a scenario level (incorporated in the thematic reports) and the summary overviews in this assessment can be used for this purpose.

12.4 Impact and likelihood combined

A review of the threats that have both a relatively high impact and a relatively high likelihood rating puts the focus on scenarios in the top right of the risk matrix. The first observation is that the top-most cells on the right are clear of any scenarios. The other dark blue cells contain the following scenarios:

- Heat/drought;
- Hurricane;
- Wildfires;
- Import of fossil-based energy;
- Trade disruption due to production issues abroad;
- Attack on a cloud service provider;
- Hybrid operations by Russia;
- Flu epidemic;
- Pandemic caused by a respiratory virus transmissible from human to human.

This list does not constitute a ranking, instead scenarios are grouped by threat theme.

The heat/drought and wildfires scenarios belong to the climate and natural disasters threat theme, and also have a logical connection to each other in terms of likelihood. Climate change is a key driver of the increased likelihood of prolonged periods of heat and drought, which bring with them an increased risk of wildfires. This illustrates that it in terms of resilience it is important to address both specific risks such as wildfires, heat and drought as well as to continue to put climate change on the agenda. The next chapter discusses this in greater detail.

The Hurricane scenario represents one of the greatest risks to the Caribbean part of the Netherlands and is based on hurricane Irma. This is yet another topic where climate change is an important factor, as it will cause future hurricanes to become more powerful.

The two scenarios relating to fossil-based energy and trade disruption due to production issues abroad form part of the economic threats theme. The fossil energy imports scenario covers a dependency on foreign suppliers and the possibility of surges in the price of products such as oil and gas, the consequences of which can include 'energy poverty'. A trade disruption due to production issues abroad arises because shortages will prompt countries to supply their own needs first. This could cause significant damage to our open economy. These scenarios highlight the risks of dependency, which could materialise as soon as there is a threat of shortages or if tensions arise between the actors involved.

The attack on a cloud service provider scenario is part of the internet disruption category within the cyber threats theme. What is extraordinary about this scenario is that it results in maximum harm to the integrity of the digital infrastructure but barely has any other effects. The scenario also exemplifies that it is difficult to assess which vital processes might be disrupted by events such as a cyber attack, highlighting that there is a certain level of unpredictability with regard to the consequences.

In the hybrid operations scenario, Russia fuels an existing societal debate with the aim of heightening tensions within society. The scenario is part of the foreign subversion of the democratic constitutional system theme. In the scenario, social discussions with regard to refugees and COVID-19 are purposefully stirred up with the help of deepfakes and other tools, while international tensions are on the rise as a result of migrant pushbacks and displays of military power towards NATO by Russia.

The final two scenarios deal with both an epidemic as well as pandemic and belong to the infectious diseases theme. The flu epidemic scenario is one scenario that occurs regularly and the pandemic scenario is based on COVID-19. In addition to large numbers of fatalities and sick people (causing severe pressure on the healthcare sector), the scenarios can also have a severe impact on the economy and society as a whole (depending on the circumstances and the measures taken).

Applying the combined perspectives of impact and likelihood, can help to prioritise risks and more closely reflect on resilience and crisis management in relation to the relevant themes. It is however important to avoid fixating on the nine scenarios listed above, as the scenarios

contained in the somewhat lighter cells of the diagram also carry a relatively high risk when viewed from the combined perspective of impact and likelihood. These bring international threats linked to China (influencing), NATO (disintegration), Europa (Bosnia) and Venezuela (with a direct impact on the Caribbean part of the Netherlands) to the fore. The international context is turbulent and mounting geopolitical tensions threaten our national security.

Other threats relate to the supply of electricity (black-out), social polarisation (conspiracy theories), a banking crisis and the flooding of a river (as happened recently in Limburg). This list shows that the third perspective (impact and likelihood combined) also highlights a broad spectrum of threat types that should be taken into account. The impact of the various threats again varies widely. Whereas a banking crisis would predominantly affect the economy, social polarisation would primarily undermine social and political stability. The consequences in case of a flood are distributed across various criteria (territory affected, casualties, costs, disruption of daily life), whereas an interruption of the power supply would lead to direct effects (e.g. on daily life) as well as chain effects, due to our high dependency on electricity.

This illustrates that both the type of threat and the impact on society can vary. This can be factored into resilience assessments and the strengthening of the crisis response.

12.5 Connecting links and interdependencies

The various connecting links between threat themes are another aspect that should be taken into account in a resilience assessment. An example is that climate and natural disasters as well as cyber threats can both potentially have a severe impact on the functioning of infrastructure that is critical to society, with either of these threat types capable of disrupting critical infrastructure. Other factors in play are the connecting links between different vital processes and the dependency on digital systems. Given that both society and a large number of vital processes are dependent on electrical supply and telecommunication services, disruptions can result in chain effects while the various dependencies also make it challenging to assess precisely what effects might occur. This would require in-depth analyses.

Connecting links and dependencies are also found in relation to other themes. International and military threats could, for example, have an impact on threats included in the economic threats theme. As set out in this theme, increasing tensions between great powers could affect economic dependencies.

The connecting links and interdependencies highlighted here do not exist in isolation and reveal that issues are complex and subject to a certain level of unpredictability. For this reason, Chapter 14 considers national security as a complex system in order to complement the review of risks on a theme-by-theme basis.

13. Overarching topics

The previous chapter examined the results outlined in the risk matrix from three perspectives. It is useful to complement this by reflecting on a number of topics that were mentioned in relation to multiple themes. This chapter discusses four overarching topics: hybrid threats, climate change, the energy transition and tensions in society.

13.1 Hybrid threats

Hybrid threats are often part of a long-term campaign. Although individual hybrid activities (such as cyber attacks) can already undermine national security in and of themselves, it is necessary to keep sight of the bigger picture in light of the fact that individual activities combined can have a bigger effect than the sum of their parts. The discussion regarding this topic in chapter 6 already noted that it is crucial to place specific threats in a holistic perspective and not lose sight of the overall picture. This section will illustrate this in greater detail with the help of an example.

Various themes within this National Risk Assessment address scenarios that could feature as part of a hybrid campaign. It is certainly useful to explore threats such as economic espionage, cyber attacks, misinformation campaigns and military incursions but it is in fact essential that those threats are also considered in conjunction with one another as they could also be part of a hybrid campaign. The example that follows illustrates how hybrid threats reach beyond the limits of individual threat themes.

The starting point of this example scenario is that Russia is seeking to prevent Finland's accession to NATO in a variety of ways. Russia attempts to influence Finland as well as other NATO countries, including the Netherlands. Russia initiates several 'influencing campaigns', the aim of which is to cause Dutch (and European) citizens to adopt a predominantly negative opinion on Finland's accession to NATO. As talks between Finland and NATO on accession become ever more specific and tensions between Russia and Finland rise, Russia seeks to divert the attention of individual NATO countries (including the Netherlands) away from the potential accession of Finland to NATO. The aim is to push Finland's accession down the agenda of NATO countries. To this end, Russia attempts to increase internal tensions in several countries by purposefully fuelling societal debate (in the Netherlands) and mounting a large-scale cyber attack. This is done in an effort to distract European countries from the tensions between Finland and Russia in a way that ultimately allows Russia free reign for long enough to occupy a Finnish airbase. This translates to a number of scenarios that appear to be separate from one another but are in fact part of a larger Russian campaign. This approach can be represented as an 'escalation ladder', with Russia moving up the escalation levels as time progresses. See figure 12 for a visualisation of the escalation ladder with the three scenarios that make up Russia's hybrid operation, which ultimately results in an escalation in Finland (breaching the threshold of armed conflict).

Figure 12 Escalation ladder with the three hybrid Russia scenarios, covering three different threat themes

In the midst of the tensions between Russia and Finland, with Russia using various channels in an attempt to turn European citizens against Finland's accession to NATO, the societal debate in relation to refugees is stirred up once again. In this scenario, Russia facilitates a large flow of refugees towards the EU with extensive media reports on pushbacks at the southern and eastern borders of Europe. The key narrative that Russia wants to establish in the minds of citizens in EU and NATO countries, namely that the EU is an incompetent and hypocritical institution, is not in any way justified. It is also noted that there is a gradual build-up of troops at the western borders of Russia. There is disagreement within the EU whether this build-up of troops requires a military response by the EU (since Finland has not yet joined NATO), with some Member States even calling for Article 42(7) to be invoked. The main effect contemplated by Russia in this scenario is to sow division within the EU (and thus among a large number of NATO countries) and influence decision-making processes. However, it is questionable to what extent this division would have a structural impact on decision-making by the EU (and NATO). The build-up of troops ultimately does not result in military action by Russia on EU/NATO territory and the increased tensions appear to fizzle out.

In the next step on the escalation ladder, Russia mounts a cyber attack in the sample scenario, aimed at shifting the attention of the Netherlands away from the international arena to domestic issues arising as a result of the cyber attack. To this end, Russia might use a criminal organisation as its proxy. This would allow Russia to deny any involvement ('plausible deniability') and possibly evade attribution.[14] An attack on a vital process could result in a severe impact (on society) but this may equally be so in the event of an attack on a non-essential sector (e.g. an attack on a chemical company) as this may lead to fatalities and casualties.[15] A hybrid actor will not risk a 'direct' attack with human losses at a lower escalation level, since this might cause a latent hybrid threat to directly escalate to open military conflict. To a hybrid actor like Russia, it is more 'interesting' to disrupt a vital process such as the supply of power. The two scenarios in the threats to critical infrastructure theme that deal with a loss of power indicate a potentially severe impact,[16] without the hybrid actor necessarily suffering any effect itself. Although there is no digital element in the power loss scenarios within the disruption to critical infrastructure theme, the impact will largely be the same (irrespective of the cause). A disruption to power supplies throughout Europe may also have an impact in light of the interconnectedness of the the European power grid.

[14] For an example, see the 'Ransomware attack on a telecommunications provider' scenario in the intentional threats against vital processes category of the threats to critical infrastructure theme or the 'Ransomware attack targeting a hospitals' scenario in the cybercrime category of the cyber threats theme.

[15] For an example, see the 'ICS cyber attack - chemical industry' scenario in the disruption to cyber-physical systems category of the cyber threats theme.

[16] See the threat category 'intentional threats against critical infrastructure and disruption of vital processes as a result of a technical or human failure' of the threats to critical infrastructure theme.

Russia seizes the moment that the Netherlands (and perhaps other Member States) are distracted by the cyber attack to launch its attack against Finland. When the first signs of this attack are flagged, the EU Member States adopt a wait-and-see attitude ('it'll probably prove to be nothing again'), giving Russia even greater room for manoeuvre in the first phase of the attack. Given that the build-up of troops in an earlier phase of the scenario of mounting tensions outlined in the scenario had ultimately led to nowhere, it is now assumed that the military threat from Russia is again relatively limited. Therefore, in order not to escalate matters further, the EU initially refrains from taking action, thereby creating the opportunity for Russia to occupy the Finnish airbase.

13.2 Climate change

Greenhouse gases are causing the climate to change – the planet is warming up. According to the Royal Netherlands Meteorological Institute (KNMI), climate change is happening at a faster pace than previously thought and the Netherlands is increasingly seeing the effects of this. Climate change is a key driver in the exacerbation of various threats, not only those within the cimate and natural disasters theme but also those related to economic threats and other themes.

Climate change increases the probability of extreme weather events, which may already pose a threat to national security in themselves but can also trigger other threats. For example, extreme rainfall can result in flooding and extreme heat and drought may lead to uncontrollable wildfires. Extreme drought, excess precipitation and flooding can in turn cause disruption to vital infrastructure such as the power grid, drinking water system and telecommunication networks. Extreme weather may also cause water levels to rise or fall too much, which can result in the disruption of trade routes and therefore threaten the logistical hub function of the Netherlands.

Threats may also be aggravated by ever higher temperatures. These cause sea levels to rise, increasing the risk of floods. Higher temperatures are also expected to increase the incidence of infectious diseases in the Netherlands that were previously not present. They may furthermore lead to a global decrease in the quality, safety and availability (scarcity) of food, resulting in higher food prices and an increase in migratory flows.

Climate change issues may also be a source of social polarisation or create an anti-government sentiment, for example in relation to decisions such as the installation of wind turbines but also the arrival of large energy consumers such as data centres. These may give rise to opposition and tensions between different interests. Left-wing views may also result in radicalisation around this topic, for example based on the view that too little is being done to limit climate change. Climate change could also result in tensions at an international level, for instance in the event that no international consensus is reached with regard to the measures that are needed or because debate on climate change is exploited to fuel tensions between countries and advance foreign political agendas. Climate change also results in economic risks arising from more structural damage. Underinvestment in mitigation and prevention (climate adaptation) could constitute grounds for international credit rating agencies to downgrade the credit rating of the Netherlands. Options to insure damages will also come under pressure.

Climate change, as a driver that intensifies numerous threats, is a latent threat that renders our national security increasingly vulnerable. It means that harm to national security as a result of climate-related threats is an increasingly realistic prospect and that the potential impact rises. Add to this the fact that the effects and risks of climate change are becoming ever more complex and difficult to manage. The IPCC report published at the end of February 2022 warns of ripple effects as a result of adverse climate effects triggering and mutually enhancing other climate impacts. An example would be a heat wave-induced drought that is followed by loss of biodiversity, increased food prices and hunger, which increase the vulnerability of humans and nature to new extreme weather events and prompt new migratory flows. Multiple climate risks will arise at the same time and various climatic and non-climatic risks will begin to interact with one another.

13.3 Energy transition

The energy transition is a profound change that includes many aspects relevant to national security. Examples include the use of technologies and substances that entail risks, such as hydrogen. The ANV mapped out these risks in a previous study (ANV, 2019b). This study concluded, inter alia, that the use of hazardous substances for the energy transition poses risks to national security that are in essence similar to those that apply today, although explicit attention will need to be paid to aspects such as the use of hydrogen in the urban environment. It was also highlighted that (unexpected) obstacles can arise in the transition phase in particular, when old and new technologies exist side-by-side and are increasingly integrated with one another.

Relevant technologies include wind and nuclear power, with the possible development of new nuclear plants. The risks this entails have been mapped out in the major accidents

theme, which shows that the likelihood of an accident is extremely low. Independently of the risks a plant itself brings, the decision to open a new nuclear power plant could cause societal commotion. Concerning wind power, there are efforts to increase the number of offshore wind farms in the North Sea. More offshore wind farms will translate to an increased likelihood of shipping accidents involving these wind farms and attention is therefore given to ways in which they can be protected. In addition to the fact that accidents on the North Sea involving wind farms could affect energy supplies, intentional threats may arise. After all, wind farms form part of the critical infrastructure and as such could become the target of cyber attacks and sabotage.

Electrification is one of the pillars of the energy transition. Electricity will increasingly replace fossil fuels such as gas and oil, as demonstrated by electrically powered transportation. This will increase both reliance and pressure on the power grid which could result in capacity issues in some areas and increase the likelihood of disruption.

Reliability and continuity of supply are pertinent issues in light of our society's heavy reliance on the supply of electricity. Disruptions can severely affect national security (as is also evident from the two scenarios on the electricity supply that were elaborated as part of the threats to critical infrastructure theme). The energy transition brings technical aspects to the fore such as the balancing of supply and demand (from different sources at different times) and the available grid capacity, especially given the drive towards electrification. Technologies such as smart grids and AI will be able to play a key role in control and optimisation, which implies a need to consider potential vulnerabilities with regard to cyber attacks.

A final group of issues to consider relate to dependency, costs and acceptance. These can affect economic security, as well as other interests. It is wise to consider issues of dependency on sources, materials, technology and (foreign) actors. A topical example in this regard is the dependency on Russian gas. The affordability and costs of the energy transition, along with related questions on the distribution of these costs, affect the feasibility of and support for the energy transition in society. Discussions on the siting of wind turbines illustrate that support is a key issue and that the energy transition can also fuel tensions in society that might subsequently lead to social polarisation and extremism. A point for attention is also the feasibility of the energy transition itself, in terms of the adequate availability of materials and workers with the required technical knowledge.

In summary, the above means that the energy transition raises a great many issues that have a bearing on national security and which need to be addressed in a holistic manner. The phase in which choices are made with regard to this transition is in fact the ideal time to implement the principle of *'safety and security by design'*.

13.4 Tensions in society

The emergence of social tensions is not exclusively linked to threats that fall under the social polarisation, extremism and terrorism theme. Tensions may arise in relation to virtually all threats considered in the NRA. These can manifest in all manner of ways, such as exclusion, protests, threats and even physical violence in the form of assaults or vandalism. Manifestations may be aimed at (groups of) citizens as well as public authorities, and have the potential to severely undermine their functioning and the proper functioning of society in a wider sense. It is therefore key that the possible emergence of such tensions is taken into account. The analyses carried out for the purpose of the NRA show that there is a broad spectrum of threats that may result in societal tensions. This spectrum also includes threat types that might not initially come to mind in this regard.

On the one hand there are numerous intentional threats where the deliberate sowing of fear, tension and division is an instrument by which state or extremist actors seek to achieve their goals. Examples include the dissemination of misinformation in the context of hybrid operations, the perpetration of a terrorist attack or the purposeful sowing of fear and division within diaspora communities or society at large.

On the other hand there are threats where a rise in societal tensions is not the outcome of a deliberate act. An event such as a flood, an earthquake or a major accident involving chemicals can cause a lot of anger about how such a disaster could have happened and who should be held accountable for the consequences. In these cases, tensions are more likely to manifest themselves in the relations between authorities and citizens for example, rather than between different groups of citizens. Organised crime is another topic that has the potential to put relations between the authorities and citizens on edge, especially if there is low confidence in the government's ability to effectively fight crime. The same applies in the case of large-scale cybercrime, such as ransomware attacks targeting hospitals or utilities.

Domestic tensions may also arise as a result of threats that have their origins outside of the Kingdom of the Netherlands. International conflicts and instability can translate into antagonism between or within different diaspora communities in the Netherlands, stigmatisation of groups of citizens with a particular nationality and higher numbers of refugees, as well as differences of opinion on how to handle these. Disruptions of international trade or energy supplies like natural gas may give rise to shortages of or significant price increases for specific goods. If this causes people to suffer financial difficulties, this may once again result in social unrest and tension, particularly when the feeling takes hold that the burdens of the situation are distributed unevenly across the population or that government efforts to improve things are inadequate.

In an effort to better reflect the impact of social tension in the NRA, we have not only addressed this topic in the analysis of the above threats but also included social polarisation as a separate, independent threat category. This is in contrast to previously analyses carried out by the ANV, such as the 2016 National Security Profile and the 2019 National Risk Assessment. Social polarisation is a phenomenon that may occur in response to a wide range of topics and developments, such as the reception of asylum seekers, the handling of an outbreak of an infectious disease (such as the COVID-19 pandemic) and even geopolitical events like the war in Ukraine. The NRA highlights three developments that must be explicitly referenced in this regard – climate change, the energy transition and the dissemination of misinformation.

Our changing climate generates a wide range of complex social issues, varying from what our response should be to the increase in extreme weather events to the potential arrival of ever higher numbers of climate refugees and the question of how to distribute the burden and the benefits of climate adaptation within society. Each and every one of these issues is subject to fundamentally different views and has the potential to cause social polarisation, even more so when those views are continuously exaggerated and presented as opposites in the public debate. There is also a close link between climate change and the energy transition. Whereas some welcome the use of renewable energy sources such as wind turbines and solar panels and consider them indispensable, others have concerns regarding the construction of large-scale wind and solar farms and their impact on the landscape. The energy transition will also prompt renewed and increased discussion in relation to the use of nuclear energy.

In parallel with this, there is an increase in possibilities to fuel social polarisation and social tension by means of misinformation. It is expected that capabilities to produce convincing deepfakes will become increasingly accessible in the years ahead. The software that facilitates their production currently still requires a certain level of expertise but this barrier will soon disappear, meaning that even people without this knowledge will increasingly be able to create convincing deepfakes. This technology can be used to influence public debate and aggravate social polarisation.

14. Threat landscape for national security as a complex system

14.1 Introduction

Similar to the 2019 National risk Assessment (ANV, 2019), the analyses in the NRA shows once more that there are many **links** between the various threats to national security. There are specific phenomena that pose a threat to national security in and of themselves but which can also manifest as part of another phenomenon. A disruption to a vital process such as the supply of electricity could, for example, arise independently after a technical failure but also as a result of a natural disaster. In the same way, a chemical accident could stem from a failure or sabotage of digital systems. The issue of hybrid threats also demonstrates how different phenomena can be purposefully combined to exploit vulnerabilities in society.

Additionally, there are latent threats that do not have a direct major impact on national security but could certainly create considerable impact in the **long** term. These can either be long-term developments that gradually create problematic situations, or a set of relatively small-scale events that do not appear to have major relevance individually but the sum of which can have severe consequences for national security over the longer term. Commonly in the case of latent threats, there is often a tipping point which, once passed, means issues can only be tackled with great difficulty. In many cases, it is possible to ascertain in retrospect that an event occurred which proved irreversible and is the cause of major issues. Risks of this nature can build up slowly and under the radar. A slow build-up of risks may for example occur in relation to economic dependencies. Where business and public authorities 'naturally' select a specific production structure for business and/or economic reasons, there is a risk that a concentrated supply will 'automatically' create an unwanted dependency over time.

Each of the threat themes highlights specific examples of **latent threats**. Some of these are directly linked to a specific threat (e.g. the emergence of AI-driven cyber attacks) but many are also relevant to the development of the threat landscape in a range of themes, such as the overarching topics of climate change, the energy transition, the increase in social tensions, and hybrid threats. This re-affirms the interconnectedness of phenomena which, combined with the greater impact of the cumulative effect of phenomena over the longer term, adds a more complex dimension to the threat landscape for national security. This chapter will therefore look at national security as complex system and briefly discuss a number of characteristics of this complexity.

14.2 Characteristics of national security as a complex system

Digitisation, interconnectedness of networks and automation lead to increasingly complex technological systems that are of major importance to processes in society (including vital processes). This makes it difficult to predict the effects of disruptions or failures in advance. The **dynamic** nature of the systems means that dependencies between phenomena are not stable either. Connecting links and interdependencies change continuously as a result of changes in society, such as the energy transition and the speed at which technological innovations are implemented. The complexity of chains and systems makes it difficult to thoroughly examine a system or chain and really understand the impact of a single cog within them.

In this context, it is also important to bear in mind that Dutch society does not exist in isolation but is part of **an international, economic** system. Shifting relations and competing interests within this system have a major influence on our freedom in choosing how to protect Dutch national security interests.

An example of this is digitisation, which is key to the economy and the advancement of society but which also creates **dependencies** on large foreign tech companies and international supply chains. The same applies to (economic) dependencies on specific products or services. Supply or manufacturing shocks in a global value chain may have spill over effects that can lead to unexpected and unpredictable outcomes elsewhere.

Globalisation plays a crucial role from the point of view of international politics. The process of globalisation blurs the boundary between internal and external security at an ever faster pace, driven by technological and digital developments. Globalisation connects humans from all parts of the world to one another and even eliminates obstacles in the flow of goods and services between countries (supraterritoriality). In terms of national security, the nexus between internal and external security is characterised by the fact that it not only crosses borders in the strict sense (internal versus external), but also the traditional borders between different sectors, policy areas and domains (justice, defence, the economy, finance, industry, technology, policing, civil society, culture, ecology and politics) (Drent, Pronk & Meijnders, 2020).

A final factor in the increasing complexity of society is the **politicisation** of topics such as the climate, health and the economy. These topics give rise to political and social debates that increasingly emphasise the contrasts between different interests. The importance of security is also increasingly drawn into these debates (securitisation). This is borne out by social tensions regarding those topics, as well as in the policy-making in those areas, including the energy transition and strategic autonomy.

14.3 Dealing with complexity and unpredictability

The above characteristics are a varied and complex threat landscape. This generates a certain level of **unpredictability** with regard to the impact if one or more threats were to materialise. This does not only apply in the technical sense in light of the connecting links and interdependencies within and between (vital) processes, but also in relation to the economy and the international political arena given the dynamic nature, interdependencies and interconnectedness of a multitude of areas. Even in the case of specific (combinations of) scenarios where we are able to arrive at an accurate assessment of the possible consequences, some degree of uncertainty continues to exist due to the influence of related developments and adjacent events.

This complexity, along with the resulting unpredictability, requires a different approach to making preparations and building resilience. Latent threats, for example, require consideration to be given to detection and monitoring. It is also key to build adaptive capabilities that enable us to mount an adequate response to unexpected events.

From the perspective of public administration, national security issues should be treated as ***wicked problems***. The response to such problems requires the involvement of multiple actors, who must also coordinate their efforts in order to safeguard coherence and counteract overlap, duplication of efforts, gaps and opposition in the development and implementation of policies. Amongst other things, this requires administrative coordination to ensure cooperation and coherence between the various public authorities. The fact that many security matters have evolved into cross-sectoral issues means success in prevention, deterrence and control will also require a cross-sectoral approach. Measures will therefore need to be designed on a *whole-of-society* rather than a *whole-of-government* approach. In this regard, it is key to consider the various interests and social tensions surrounding the issues that have an impact on national security (and other matters). Different sections of society can have widely differing perceptions of safety, which may be influenced by interests other than security. This implies sensitivity is required in the response to threats.

SECTION III: Final conclusions

How can the outcomes of the National Risk Assessment be used to arrive at substantiated policy choices?

15. Final conclusions

This National Risk Assessment provides the opportunity to put a wide variety of threats that can potentially destabilise our society in a comparative perspective. The insights derived from this can help to inform the prioritisation of threats in instruments such as the National Security Strategy. In addition to this, the thematic reports provide insight into relevant trends, risks and latent threats specific to a theme. These insights can in turn be used to assess whether our society has sufficient capacity to withstand the threats in question or whether improvements are required, for example through the strengthening of crisis management. The thematic reports offer a wealth of information that can serve as a foundation for enhancing safety and security in the Kingdom of the Netherlands.

Given the scope of this risk assessment and the number of scenarios that were assessed, there could conceivably be some difficulty in determining how to proceed. That would be a pity, given that the risk assessment is specifically intended to support substantiated policy choices. The interpretation of the scenarios in the risk matrix (chapter 12) therefore describes a number of angles from which the matrix could be viewed. These angles could also prove useful in the follow-up process:

- In respect of threats that would have the largest impact on national security, it seems sensible to minimise the likelihood that these might materialise. In this context, the question naturally arises as to what possibilities are at our disposal to minimise that likelihood (or keep it as low as possible), and whether additional investments would be proportional to the security gains made.
- When determining priorities from a risk-oriented perspective, threats with a relatively *large impact and a high likelihood* can be used as a guide. Further analysis of the relevant threats can provide insight into whether risk reduction measures are best focused on the aspect of likelihood or impact.
- Examining the specific consequences of a particular threat makes it possible to produce a focused resilience analysis and use the results to strengthen crisis management. In relation to threats that could result in a high number of casualties for instance, this could mean checking how the required assistance would or could be made available. In this way, it becomes possible to establish a direct link between risk analyses and resilience assessments.
- If a threat has a high likelihood, it would seem sensible for society to make preparations and check whether it is sufficiently resilient in that regard. Examples are be wildfires, attacks by a lone actor and the collateral damage of a cyber attack.

This risk assessment offers the opportunity to directly examine into specific risks, but also reveals that there are a large number of connecting links and interdependencies between the various risks that must be taken into account. Consider, for example, the connecting links and interdependencies between vital processes and digitisation, and between economic and international developments. In addition to this, the assessment has brought a number of overarching topics to the fore where different developments intersect. These are: climate change, the energy transitions, tensions in society and hybrid threats. A holistic analysis of these overarching topics can be carried out from the perspective of resilience and crisis management.

The connecting links and interdependencies that have been identified create a certain level of unpredictability with regard to the consequences that will arise if a risk materialises. Since this requires a more holistic approach, the previous chapter outlines an approach that allows those issues to be treated as a complex system.

The NRA considers a large number of threats and their associated risks. Although it is true that some of these threats have not occurred in the Netherlands for some time or are considered unlikely or very unlikely to emerge in future, others have indeed already materialised. For others still, estimates are that they are likely to arise or arise again as challenges for our society in the years ahead. It is emphasised that the threat assessment presented in the NRA is not static but can evolve as a result of social, international, technological and other developments. It is key for our society to be aware of and keep up to date with the set of threats that could undermine our national security, for example by carrying out periodic analyses such those included in the NRA. This will provide tools for the creation of a resilient Kingdom of the Netherlands.

Afterword

The ANV is keenly aware that current international events, particularly the war in Ukraine, evolve at a tremendous pace. It is important to bear in mind that the scenarios presented in this main report and the underlying thematic reports were developed and assessed before the Russian invasion of Ukraine. In the risk assessment and the underlying reports, the ANV aims to strike an appropriate balance between scenarios that are representative of what the future may hold and scenarios that sufficiently echo current events. It is a fact, however, that as soon as the most recent events are included the assessment, the risk arises that these events will quickly become outdated. The ANV has therefore made efforts to develop scenarios that are as futureproof as.

This does not detract from the fact that the war in Ukraine does impact the assessment and more particularly the likelihood of several scenarios considered within the NRA. Among these are a number of scenarios from the international and military threats themes, such as the development of a rift within the European Union in respect of the policy choices (with regard to Russia), the disintegration of the OSCE (a scenario which is currently taking place as Russia has withdrawn from the OSCE) and the temporary occupation of an EU Member State (the applications by Finland and Sweden to join NATO will increase the risk of this scenario taking place). There is also a potential increase in likelihood for a number of threats considered as part of the economic threats theme, in particular those concerning strategic dependencies on commodities such as oil and gas.

In order to preserve the integrity of the methodology used within the risk assessment, it was decided not to amend or update the contents of the scenarios based on current events. This would have required the scenarios to be revalidated by experts and re-assessed in terms of impact and likelihood in new expert sessions. The ANV believes that the analyses are sufficiently robust to use the results for the purpose of resilience assessments and as input to the National Security Strategy.

References

National Network of Safety and Security Analysts (ANV). (2016). *Nationaal Veiligheidsprofiel 2016* (2016 National Security Profile). At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2019). *Geïntegreerde Risicoanalyse Nationale Veiligheid 2019* (2019 Integrated Risk Assessment National Security). At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2019). *Verkenning risico's van de energietransitie voor de nationale veiligheid* (Exploring the national security risks of the energy transition). At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2020). *Horizonscan Nationale Veiligheid 2020* (2020 National Security Horizon Scan. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022a). *Leidraad risicobeoordeling* (Risk Assessment Guidelines). At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022b). National Risk Assessment – Thematic report on infectious diseases. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022c). National Risk Assessment – Thematic report on climate and natural disasters. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022d). National Risk Assessment – Thematic report on threats to critical infrastructure. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022e). National Risk Assessment – Thematic report on cyber threats. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022f). National Risk Assessment – Thematic report on major accidents. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022g). National Risk Assessment – Thematic report on social polarisation, extremism and terrorism. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022h). National Risk Assessment – Thematic report on foreign subversion of the democratic constitutional system. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022i). National Risk Assessment – Thematic report on international and military threats. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022j). National Risk Assessment – Thematic report on economic threats. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

National Network of Safety and Security Analysts (ANV). (2022k). National Risk Assessment – Caribbean part of the Netherlands. At: *https://www.rivm.nl/onderwerpen/nationale-veiligheid*.

Drent, M., Pronk, D. en Meijnders, M. (2020) *Verbondenheid in veiligheid. De contouren van een onderzoeksagenda voor drie ministeries* (Security and cohesion – Contours of a research agenda for three Ministeries). Clingendael Report. The Hague, Clingendael Institute.

The references for the individual thematic chapters have been included in the associated thematic reports.

Annex 1. The National Network of Safety and Security Analysts

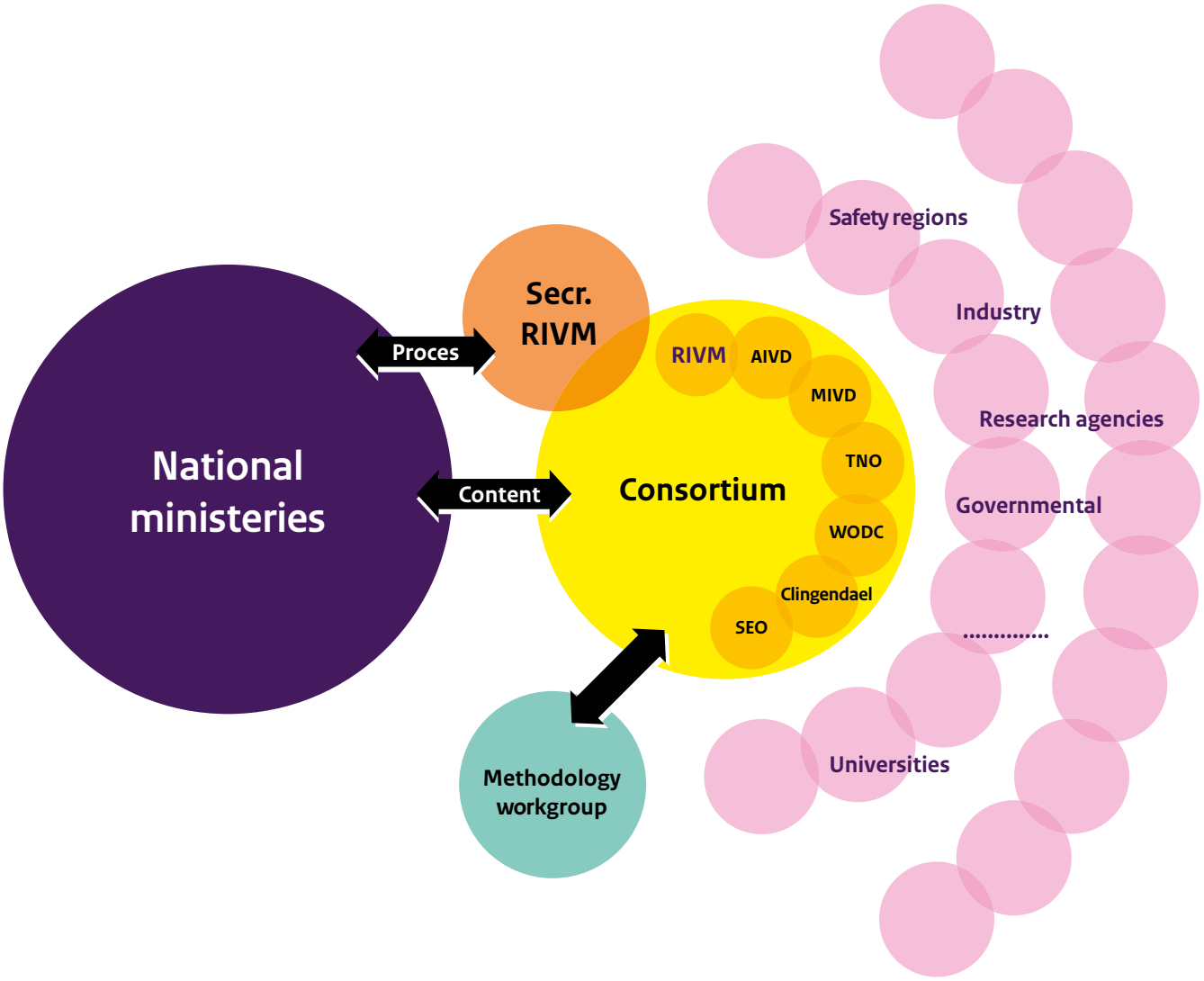
The National Network of Safety and Security Analysts (ANV) is a knowledge network that was established in 2010. At the request of the Ministry of Justice and Security, the network has since then prepared national risk assessments and other in-depth analysis studies in the area of national security on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

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 B1 Network structure of the ANV



Annex 2. Methodology

This Annex explains the way this risk assessment was carried out and also gives a broad outline of the applied methodology.

2.1 Risks and threats

This risk assessment provides an overview of threats that can disrupt the functioning of our society and their associated risks. Different definitions exist for both concepts (risks and threats) and we therefore briefly set out what each of these terms is understood to mean in the context of this risk assessment. A *threat* is 'a demonstrable development, event or phenomenon that may be detrimental to security or stability'. By contrast, a *risk* is understood to mean the interaction between 'impact' (the overall consequences of a specific threat) and 'likelihood' (the extent to which a threat is expected to materialise). Very briefly put, the assessment provides insight into threats in terms of risks.

This risk assessment does not evaluate resilience against the threats being reviewed.[17]

2.2 Scenarios

Scenarios are used in order to provide a better understanding on the risk associated with a particular threat. For each type of threat considered in the NRA, one or more scenarios (brief story lines or narratives) were developed and subsequently assessed in terms of their impact on national security and their likelihood of occurrence. In this way, the rather abstract threat posed by a phenomenon such as terrorism is described in a number of scenarios that for example look at a relatively small-scale attack by a lone actor and at a large-scale attack on multiple location using explosives and firearms.

The scenarios paint a concrete picture of a specific type of threat and the risk it entails. They illustrate this combination and demonstrate what possible consequences could arise. The scenario are not intended to provide a comprehensive view of all possible manifestations of a threat but serve as examples of a threat and its associated risks.

2.3 National security methodology

The ANV's assessment of the scenarios and their impact and likelihood is based on the national security methodology. This methodology is used to verify if and to what extent a specific event could harm the six national security interests. National security is at stake when one or more of the six national security interests are threatened to the extent that society is or could be disrupted (ANV, 2022a). Each of the six national security interests are expressed as one or more measurable impact criteria that help to define potential consequences. An overview of all the interest and criteria is given in the following table. A detailed explanation for each of the elements shown here can be found in the *Leidraad risicobeoordeling* (Risk Assessment Guidelines) compiled by the ANV (ANV, 2022a).

[17] The assessment implicitly uses current resilience levels as the starting point. In the event that experts have made comments with regard to resilience, these have been incorporated as additional information. However, a specific resilience assessment is out of scope for the NRA but could possibly form part of the follow-up process.

Table 2 Interests and impact criteria within the national security methodology

Interest	Impact criteria
1. Territorial security	1.1 Violation of the territorial integrity of the Kingdom of the Netherlands
	1.2 Violation of the international position of the Kingdom of the Netherlands
	1.3 Violation of digital infrastructure integrity
	1.4 Violation of the territorial integrity of allied states
2. Physical safety	2.1 Fatalities
	2.2 Seriously injured and chronically ill people
	2.3 A lack of basic needs (physical suffering)
3. Economic security	3.1 Costs
	3.2 Violation of the vitality of the Dutch economy
4. Ecological security	4.1 Long-term violation of the natural environment
5. Social and political stability	5.1 Disruption of daily life
	5.2 Violation of the democratic constitutional system
	5.3 Societal impact
6. International legal order and stability	6.1 Violation of state sovereignty, peaceful coexistence & peaceful conflict resolution (as codified in the UN charter)
	6.2 Violation of the functioning and legitimacy of or adherence to international treaties and norms on human rights
	6.3 Violation of a rule-based international financial-economic system
	6.4 Violation of the effectiveness and legitimacy of multilateral institutions and international regimes
	6.5 Instability of states bordering the Kingdom of the Netherlands and in direct vicinity of the European Union

In order to give a verdict on the precise extent of the consequences of a scenario, the impact is rated as 'not applicable', 'limited' (A), 'substantial' (B), 'serious' (C), 'very serious' (D), or 'catastrophic' (E) for each criterion. This classification is based on a logarithmic scale. For criterion 2.1 (fatalities) for example, this means that the rating 'limited' represents between 0 and 10 fatalities, 'significant' represents 10 to 100 fatalities, etc. Criterion 3.1 (costs) is based on a similar reasoning. Societal disruption is deemed to occur when one or more interests are affected and the consequences are rated as 'serious' (C) or higher.

Table 3 Example illustrating the different impact classes within the national security methodology

Impact class	Example criterion: Fatalities (2.1)	Example criterion: costs (3.1)
A. Limited	Less than 10	< 50 million euro
B. Substantial	10 to 100	< 500 million euro
C. Serious	100 to 1000	< 5 billion euro
D. Very serious	1000 to 10,000	< 50 billion euro
E. Catastrophic	More than 10,000	> 50 billion euro

Unlike the above criteria 2.1 and 3.1, some criteria cannot be expressed as an absolute number. An example of this is criterion 5.2 – violation of the democratic constitutional system. In this context, the ultimate rating is calculated by assessing if, to what extent and for what length of time various elements of the democratic constitutional system will be negatively affected. These elements are:

- The functioning of political representation;
- The functioning of public administration and the officials working in public administration;
- The functioning of the public order and security system;
- The functioning of an independent judiciary;
- Rights and freedoms enshrined in the constitution and legislation (freedom of religion, freedom of expression, freedom of association, voting rights, etc.).

The greater the harm, the higher the number of aspects that are impacted and the longer the duration, the higher the impact rating will be.

The methodology takes into account the impact of an event as well as the likelihood that the event will occur. Likelihood is determined based on the probability that an event will occur within five years from the time at which the analysis is carried out (first quarter of 2022). Depending on the type of event this probability is expressed in qualitative or quantitative terms, using a five-point scale that runs from 'very unlikely' to 'very likely'. The impact and likelihood of a scenario is established on the basis of *expert judgement*.

Table 4 Likelihood estimates within the national security methodology

Likelihood classes	Qualitative description of the threat	Quantitative approach (% over a 5-year term)
A. Very unlikely	Lack of concrete indications; scenario is not considered plausible	< 0.05%
B. Unlikely	Lack of concrete indications; scenario is considered somewhat plausible	0.05 - 0.5%
C. Somewhat likely	Lack of concrete indications; however, scenario is considered plausible	0.5 – 5%
D. Likely	Scenario is considered highly plausible; some indication that the scenario will indeed materialise	5 – 50%
E. Very likely	Concrete indications that the scenario could become reality	50 – 100%

2.4 Building blocks, latent threats and wild cards

'Building blocks', an overview of aspects and actors relevant to a specific threat category, were used to assist in the identification and development of the scenarios. Combining aspects and actors makes it possible to create multiple cases or scenarios. Different combinations will evidently result in different scenarios with variable outcomes. The building blocks help to clarify, at a single glance, what elements have or have not been included in a scenario and provide the reference framework for the eventual storyline contained in the scenario.

In addition to the (standard) scenarios created using building blocks, the assessment also considers latent threats and wildcards. Latent threats are threats that do not have an immediate, major impact on national security but could certainly create considerable impact on national security in the **long term** (10-20 years from now). These are either long-term developments that gradually create problematic situations or a group of relatively small-scale events that do not appear to have major relevance individually, but the sum of which can have severe consequences for national security over the longer term.

Commonly in the case of latent threats, there is often a tipping point which, once passed, means issues can only be tackled with great difficulty. In many cases, it is possible to ascertain in retrospect that an event occurred which proved irreversible and is the cause of the issues. Risks of this nature can build up slowly and under the radar.

Wildcards are less obvious scenarios focusing on phenomena that are conceivable yet less plausible. For many of these wildcards, there is still great uncertainty with regard to their consequences, although the general expectation is that the impact would be major if such an event were to occur.

Latent threats and wildcards were only elaborated in qualitative terms and serve to complement the standard scenarios. Again, they only provide additional information to the NRA and are not intended to be exhaustive.

2.5 Inventory and selection of themes

Each of the scenarios developed in the context of the NRA sits within a specific threat category, which in turn belongs to a threat theme with a broader scope. An example is the climate and natural disasters theme, which includes the extreme weather events and floods threat categories. The floods category in turn consists of a variety of scenarios that illustrate this specific threat. The risk assessment is based on an all-hazard approach, which covers safety and security threats with both foreign and domestic origins. The threats were selected based on a desk study of existing analysis products and input from experts within the wider network of the ANV. Recent disasters and crises were also reviewed and it was established what these might mean for this current risk assessment.

The set of threats that were selected were grouped into threat themes, which are split into categories. The following table provides an overview of this.

Table 5 Overview of threat themes and threat categories

Threat theme	Category
Infectious diseases	Human infectious diseases and zoonoses
	Animal and plant diseases
Climate and natural disasters	Extreme weather events
	Flood
	Wildfire
	Earthquake
Threats to critical infrastructure	Intentional threat against vital processes
	Disruption of vital processes due to technical or human failure
	Natural event disrupting vital processes
Cyber threats	Disruption of the internet
	Disruption of cyber-physical systems
	Cybercrime
Major accidents	Radiation accidents
	Chemical accidents
	Transport accidents
Social polarisation, extremism and terrorism	Social polarisation
	Non-violent extremism
	Violent extremism
	Terrorism
Foreign subversion of the democratic constitutional system	Espionage
	Foreign interference
	Foreign influencing (hybrid operations)
	Organised crime
International and military threats	Pressure on multilateral security institutions
	Fragility in the vicinity of the Netherlands and/or the EU
	Armed conflict between centres of power
	Proliferation of weapons of mass destruction
Economic threats	Threats to the Netherlands' role as an important logistical hub
	Foreign interference in industry
	Contraction or distortion of international trade
	Unwanted strategic dependencies
	Destabilisation of the financial system

The outcomes of the analyses have been described for each theme separately in the various thematic reports. Amongst other things, these reports include tables listing the ratings for the impact criterions of each scenario and the associated likelihood.

Government of the Netherlands

National Network of Safety and Security Analysts

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*)

July 2022

014482