National Risk Assessment

The National Network of Safety and Security Analysts

Colofon

The National Risk Assessment has been compiled by the National Network of Safety and Security Analysts (ANV) on the request of the Ministry of Justice and Security (NCTV).

The National Institute for Public Health and the Environment (RIVM)
Research and Documentation Centre (WODC)
General Intelligence and Security Service of the Netherlands (AIVD)
The Netherlands Organisation for Applied Scientific Research (TNO)
The Netherlands Institute of International Relations 'Clingendael'
Erasmus University Rotterdam, Institute of Social Studies (ISS)

Contact: ir. L. Gooijer
(leendert.gooijer@rivm.nl)

National Risk Assessment

The National Network of Safety and Security Analysts

Content

1 Introduction

In 2018, the Dutch government decided to develop a long-term National Security Strategy (NVS). To draw up this strategy, an understanding of the most important risks for Dutch national security in the coming years is needed. Therefore the National Coordinator for Security and Counterterrorism (NCTV) asked the National Network of Safety and Security Analysts (ANV) to produce a National Risk Assessment (NRA). The NRA is the foundation on which the new National Security Strategy will be based. Annex 1 provides more information on the ANV.

1.1 Aim

The aim of the National Risk Assessment is to provide an understanding of the main risks for Dutch national security in the coming five years. This report provides an overview of the main risks attributed to different disasters, crises and threats with potentially disrupting effects on society.

There is a potentially disrupting effect on society if at least one of the six national security interests is seriously affected.

In order to present an overview of the most important disasters, crises and threats, an 'all-hazard' approach has been applied. Both non-malicious and malicious threats (safety and security) as well as internal and external risks and threats are included in this type of risk analysis. Because different risks are analysed and assessed in the same manner, they can be compared to each other. The results of the analyses are recorded in a number of thematic reports. The main results of these thematic reports are summarised in this final report[1].

[1] For the purposes of the NRA, the ANV has composed nine separate thematic reports. These reports contain the context, risk categories and scenario analyses belonging to the different risks.

Table 1. The six national security interests

The six national security interests	
Territorial security	The unimpeded functioning of the Netherlands as well as her 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 its 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 being disturbed and groups of people enjoy living together within the benefits of the Dutch democratic system and values shared therein.
International legal order	The proper functioning of the international system of norms and agreements aimed at promoting international peace and security.

1.2 Approach and focus

The NRA takes two aspects into account when determining which risks pose the greatest threat to Dutch society: their impact on the six national security interests and the likelihood of their occurrence. Viewing these two dimensions separately from each other is a deliberate choice. In addition to impact and likelihood, the context and developments belonging to the different risks have been examined as well. This also applies to interdependencies and connections between different risk categories and themes. Consequently, both risks and threats are viewed from a broader perspective, resulting in an integrated risk analysis. Questions concerning resilience and capacity building have not been taken into account.

An important foundation for the analysis is the 2016 National Risk Profile (NVP), commissioned by the NCTV and produced by the ANV.[2] In addition to the NVP, other documents containing assessments, including ANV and third party publications, were also consulted. A first step was to verify whether the conclusions contained in the 2016 NVP were still up to date. Next, a number of additional analyses and expert consultations took place, all of which were based on risk scenarios drawn up by the ANV. In these additional analyses and consultations, there was more focus on risks and threats of an international nature in comparison to the 2016 NVP.
In addition, for each of the risk categories, a literature review was conducted, with the aim of further examining recent developments. The results are documented in the thematic reports, together with the scenario descriptions, impact and likelihood scores, as well as the accompanying analysis. The figure below contains a schematic summary of the process.

The NRA applies and extends the methodology used in the 2016 NVP. The national security interests are the foundation of the analysis. In previous analyses, five national security interests were considered, as mentioned in the 2007 National Security Strategy (SNV): territorial, physical, economic and ecological security as well as social and political stability. The current analysis features an additional interest: the international legal order. Furthermore, within the security interest 'territorial security', two extra criteria have been added: the digital domain and the integrity of allied states' territories. This will be further explained in chapters three and four.

The timeframe of this NRA is 0 – 5 years. Consequently, it focusses on the main risks that currently threaten Dutch society. Long-term developments receive more attention in the thematic reports. The 2018 National Security Horizon Scan (ANV, 2018) also describes these developments in further detail. However, a number of long-term developments are mentioned in this NRA, for example, when developments could have an impact on the risks just beyond the five year timespan. In this way, risks are placed in a broader context.

The NRA limits itself to Dutch territories on the European mainland. Caribbean territories which are part of the Kingdom of the Netherlands have been excluded from the analysis.

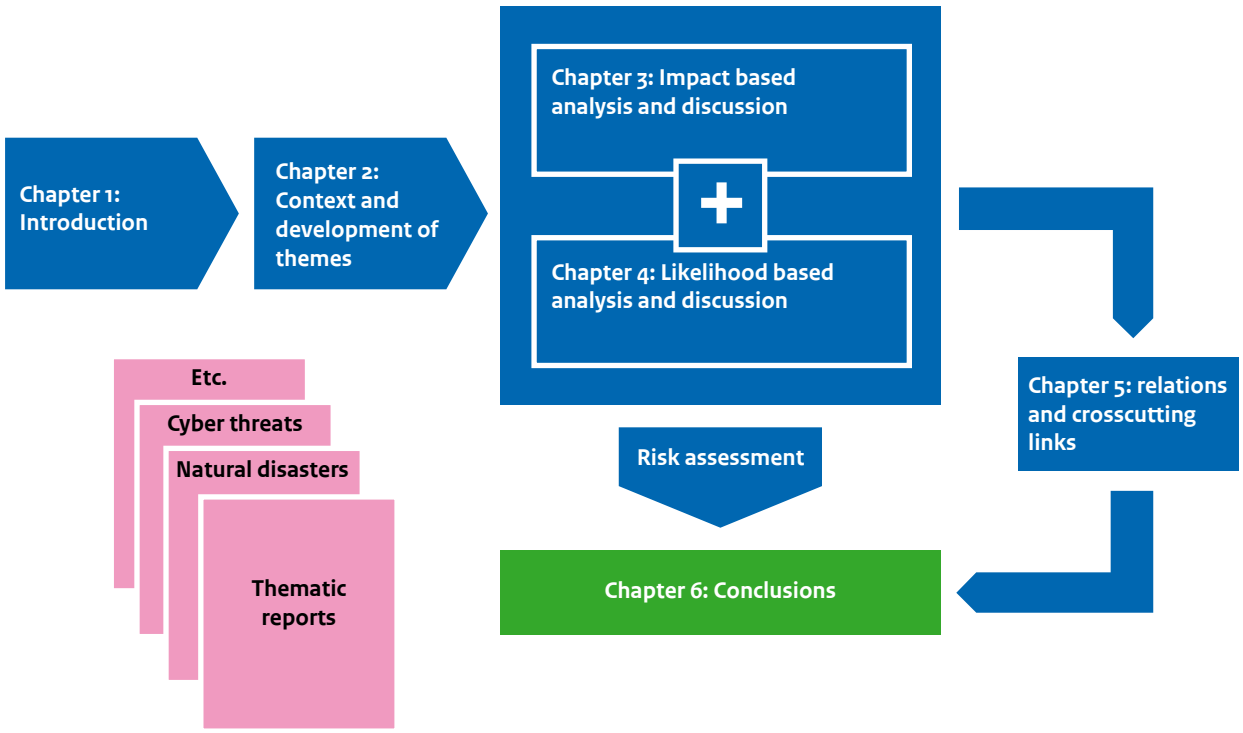
Figure 1. Schematic summary of the process

[2] ANV, National Risk Profile 2016

1.3 Structure of this report

The next chapter provides an overview of all the themes and risk categories that have been included in the NRA. Both the context and (current) developments are discussed for each theme. Using the six national security interests, chapter three provides an overview of risks with the largest potential impact on Dutch society. This answers the question as to how seriously the six national security interests could be affected and thus to how compromised national security could be. Whereas chapter three focusses on potential impact, chapter four looks at risks with the highest likelihood of occurrence. Together, these two chapters form the risk assessment. Chapter five focusses on interdependencies and connections, providing additional context. Finally, all findings are brought together in chapter six. This final chapter also contains the main conclusions of the NRA and gives an answer as to which risks (in the coming five years) pose the greatest threat to Dutch national security.

Figure 2 Schematic overview of the contents of the NRA



2 Considered themes and risk categories

The NRA mostly adheres to the grouping of themes and risk categories in the NVP. There has also been an evaluation of whether additional risks and/or trends need to be included in the NRA. This evaluation was based on up-to-date documents and reports.[3] A couple of existing risk categories have been updated and a few new ones have been added. The new risk categories are: the proliferation of CBRN (chemical, biological, radiological or nuclear) weapons, military threats, instability in Europe's neighbouring countries, security arrangements under pressure (e.g. within NATO, EU), threats to the Netherlands' function as a hub and to its supply lines (flow security), and unwanted foreign influence via hybrid operations. Furthermore, additions have been made to the risk categories digital sabotage, (violent) extremism and the global trade system (belonging to the theme financial and economic threats).

Desk studies and in some cases expert consultations took place for all the themes in order to shed light on recent developments. When risks were still up to date, no further analysis was conducted. These are the risks that belong to the following themes: natural disasters, threats to public health and the environment, major accidents and disruption of critical infrastructure. Naturally, these risks were still included in the results of the NRA. For each of the NRA themes, a thematic report was compiled in which the outcomes of the evaluation and additional analysis were included. These thematic reports should be consulted for a more in-depth analysis. Only the largest risks with a potentially disruptive effect on society were included in the NRA. Additional, less urgent or smaller risks were detailed in the thematic reports. Figure 4 provides an overview of these themes and risk categories.

[3] Documents and reports have been consulted, such as (and not limited to) the Integrated Foreign and Security Strategy, the Defense Memorandum (Defensienota), Clingendael and HCSS strategic monitors, Terrorist Threat Assessment Netherlands, CSBN, MIVD/AIVD annual reports, Cybersecurity Strategy, ANV 2018 Horizonscan National Security.

Each of the following paragraphs briefly describes one of the themes included in the NRA, plus some of the main developments in recent years as well as expected trends. A number of scenario descriptions have been added throughout the text (in separate boxes) as an example. These fictional scenarios provide a better understanding of the risks within a certain category (see the thematic reports for additional information).

2.1 Threats to public health and the environment

The theme of threats to public health and the environment focusses on acute threats to public health and the environment that manifest themselves as a crisis. The following two risk categories have been included: a large-scale outbreak of a human infectious disease (such as an influenza pandemic) and a zoonosis or animal disease. Other, less urgent or smaller-scale threats have been included in the accompanying thematic report.

Concerning this theme, there are a number of relevant points for risks in the longer term. The first point is the rate of vaccination in the Netherlands. The number of young children that receive vaccinations as part of the Dutch National Immunisation Programme (RVP) is still high, but has shown a slight decrease during the last years. However, provisional (beginning of 2019) vaccination rate numbers do not show a further decrease amongst infants. If the vaccination rate drops any further, the chance of infectious disease outbreaks may increase in the long term. There is also a chance that infectious diseases which do not occur anymore in the Netherlands could reappear.

Table 2: Overview of themes and risk categories

Theme	Risk category
Threats to public health and the environment	Human infectious diseases
	Animal diseases and zoonosis
Natural disasters	Extreme weather
	Floods
	Wildfires
	Earthquakes
Disruption of critical infrastructure	Disruption of critical infrastructure
Major accidents	Nuclear disasters
	Chemical incidents
Cyber threats	Digital sabotage
	Disruption of the internet
	Cyber espionage
	Cyber crime
Subversion of the democratic system	Non-violent extremism
	Subversive crime (subversive enclaves)
	Unwanted foreign interference
	Unwanted foreign influence (hybrid operations)
Violent extremism and terrorism	Violent extremism
	Terrorism
Financial and economic threats	Criminal interference
	Threats to the hub function and supply lines of the Netherlands (flow security)
	Trade contraction/disruption of international trade
	Destabilisation of the financial system
Threats to international peace and security	Instability on European borders
	Military threats
	Proliferation of CBRN weapons
	Security arrangements under pressure (NATO, EU)

In addition, Antimicrobial Resistance (AMR) should be monitored as well. In some parts of the world AMR has become a major public health problem. In the Netherlands, the presence of resistant bacteria in humans has remained relatively stable over the past years. The use of antibiotics and the number of healthcare related infections have also remained more or less at the same level, although this varies per type of antibiotic and infection. In order to maintain these levels, the Netherlands should keep protecting itself against the increasing threat of cross-border introduction of AMR.

In terms of the environment, there are a number of developments which can influence food safety and security. Due to a further loss of biodiversity and biomass, there could be significant degradation of both the natural environment and agricultural land. Furthermore, increases in bee mortality and the overall deterioration of insect populations in the Netherlands can potentially affect the pollination of fruit and crops.

2.2 Natural disasters

The theme of natural disasters concerns (potential) disasters caused by forces of nature. These disasters have predominantly natural causes, but can also be triggered (directly or indirectly) by human actions. In addition to floods (from both the sea and rivers), events such as extreme weather (very severe storms, severe snowstorms and frost), wildfires and earthquakes can also have a (serious) impact on society.

An important development within this theme is climate change in combination with an (accelerated) rise in sea level. Because of climate change, the long-term likelihood of natural disasters will increase. Extreme weather events will happen more frequently.

Scenario Extreme weather in the Randstad region

Concerning extreme weather, a scenario can be constructed where due to servere snowfall and frost parts of the Randstad region will be cut off. If the situation lasts for several days, public life in the region will shut down with major disruptions of daily life as a result.

An additional risk related to extreme weather is the combination of two events, for example, the combination of increased amounts of water flowing though the rivers and a westerly storm. Water will be pushed towards the shore from both the sea and the Ijsselmeer and this will impede the flow of water from the rivers into the sea. Subsequently, the risk of river floods will increase.

2.3 Disruption of critical infrastructure

Some processes are critical for the functioning of society to the degree that a disruption may result in severe societal disruption as well. Together, these processes comprise the Dutch critical infrastructure. Disruption of critical infrastructure does not only include the partial or complete failure or disruption of a critical process, but it also includes the (partial) loss of control of these processes due to unwanted foreign take-overs or influence, threatening the continuity and integrity of vital processes.

Disruption of critical infrastructure can be a threat to national security on its own. It can also amplify other threats, such as floods and major accidents. Conversely, a flood, major accident or cyber-attack can also disrupt the functioning of critical infrastructure. Consequently, there is a strong connection between critical infrastructure disruptions and others types of risk. This will be revisited in chapter five. Disruptions of critical infrastructure can be of a malicious as well as a non-malicious nature.

The consequences of a critical infrastructure disruption are often amplified by cascading effects resulting from interdependencies between different critical processes. These interdependencies are often hard to identify. Cascading effects are often limited by auxiliary systems serving as a back-up for crucial parts of critical processes. Effects only emerge when these systems stop functioning. In addition, cascading effects can be influenced by circumstances, such as the season, the time of day and weather conditions (e.g. drought or heavy rainfall). Cascading effects mostly arise through disruption of critical processes within the domains of power supply and IT services.

An important development has been an increase in interdependencies and connections between critical processes. In addition, networks of interconnected systems (also intersectoral) are becoming more and more complex. For instance, the introduction of ‘smart’ technology has resulted in systems that are increasingly dependent on access to electricity and data traffic. Internet dependency is also increasing as process control systems are connected via IP networks on the internet. More traditional alternatives (such as landlines) are rapidly disappearing due to technological innovations. As a result, IT disruptions have an increasing impact on system components. For some vital processes, (European) networks are increasingly connected. As a result, disruptions in one part of the network can have an effect on other parts of the network.

Due to growing societal dependency on digital infrastructure and potentially major cascading effects, a couple of transitions are especially relevant for both the continuity and security of critical infrastructure: the transition to sustainable energy and to autonomous systems. It is currently not possible to predict the effects of the transition to sustainable energy on energy supply in the long term. However, a transition will take place and there will be new vulnerabilities. The risks associated with autonomous systems will increase as these systems are becoming more widespread in different areas, such as the electricity sector, the financial sector and industry. Autonomous systems often do not stand alone and need communication and interaction (mostly via internet) between different components or entities in order to function. This makes them vulnerable to outside interference. Interactions between autonomous systems can also result in the disruption of critical processes, for example, due to software design flaws or unanticipated 'behaviour'.

2.4 Major accidents

This theme consists of all major accidents with the potential to disrupt society. These include nuclear disasters (nuclear power plants), major chemical accidents and major transportation accidents. In the case of a major transportation accident (such as a plane crash), a large number of casualties is to be expected. However, as with the 2016 NRP, no transportation accidents have been included in this report as the (overall) effects of chemical accidents and nuclear disasters are larger.

There have been no major accidents affecting national security in the past years. There are however concerns amongst parts of the population about the safety and supervision of several Belgian nuclear power plants close to the Dutch border. A number of developments related to the chemical industry are also worth mentioning. First of all, the ageing of chemical installations is something many companies will have to face in the coming years. Furthermore, major companies are increasingly being divided into multiple, smaller ventures. As a result, increasing numbers of companies can be found on the same site. This means that safety arrangements have to be coordinated amongst more parties than before.

2.5 Cyber threats

This theme looks at events or activities that compromise the confidentiality, integrity or availability of IT systems, the information they contain or services that depend on them. These events include digital sabotage (including any collateral damage), cyber espionage, cybercrime and disruption of the internet.

Cyber threats include a wide range of disruptions or incidents which have a digital origin. A cyber threat can be both a means as well as a goal in itself. For example, cyber threats can be deployed as a means during hybrid operations. However, digital systems can themselves also be targets. These disruptions can have non-digital causes. Because the disruption of digital systems will also have (additional) non-digital consequences, it is not always easy to distinguish between cyber threats and other threats.

Scenario digital sabotage

Scenario 'collateral damage': A foreign hacking collective has successfully hacked an Indian software supplier which provides popular administrative software programmes. The software is used globally by both public and private organisations in a wide range of branches. The hack allows the perpetrators to provide a malicious security update for the software to its users. Because many organisations have a policy of rapidly installing new security updates, the malware spreads fast. Organisationsoperating in the Netherlands are also affected.

Recent analyses emphasise the (digital) threat posed by state actors. Their aim is mostly to subvert or disrupt an open and democratic society, acquire strategic information through espionage and disrupt or even sabotage crucial systems. Digitalization has resulted in a stronger connection between internal and external security. The threat of Russia is particularly mentioned. This country takes advantage of the vulnerabilities of open and democratic societies, using digital means to achieve political objectives. China is also often mentioned due to its economically and strategically driven activities including (cyber) espionage.

Besides direct attacks aimed at Dutch targets, collateral damage caused by an attack aimed at another target also has to be taken into account in relation to digital sabotage. Although it is hard to attribute attacks to specific targets and perpetrators, most damage is incurred by collateral damage. The 2017 NotPetya incident is a well-known example of collateral damage. The effects of digital sabotage quickly spread to different countries and industries, including several companies operating in the Netherlands (for example Maersk operating from the port of Rotterdam). The same applies to WannaCry (2017). It affected 150 countries with large societal and economic impact (such as severe disruptions of processes in UK hospitals). In both cases, the Netherlands remained relatively unaffected. It is however very likely that the effects of similar attacks could be much more substantial in the Netherlands as well.

In general, digital threats are very likely as cyberattacks are not difficult to perpetrate, are low risk and can simultaneously be very profitable. Because society increasingly uses and depends on information and IT systems, the risks are also increasing. Technological developments add to the interconnectedness, complexity, uncontrollability as well as dependency on systems and processes. The strategic dependency on foreign parties, suppliers, producers and service providers also contributes to the increased vulnerability to espionage, sabotage and disruptions. Chapter five shows the influence of some of these links, and the interconnectedness between the themes. This is also dealt with in the thematic report on cyber threats.

Cyberattacks will have more severe consequences (and better outcomes for perpetrators) as society's level of digitalisation keeps increasing. In addition, research has shown that defences against cyberattacks are at risk due to a failure to keep up with the fast-paced developments in the digital domain.

2.6 Subversion of the democratic system

This theme focusses on the structural, intentional and in many cases hidden activities of (non-)state actors that, due to their objectives, means or effects, can affect the Dutch political and societal systems. This includes compromising, weakening, destabilising, undermining or sabotaging the systems in question. The damage caused to essential societal cohesion has also been included by reviewing solidarity and mutual trust amongst citizens. The activities of both state and non-state actors (extremist and criminal entities) have been examined.

Subversion by non-state actors

National security is threatened when subversive activities become both structural and large-scale: the functioning of administrators and politicians is impeded, democratic institutions are disrupted and citizens cannot exercise their fundamental rights. Subversive groups can spread non- or anti-democratic narratives or can try to create parallel societies by actively rejecting an open and democratic one. Parallel societies can also be created by criminal groups, not just extremists. In some cities, there are signs of the creation of enclaves that disrupt, undermine, counteract and openly reject the local administration. In relation to other European countries, the Netherlands is still relatively unaffected by this trend.

Scenario subversive enclaves

Extremists groups (in particular radical Islamic movements) try to create their own parallel societies (subversive enclaves). They actively spread intolerant and antidemocratic views and people are encouraged to reject an open and democratic society. In time, this can violate government authority.

Subversion by state actors

In the Netherlands, there are several specific examples of activities executed by foreign governments with the aim of (secretly) interfering and exerting influenceng.

On the one hand, foreign governments can (secretly) interfere by maintaining relations with or keeping in check local diaspora communities. Blackmail and intimidation are often used for this purpose. On the other hand, unwanted influence can be aimed at compromising, weakening, undermining or destabilising the Netherlands, including its democratic constitutional system.

Hybrid conflicts are not new. However, the scale and frequency with which increasingly assertive states use these methods are new. The higher frequency of hybrid operations aimed at subverting foreign societies is part of an ongoing international competition between states. Part of this competition is the exploitation of societal and political vulnerabilities, with major potential consequences if destabilising circumstances and unwanted foreign activities coincide. IT developments facilitate this type of influencing and subversion.

Hybrid operations – explanation

The analysis focusses on hybrid operations by both Russia and China. The main Russian objective is to expand its relative powerbase by weakening other societies and institutions such as NATO and the EU. In the past years, China has solidified its position on the world stage and has expanded its influence mainly through economic instruments. China is also trying to acquire influence in Europe through setting up a vast network within politics, industry, think tanks and universities. This could (in time) undermine European unity. China's hybrid influencing should be seen as a long term development.

2.7 Violent extremism and terrorism

Extremism can be defined as actively striving for or supporting profound changes in society that could endanger our democratic legal order. This could be through the use of undemocratic methods, such as violence and intimidation, with detrimental effects for our democracy. Acts of terrorism are the most extreme manifestation of violent undemocratic means. The (potential) consequences of violent extremism and terrorism are discussed within this theme.

There are a number of noteworthy developments. For example, there are signs that the traditional axis of left- and right-wing extremism may become less relevant in the coming years. Instead, they will be transcended by new phenomena, such as 'identity based extremism' or 'anti-government extremism'. New groups have emerged that, from an ideological points of view, aim to 'keep the white race pure'. Subsequently, they agitate against 'racial mixing' and changes in the ethnicity of the population. In addition, there are (groups of) angry citizens that agitate against the government for various reasons. Despite the rise of these sentiments, which are mainly voiced online, it remains uncertain whether extremists' willingness to commit violence in the Netherlands will increase in the short term.

Where terrorist threats in the Netherlands are concerned, the greatest risk is represented by jihadism. ISIS supporters continue to pose a threat, but also the capabilities of (core) al-Qaeda members should not be underestimated. When currently detained and persistent jihadists are released, a potential future threat will arise, especially if they do not renounce their jihadist ideas. Both the occurrence of attacks by violent loners and large(r)-scale attacks are considered to be (very) likely; there are (several) indications that they might actually take place (in different but comparable forms). Furthermore, it cannot be ruled out that other politically or ethnically inspired forms of terrorism will gain more importance in the coming years.

2.8 Financial and economic threats

This theme covers potential incidents or crises that can occur within the financial and economic system. In particular, it looks at events that occur outside of normal patterns of economic fluctuations (economic cycle). These events include the destabilisation of the financial system and criminal interference. Disruptions to the system of international trade, such as a trade war or a strong (sudden) disruption of the system, are also included. The same applies to threats to the hub function and supply lines of the Netherlands (flow security). In particular, the latter two threats are detailed in the analyses.

As both China and the United States are currently imposing trade-restricting measures, a disruption of the international trade system will be a relevant risk for the coming years. This is in line with ever increasing fragmentation and protectionism within the international financial and economic system. These developments are in turn part of an overarching trend of (economic) deglobalisation and shifting economic power relations that will lead to changes in the position of the United States relative to China.

Regarding threats to the hub function and supply lines of the Netherlands (flow security), a number of major transport hubs for goods (the ports of Rotterdam and Amsterdam), people (Schiphol airport) and data (the Netherlands is the 'digital gateway to Europe') are located in the Netherlands. This hub function as well as the accompanying supply lines can be threatened in different ways in both the long and short term. It is not expected that (potentially conflicting) strategies aimed at improving the links between states and regions (such as the Chinese Belt Road Initiative (BRI) or developments in the Arctic) will have (direct) effects on national security in the coming five years. Other developments, such as blockades or other regional tensions that impede free shipping, could have consequences for security between now and five years. This is especially envisaged in regions where tensions can run high, such as the Middle and Far East. As a result, consequences for the Netherlands will remain limited.

2.9 Threats to international peace and security

This theme considers the risks of (international) political issues and developments as well as conflicts over the control of land, sea and airspace aimed at demarcating boundaries and spheres of influence.

The international order is changing profoundly. The age during which the international system of states and the power relations amongst them was dominated by the United States seems to have come to an end.
A resurging China and a revisionist Russia are both challenging the United States. Even the European Union and the United States, that together have been the cornerstone of the liberal world order, have regularly been in disagreement over the past few years. As a result of these developments, shifting coalitions have arisen in different fields. Instead of a bilateral or multilateral order, a multi-order has emerged. These changing international relations will contribute to insecurity and a worsening international security situation. This is compounded by ongoing polarisation between certain groups within the population which puts pressure on our democracies as well as on the current consensus on international cooperation.

Four risk categories have been elaborated on within this theme: instability on the borders of Europe; military threats; CBRN proliferation; and Pressure on security institutions (NATO, EU).

Instability on European borders

The European Union, and therefore the Netherlands, is being confronted with a 'ring' of increasing instability, conflict and the ever present chance of newly arising conflicts. Libya, Syria and Lebanon remain highly fragile countries and Turkey and Egypt are at risk as well.
The fragility of (inter alia) the Ukraine and Bosnia-Herzegovina, bordering directly on the European Union (hereinafter: Europe), has also increased. Regions with the highest degree of fragility are located in a wider ring around Europe, running from West Africa to Afghanistan and Pakistan. It is expected that this fragility will increase in the next five to ten years. Instability leads to refugees and facilitates migration movements in general. This results in humanitarian and security issues at European borders. More importantly, the influx of refugees can, in the current political climate, lead to social and political tensions, both domestically or between EU governments.

Scenario instability on European borders

The destabilisation of a country at the borders of Europa is accompanied by conflict, migration, crime and violent extremism with effects in the EU itself. This endangers EU cohesion and especially the Schengen system. The scenario is based on the destabilisation of a Northern African country.

Pressure on EU and NATO

Taking into account persistent uncertainties and increasing threats, it is important for the Netherlands that the two organisations it uses to safeguard its security interests, NATO and the EU, function well.
The United Nations as a global organization is also vital to the Netherlands, especially as a hub for the functioning of the international legal order. However, the EU and NATO have been selected here because of the direct importance of these organisations for national security. The EU is a comprehensive security actor with an involvement in both domestic security as well as in the security of Europe and its neighbouring countries. The Netherlands has enshrined its collective security in NATO, which embodies U.S. security guarantees.

External and internal factors are severely challenging both the EU and NATO. U.S. governmental policies are putting a large strain on transatlantic relations. Whereas in the past, cooperation and joint interests were key to resolving transatlantic tensions, these joint interests are becoming increasingly fewer. In addition, NATO is under threat from the inside by an increasingly autocratic Turkey which is strengthening political and military ties with Russia. A lack of unity amongst EU member states means that the EU is insufficiently able to exert its (political) weight when it comes to the international order. The EU's ability for effective negotiation is further hampered by Brexit, migration issues and the imbalance in the Eurozone.

Military threats

The chance of armed conflict has been increased by tensions between major powers and instability at the outer borders of Europe. Military developments have contributed to this as well. Since the end of the Cold War, global defence expenditures have never been as high as the figures from 2017. The largest budget increases originate from China, Russia, Saudi Arabia, but also European NATO countries (put together). Other indicators also point to increasing military threats. Increased tensions between states are reflected by the use of more aggressive rhetoric, ever larger military exercises and many violations of both territorial waters and airspace.

Proliferation of CBRN weapons

Finally, recent technological developments have given rise to concerns about the possible deployment of biological weapons. Similarly, nuclear weapon arsenals are being modernised and expanded worldwide whilst treaties on arms limitation are under pressure (Intermediate-Range Nuclear Forces), ending (New START) or are being ignored (Non-Proliferation Treaty). As doctrines for the use of nuclear weapons are changing, low yield nuclear weapons may acquire a place during armed conflict. Additionally, there are concerns that nuclear and radiological materials may get in the hands of non-state actors (this is considered in the theme violent extremism and terrorism).

2.10 Reflection

This chapter has provided an overview of the different themes and risk categories. We checked whether the analyses of scenarios contained in the 2016 NRP were still up to date or needed revision. In addition, we considered whether new risk categories needed to be developed based on current developments within the existing themes.

No additional analyses were performed for the following themes: Threats to public health and the environment, Natural disasters, Major accidents and Disruption of critical infrastructure. The 2016 NRP analyses were used for these. However, within these themes, a number of recent developments that are relevant for national security have been included. We have considered two of them:

- An obvious example is climate change. The long-term likelihood of natural disasters is increasing due to climate change and the accompanying (accelerated) rise in sea levels. Climate change can also lead to an increase in heat stress and facilitate the spread of pathogens. From a broader perspective, climate change is also mentioned as one of the factors that drive migration. Geopolitical tensions related to the Arctic region are also related.

- A second development is the increasing (societal) dependence on and interconnectedness of critical processes. This development is already of importance, but in the future, ongoing technological progress will be especially relevant for national security. The increased use of autonomous systems in different industries and their accompanying risks was mentioned as an example of this.

For the other themes, new analyses (additional to the 2016 NRP studies) have been conducted. From the analyses, a number of developments were seen as relevant for future risks. An example is the use of hybrid operations that, due to developments, inter alia, in the digital domain, have become larger in scale and more frequent than in the past. Several international developments (see paragraphs 2.8 and 2.9) also necessitated additional analysis concerning Financial and economic threats as well as International peace and security. Within these themes, a number of scenarios were developed. These were analysed in terms of their likelihood and consequences during expert consultations sessions. The results of these analyses (together with the still up to date results from the 2016 NRP) can be found in the following chapters.

3 Risks with greatest impact on national security interests

This National Risk Assessment (NRA) uses the same risk assessment methodology as described in the Dutch National Risk profile published in 2016. However, as requested by the National Security Strategy interdepart mental project group, an additional national security interest has been identified (International legal order). A number of additional impact criteria were added as well, which are explained under Table 3.

Table 3. National security interests and impact criteria

National security interest	Impact criteria
1. Territorial security	1.1 Encroachment on Dutch territory
	1.2 Infringement of the international position of the Netherlands
	1.3 Infringement of digital infrastructure integrity
	1.4 Encroachment on allied territory
2. Physical safety	2.1 Fatalities
	2.2 Seriously injured and chronically ill
	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	**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

Table 4. Example of an assessment using two impact criteria and five severity classes

Class	Example criterion: Number of fatalities	Example criterion: violation of the democratic constitutional system
Limited	Less than 10	Limited violation of the functioning of a couple of institutions
Substantial	10 to 100	Limited violation of the functioning of several institutions
Serious	100 to 1,000	Considerable violation of the functioning of several institutions and/or violation of freedoms, rights and core values
Very serious	1,000 to 10,000	Structural violation of the functioning of several institutions and freedoms, rights and core values
Catastrophic	More than 10,000	Structural violation of the functioning of institutions and freedoms, rights and core values

By expanding on both security interests and impact criteria, a more consistent link between internal and external security topics has been established.[4]
Explanation of the new criteria:

- Infringement of digital infrastructure integrity involves the loss of function or control of essential digital infrastructure due to degradation of availability, confidentiality and integrity of these systems. Digital infrastructure is defined here as the conglomerate of IT resources and services, containing all entities that are (or may be) digitally connected.
- Encroachment on the integrity of allied territory concerns the inaccessibility of, or the loss of control over (parts of) the territory of EU member states and/or NATO members (allies). This includes airspace, territorial waters and digital infrastructure. Encroachment only includes deliberate actions of groups and states aimed at disrupting the territorial integrity of allies.
- The newly identified national security interest 'International legal order' is comprised of four impact criteria that together clarify the full context and scope. It comprises a combination of violation on the following: state sovereignty, human rights, a well-regulated financial-economic system, and effective multilateral institutions and regimes.[5]

All the criteria have been created in order to provide insight into the potential impact of threats on the six national security interests. An important aspect of the methodology is scenario analysis, in which impact and likelihood of fictional incidents are assessed using a predetermined scale. These scenarios are representative for, and illustrative of, the risks posed within a category. During sessions with a wide range of experts related to the ANV, scenarios helped assess the risks in terms of both impact and likelihood (see Chapter 4).
The predetermined scale used elaborates on the set of impact criteria as shown in Table 3. This chapter explains which risk categories have the greatest impact on each of the described security interests and associated impact criteria.

The impact criteria have been made measurable using a system of classes to determine the degree of severity. A distinction is made between five classes varying from limited (A) to catastrophic (E). Table 4 shows the general division into classes, including two examples.

3.1 Territorial security

The security interest territorial security first of all includes our country's physical territory and corresponding infrastructure. In addition, potential risks regarding digital infrastructure and the image and reputation of the Netherlands are taken into account. Finally, encroachment on allied territory falls within the scope of territorial security as well.

The table below provides an overview of risk categories with the highest impact on each of the four impact criteria. A short explanation is provided for each impact criterion as well.

[4] A detailed description on security interests and impact criteria can be found in the Integrated Criteria Risk Guideline (ANV, 2019).

[5] This elaborated on the paper 'International Legal Order as the sixth National Security Interest', which was drafted by Clingendael Institute on behalf of the ANV.

Impact criteria Territorial security	Most relevant Risk categories
1.1 Encroachment on Dutch territory	Floods Nuclear disasters
1.2 Infringement of the international position of the Netherlands	Military threats Tensions within security institutions
1.3 Infringement of digital infrastructure integrity	Natural disasters (as an example: floods) Digital sabotage Cyber espionage Unwanted foreign influence (hybrid operations) Military threats
1.4 Encroachment on allied territory	Military threats Unwanted foreign influence (hybrid operations) Digital sabotage

3.1.1 Encroachment on Dutch territory

The territory of the Netherlands can be affected in a number of ways. Analyses show that risks emerge primarily from disasters such as floods and nuclear disasters. The consequences of such disasters are that part of our territory will be unusable or inaccessible for a long period of time. No risks associated with the occupation of Dutch territory, which violates state sovereignty of the Netherlands, have been considered.

3.1.2 Infringement of the international position of the Netherlands

An international conflict and interference by subversive parties operating in the business community can seriously damage our country's international position, either at political-administrative level or economically, as well as threaten our autonomy.

In the context of an international conflict, a scenario can be envisaged involving tensions between a superpower and a NATO, causing the Netherlands to get involved. If these tensions escalate into a military conflict, the impact on this criterion will be catastrophic (scored as E). Both political and non-political relations will come under pressure, for example, by expulsion of diplomats and through boycotts. In addition, negative publicity may be generated via the use of hybrid actions.

Tensions within NATO or the EU may harm the position of such an alliance as well, including the Netherlands. This clearly affects the international legal order in terms of functioning of multilateral institutions.

3.1.3 Infringement of digital infrastructure integrity

Digital infrastructure can be affected by both malicious and non-malicious incidents and concerns the availability, integrity, and confidentiality of essential information systems (e.g. digital government systems, service providers, and process control of critical infrastructure). Non-malicious incidents include the disruption of critical infrastructure, whereby essential process control systems malfunction. In the event of a natural disaster, such as a flood, it is possible that digital services which are needed as part of disaster relief could be severely hampered.

Cyberattacks are used to deliberately disrupt digital infrastructure. Examples include cyber espionage compromising information systems, or digital sabotage of essential information systems. In the case of digital sabotage, the intention behind it is not necessarily to cripple or damage specific systems. Rather, such systems can become 'collateral damage'; they can get seriously affected as a side effect of other intentions. Due to digital interconnectedness, a cyberattack between two actors, for example in the Middle East or Asia, can cause serious disruption of industrial automation and process control systems or other digital services in the Netherlands.

Cyber capabilities can be deployed as part of hybrid operations as well, including targeting essential information services.

The analysis reveals that if military threats escalate, hybrid conflicts will occur as well. In such cases, digital infrastructure will be targeted as well. If a military conflict between a foreign actor and NATO becomes imminent, the Netherlands may become a specific target due to its logistic facilities.

3.1.4 Encroachment on allied territory

Encroachment on allied territory is relevant only in case of an international conflict. Through Article 42.7 of the EU Treaty and Article 5 of the NATO Treaty, the Netherlands has committed itself to assist its allies. The relevance of such an event is described in a scenario where tensions between NATO and a foreign actor arise. An example is an escalating incident between the Russian Federation and one of the Baltic States.

Such an incident will most likely be accompanied by hybrid operations. When digital sabotage is part of the operation, it could fall within the definition of 'encroachment on allied territory' as well, especially if NATO regards the particular case as an Article 5 situation. Should loss of control over allied territory occur, e.g. if parts of the territory of a NATO ally have been occupied, this impact criterion will receive a maximum impact score (E). The Netherlands can also become a target of undesirable interference from foreign state actors as well.

3.2 Physical safety

Physical safety as a security interest concerns people's health and well-being. The impact of this criterion is measured as numbers of casualties (fatalities, seriously injured and chronically ill, including psychological disorders) and lack of basic needs. Large numbers of casualties will primarily occur during natural disasters, major accidents and threats to public health, such as a pandemic). Access to basic needs will be severely impacted if critical infrastructure fails.

3.2.1 Fatalities and injured

Large numbers of victims (criteria 2.1 and 2.2 are taken together here), come about primarily in the event of natural disasters and infectious diseases. Both floods and an influenza pandemic can potentially lead to tens of thousands of casualties (catastrophic impact).

In the event of a severe coastal flood (flood – severe (sea)), the affected area is estimated to be substantial (approximately 4,000 km^2). Based on an average population density of 450 persons per km^2, the number of fatalities that can be expected in such an event exceeds 10,000.

A severe influenza pandemic affects national security because it may create numerous fatalities and ill people. This can have an impact on the proper and adequate functioning of society in general and the public health sector in particular.

Major accidents have an impact at national level in extreme cases only, for example, in the event of a large-scale chemical incident. Should an incident with chemicals occur, a large numbers of people may be exposed. As a result, the number of fatalities and, in particular, (seriously) injured and chronically ill people could be relatively high. In the case of nuclear disasters, e.g. at a nuclear power plant, no fatalities due to direct radiation exposure will occur. However, people will become ill and may eventually die of cancer due to exposure. Transportation accidents are more likely to

Impact criteria Physical safety	Most relevant risk categories
2.1 & 2.2 Fatalities, seriously injured and chronically ill	Floods Infectious diseases (human, influenza pandemic) Animal diseases and zoonosis (Avian influenza epidemic) Chemical accidents Nuclear disasters (long-term) Transport accidents Terrorism
2.3 A lack of basic needs (physical suffering)	Disruption of critical infrastructure Floods Extreme weather Wildfires

Scenario Influenza pandemic - severe

In this worst-case scenario, millions of people become infected during a severe influenza pandemic. The number of people admitted to hospitals ranges between 40,000-50,000, and the number of fatalities exceeds 10,000. This leads to severe pressure on the public health sector and a disruption of daily life.

have an impact at regional rather than national level, although impact at national level is possible in the event of a large number of victims (plane crash).

In addition to disasters and incidents that occur unintentionally, malicious threats can lead to casualties. For instance, a major (multiple) terrorist attack can cause a substantial number of victims (tens to more than 100). This was exemplified by the attacks in Paris (2015) and Brussels (2016). Such incidents were taken as a starting point for the analysis. Attacks resulting in thousands of fatalities, such as the 2001 attacks in the United States, will result in a higher score on impact criteria, but at the same time are highly unlikely to occur (due to the capacity required to execute such an attack). Small-scale attacks, by violent loners or rapidly radicalised groups are more likely to occur.

3.2.2 A lack of basic needs

An important cause of a lack of basic needs is the disruption of critical infrastructure. The impact severity depends on the duration and scale of the disruption. If cascading effects occur as well, e.g. if energy and drinking water supply, and telecommunications are also affected for a prolonged period of time, the impact will be catastrophic, especially if disruptions carry on for several weeks.

Disruption of critical infrastructure can occur intentionally, through a cyber-attack, or unintentionally due to technical failure. Due to the increasing digitisation of critical infrastructure, it can become more vulnerable.

A lack of basic needs can also emerge if densely populated areas become isolated for a few days due to natural disasters, such as floods, wildfires, or extreme weather. Although the actual consequences of extreme weather events depend on the duration of the particular phenomenon (heavy storm, black ice, snowstorm) and the area affected, the impact is generally considered to be regional in scale.

3.3 Economic security

Economic security as a security interest concerns both economic damage (costs) and the vitality of our economy (for instance, a sharp increase in unemployment). It is evident that financial-economic crises can affect the economic security of the Netherlands. In particular, this refers to events which can be differentiated from the normal pattern of fluctuations in the economy, such as destabilisation of the financial system and criminal interference in the business community. Large disruptions or (natural) disasters can also cause significant costs.

Impact criterion Economic security	Most relevant risk categories
3.1 Costs	Disruption of critical infrastructure
	Floods
	Nuclear disasters
	Destabilisation of the financial system
	Trade contraction/disruption of international trade
	Criminal interference
3.2 Violation of the vitality of Dutch economy	Destabilisation of the financial system
	Trade contraction/disruption of international trade

3.3.1 Costs

Almost all risk and threat variants identified during the analysis affect the economy; in particular the 'costs' criterion. This criterion primarily concerns financial damage.

In addition to financial-economic threats (destabilisation of the financial system, trade contraction/disruption international trade and criminal interference), disruption of critical infrastructure with cascading effects, floods and nuclear disasters can cause significant costs. The impact criterion 'costs' can be very seriously or even catastrophically affected in such cases. In the severe flood scenario (caused by the sea), for example, costs are estimated to exceed 100 billion euros after the first 48 hours. This includes direct financial losses (for individuals), companies and institutions (permanent financial losses), and indirect financial losses. This is already considered as catastrophic (E), even without a complete picture of all costs involved.

3.3.2 Violation of the vitality of the Dutch economy

The vitality of the Dutch economy is robust and will only be very seriously affected in the event of several international economic threats: destabilisation of our financial system (a financial crisis), and a trade contraction or disruption of international trade.
For example, an escalating global trade war in which the EU or the Netherlands gets involved, or a severe shock to global trade systems. If there is no recovery from the shock (a decrease of 10 percent in the case of a trade contraction) after a single year, the impact on the vitality of the Dutch economy may be catastrophic (E). This may also be the case if EU internal tensions escalate, for example, as a result of a chaotic Brexit combined with increasing tensions between South/East and North/West EU member states. The likelihood of occurrence of such a combination of events is lower than of one of the events occurring individually.

These risks are all linked to international economic and (geo)political developments.

Economic security – broader perspective

Experts find that in particular (digital) espionage from an economic point of view can have severe consequences for, for example, competitive positioning of businesses. However, a solid estimation of the exact impact remains challenging, because effects often only emerge after long periods of time. Other aspects that are important from an Economic security perspective are difficult to express in terms of national security impact criteria. Examples include the protection of high quality knowledge regarding Dutch competitive position, the protection of businesses within top sectors and critical infrastructure against undesirable foreign take-overs or strategic dependence on foreign actors.

3.4 Ecological security

Ecological security as a security interest concerns long-term violations of nature, the environment and ecosystems. All the analyses that the National Network of Safety and Security Analysts have performed, including in the past, show that the impact on this security interest occurs only in the event of a natural disaster.

Impact criterion Ecological security	Most relevant risk categories
4.1 Long-term violation of the nature (flora and fauna) and the environment	Floods
	Wildfire

A flood can affect multiple nature reserves for long periods of time. For example, the coastal flood scenario analysis reveals that, within a large part of the natural reserve affected, more than half of the species may be affected for more than ten years. After a flood, it will take time for nature to recover. A matter of concern is salt water intrusion; most (Dutch) natural habitats need fresh water. It is therefore unclear in how far they will recover.

In addition to a severe flood, the natural environment can be affected by a wildfire as well. In the Netherlands, several large wildfires (by Dutch standards) occurred in the past years. Higher temperatures, and in particular the hot, dry summers that will occur more frequently due to climate change, may result in an increase in wildfires. Most wildfires in the Netherlands are rather small-scale in nature though, with limited effects.

It is striking that nuclear disasters or chemical accidents have no or only a limited impact on Ecological security. Although environmental norms may be exceeded to a small extent, ecosystems and the natural environment will not actually be impaired.

3.5 Social and political stability

This security interest focuses on the disruption of daily life, violation of democratic institutions and society's norms and values, and destabilisation of our social climate and accompanying emotions (fear, anger, grief). In this security interest, there is a clear distinction between malicious and non-malicious intent. Non-malicious threats, such as a human infectious disease or a flood, can disrupt daily life. Violation of the democratic constitutional system and the concomitant social impact are (mainly) caused by malicious threats, as well as (foreign) interference and influence. Additionally, internal tension within NATO or the EU can have an impact on society.

Impact criterion Social and political stability	Most relevant risk categories
5.1 Disruption of daily life	Disruption of critical infrastructure
	Floods
	Human infectious diseases (influenza pandemic)
5.2 Violation of the democratic constitutional system	Criminal interference
	Cyber espionage
	Violent extremism
	Non-violent extremism
	Subversive enclaves
	Unwanted foreign influence (in diaspora communities)
5.3 Societal impact	Terrorism
	Pressure on security institutions (NATO, EU)
	Undesirable foreign influence (hybrid operations)

3.5.1 Disruption of daily life

Disasters that affect critical infrastructure, such as electricity supply or internet services for example, as well as large-scale evacuations due to floods, will quickly lead to very serious or even total (catastrophic) disruption of daily life. Large groups of people will (temporarily) not be able to participate in society (attending school, work, or other social activities).

A human infectious disease (influenza pandemic scenarios) can seriously disrupt daily life as well. Since a large part of society will fall ill, educational systems and business operations will stagnate and such an event will put an enormous pressure on public health system.

3.5.2 Violation of the democratic constitutional system

A temporary violation of the democratic constitutional system can occur as a result of various risk factors or threats. However, this criterion concerns a structural violation of the democratic constitutional system and the norms and values of our open society. The analysis has revealed various threats that can have a very serious impact on the democratic constitutional system in the Netherlands. For instance, criminal interference in business operations and in public administration can result in distrust towards (government) parties involved. The same applies to cyber espionage; it may lead to decreasing confidence in official bodies, especially if the government has been targeted. Other threats intentionally undermine the democratic system. For example, violent and non-violent forms of extremism, in particular if they includes hate campaigns with a focus on identity aspects or when anti-government sentiments are expressed, which may contribute to the emergence of parallel societies. Subversive criminality (enclave forming) affects our democratic constitutional system as well. Similar to extremists, criminal groups may try to enforce parallel societies or create their own 'no-go areas'. Administrators and politicians who try to restrict their space and influence can end up facing intimidation and threats.

A very serious violation of the democratic constitutional system can arise due to undesirable interference of a foreign actor. Specifically, this concerns state actors exerting influence on diaspora communities in the Netherlands, or via hybrid operations. These operations often exploit already existing public debates and facilitate increasing polarisation. In order to achieve this polarisation, disinformation campaigns are deployed that, for example, reinforce conspiracy theories and undermine confidence in governmental bodies and institutions.

3.5.3 Societal impact

Although most scenarios lead to a certain degree of unrest and fear or anger among the Dutch population, only a few will lead to an actual destabilisation of society. This is particularly the case for situations in which there is a large degree of uncertainty about the future course of events; in which there is a feeling that (governmental) bodies or companies are culpable; or which result in various groups opposing each other (based on different interests or viewpoints) which in turn can lead to outbreaks of violence (riots or revolts, as well as looting) or a structural violation of the social cohesion.

It is conceivable that terrorism will have a serious societal impact, especially if it concerns a series of attacks, large numbers of casualties or perpetrators that are difficult to trace. It is expected that the societal impact will be limited after a small-scale attack.

Scenario Undesirable foreign influencing (long arm activities)

A foreign state actor, with a large diaspora community in the Netherlands, decides to invoke a control mechanism that enables the monitoring of all critical statements towards the regime within the diaspora community. When signals of this start to emerge, an increase of fear and mistrust within the diaspora community is reported. In addition, conversations in public on politics or other sensitive issues become increasingly difficult. Out of fear for repercussions by the foreign state actor, public statements by the diaspora community against the control mechanism become limited as well. The Dutch government is not able to curb the current situation, without the possibility of a negative impact on international relations. As a result, the diaspora community withdraws from society, which has a negative impact on the already difficult integration process of the community into Dutch society. The situation results in a negative image of the diaspora community within Dutch society. The members of the diaspora community feel that they are not considered full members of Dutch society, and feel that they have an obligation to abide by the laws of the foreign state actor.

Another example that may lead to a very serious societal impact is a situation in which internal tensions within NATO or the EU escalate to the extent that there may be a confrontation, or if EU migration policy becomes disrupted. This can lead to hostilities between diaspora communities in the Netherlands or to consequences for migration, leading to tensions within Dutch society. Here, the interconnectivity between internal and external security becomes apparent.

Unwanted foreign influence can also have a very serious societal impact. A foreign actor can exploit an existing public debate to disseminate conspiracy theories, enforce existing contradictions, and to further cast aspersions on the government via a campaign of disinformation. An example of a public debate that could be exploited is the issue of vaccination, which has led to differences of opinion in society with fierce debates taking place on social media, and parts of the population mistrusting official (governmental) bodies.

3.6 International legal order

This security interest concerns the proper functioning of the international system of norms and rules aimed at promoting international peace and security. The analysis shows that the impact criteria belonging to the international legal order can be very severely affected in a number of ways. Risks associated with the upholding (or not) of (CBRN) arms control and non-proliferation agreements, economic developments (trade wars), and changes in the balance of power, in combination with instability and (internal) tensions within NATO and EU can all be found in relation to the different criteria.

A well-functioning international legal order can be affected without there being a short-term impact on one of the other security interests. For instance, the annexation of the Crimea has had no significant direct consequences for the other Dutch security interests. However, as this event has violated the norm of state sovereignty, peaceful co-existence and peaceful conflict resolution, it compromises the foundations of the international legal order. Events such as the annexation of the Crimea may promote impunity and help set precedents that can increase feelings of insecurity and instability within international relations.

3.6.1 Violation of state sovereignty, peaceful coexistence and peaceful conflict resolution

Respecting state sovereignty is one of the most important rules of international relations. State sovereignty and peaceful conflict resolution can be severely threatened by military threats or unwanted foreign influence (hybrid operations). State sovereignty can be affected on different levels, going as far as the permanent occupation and/or annexation of a sovereign state. Even a temporary occupation, such as a blockade of strategic waterways and straits, can severely affect a state's sovereignty. Short-term hybrid operations using military assets on the territory of allied states are another example. In these events, perpetrators push the limits of state sovereignty in such a way that NATO or the EU are challenged and further escalation is possible.

The use of weapons of mass destruction is also considered a violation of state sovereignty and peaceful conflict resolution. Risks regarding CBRN proliferation in combination with an unstable arms limitation regime and the (potential) deployment of CBRN weapons are features of this.

Impact criterion International law	Most relevant risk categories
6.1 Violation of state sovereignty, peaceful coexistence & peaceful conflict resolution	Military threats
	CBRN proliferation
	Unwanted foreign influencing (hybrid operations)
6.2 Violation of human rights	CBRN proliferation
	Instability on European borders
	Terrorism
6.3 Violation of financial-economic systems	Trade contraction/disruption of international trade
	Pressure on security institutions
6.4 Violation of multilateral institutions	Unwanted foreign influence (hybrid operations)
	Military threats
	Pressure on security institutions
	CBRN proliferation

3.6.2 Violation of human rights

When crimes against humanity or war crimes are committed, these are considered a severe violation of human rights. Depending on the scale, and whether they are committed as part of a plan or policy, such violations can potentially cause maximum (catastrophic) impact on this criterion. Violations of human rights are considered as more severe if committed by a member of the United Nations Security Council. Violations of human rights are considered as catastrophic if nuclear weapons are used (CBRN proliferation).

War crimes committed by leaders to suppress resistance of the population against the ruling regime are another example. This type of event is further described in the risk category Instability on the borders of Europe, where destabilisation of a country within the MENA-region (Middle-East and North-Africa) is considered in one of the scenarios.

Terrorism in the form of acts committed by organisations linked to terrorist groups, such as ISIS, can violate human rights as well.

3.6.3 Violation of the financial and economic systems

In order to determine whether the financial and economic system is impaired, the functioning of the World Trade Organisation (WTO) and organisations such as the International Monetary Fund (IMF), World Bank, and the Organisation for Economic Cooperation and Development (OECD) have been studied. The analysis shows that this impact criterion can be seriously affected a number of times, which implies that decision-making and other processes become paralysed, or that alternative organisations are set up. However, no risks have been identified that indicate that the system as a whole will collapse.

Scenario Trade war

This scenario describes a situation where a trade war between the US and China escalates, affecting the EU as well. In this scenario, multiple import tariffs and other trade-restricting control measures are implemented by the two superpowers and multilateral treaties and agreements (WTO) are ignored. The US even threatens to leave these treaties all together.

In the event of a trade contraction or disruption of international trade due to, for example, an escalating trade war, international decision-making can become paralysed. The same applies to a situation in which tensions within the EU increase (pressure on security institutions). European cooperation is generally robust, however, if major unexpected events coincide, such as a chaotic Brexit in combination with strongly increasing internal tensions around budgets in the Eurozone, risks can become significant.

Other risks that can affect the financial-economic system involve threats in relation to international tensions that pose a threat to supply lines (flow security). For instance, increasing (military) tensions in the South China Sea could lead to economic blockades and facilitate the development of new (parallel) institutions in Asia. This is not expected to lead to a collapse of the existing system because China also benefits from thriving trade with western countries.

In addition, risks that affect the financial-economic system can emerge due to increasing power and influence of China in western economies. This is a long-term development that can have major consequences for both the financial-economic system and the functioning of multilateral institutions.

3.6.4 Violation of multilateral institutions

Given current international developments and scenarios, risks that may affect multilateral institutions, such as the United Nations, the EU and NATO can occur. A hybrid operation with a short-term border crossing or even temporary annexation (military threat) of a NATO member state can also paralyse NATO. Such events may arise if the unity of the alliance comes under stress as differences between member states' interests become apparent.

It is also clear that if NATO or EU internal tensions increase and escalate, processes such as decision-making may be paralysed (pressure on security institutions). If tensions between member states increase to such an extent that, for example, a member state withdraws from NATO, the alliance will be very seriously affected. However, although threatening to leave may be realistic, actually withdrawing is only moderately likely.

Multilateral institutions include international treaties and agreements as well. For example, the important system of treaties and agreements regarding CBRN non-proliferation that in recent decades, by trial and error, have regulated the prohibition and proliferation of CBRN weapons. This system has come under pressure because the future of the INF Treaty (Intermediate-Range Nuclear Forces) has become precarious, it is unclear whether the New START Treaty (Strategic Arms Reduction Treaty) will get a follow-up, and the Non-Proliferation Treaty has been unable to further prevent proliferation of nuclear weapons. The U.S. withdrawal from the Iran nuclear deal in April 2018 (JCPOA), and the potentially serious consequences thereof for the Middle East region, contribute to the erosion of the international system of treaties and agreements.

3.7 Reflection

This chapter has described the most important risks related to the six national security interests. The emphasis has been on risks with the highest impact on the security interest concerned. There are several risk categories that have a serious impact on multiple security interests. This is shown in Table 5. The table portrays the scenarios in which a high impact (D or E) was scored multiple times.

A number of observations follow from this table. Risks with a physical impact, such as floods and a severe influenza pandemic, emerge as risks that very seriously affect multiple security interests. This is particularly true in the case of a (worst-credible) coastal flood (scenario: flood – severe (sea)). Such large-scale natural disasters can lead to a long-term failure of critical infrastructure with consequences for daily life, large numbers of casualties, and (possible) lack of basic needs. Also, large parts of the territory will be unusable or inaccessible for a long period of time. They also lead to major economic consequences (costs) and the vitality of the economy will be affected (due to the possible long-term nature of the event). Because of this, a combination of national security interests is impaired: territorial, economic, physical and socio-political.

There are also a number of risks from the theme Threats to international peace and security that very seriously affect national security via multiple criteria. This clearly applies to the scenario "annexation of a NATO member state".

Furthermore, risks within the category "Pressure on security institutions (NATO, EU)" cause (very) serious effects on multiple national security interests and impact criteria; in particular the International system of norms and rules, Social and political stability, the encroachment on allied territory and the economy. This risk mainly concerns escalation of internal tensions within NATO or the EU.

Military threats – an explanation

Although tensions are increasing along NATO's borders, it is very unlikely to unlikely that annexation of physical territory will become an issue. It is more likely that activities will lead to discussions on whether a state's sovereignty is being violated or not. For instance, military deployments of foreign special forces that may lead to campaigns of disinformation showing ambiguous intentions.

Table 5. Scenarios with a high impact on multiple criteria

Risicocategorie	Scenario	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	3.2	4.1	5.1	5.2	5.3	6.1	6.2	6.3	6.4
Human infectious diseases	Influenza pandemic - severe					E	E					E						
Extreme weather	Extreme weather							D				D						
Flood	Flood - severe (sea)	E		D		E	E	E	E		E	E						
Flood	Flood (river)	D							D			D						
Disruption of critical infrastructure	Disruption of power supply							D				D						
Disruption of critical infrastructure	Cascading effects of power supply failure							E	D			E						
Disruption of critical infrastructure	Satellite disruption							D	D									
Nuclear disasters	Nuclear disaster (the Netherlands)	E							D									
Disruption internet	IP network failure (ICT)								D			D						
Unwanted foreign influencing (hybrid operations)	Challenging and paralyzing NATO and EU		D												D			
Trade contraction/ disruption international trade	Schock to international trade system								D	D								
Trade contraction/ disruption international trade	Schock to international trade system (permanent)								E	E								
Trade contraction/ disruption international trade	Trade war								D	D								
Destabilisation of the financial system	Destabilisatie financieel systeem								D	D								
Military threats	Annexatie NAVO lidstaat		E	D	E										E			
proliferation of CBRN weapons	CBRN - Nucleair														D	E		
proliferation of CBRN weapons	Internal tensions NATO		D											D				D
proliferation of CBRN weapons	Internal tensions EU		D						D	E								D

4 Risks seen from a likelihood perspective

The previous chapter described the main results concerning impacts on the six national interests, emphasising risks with a substantial impact. This chapter looks at the risks which are most likely to occur.

Similar to the impact assessment, five severity classes are used to classify the likelihood of risks, ranging from very unlikely (A) to very likely (E). The following three characterisations are used to classify likelihood:

- Quantitative scales for risks that can be statically or probabilistically analysed;
- Qualitative scales for malicious threats (based on aspects such as conceivability, indications and vulnerabilities);
- Qualitative scales for other risks.

The table below explains how the different classes are classified.

Table 6. Scales used for likelihood

Class; general qualitative approach	Quantitative approach	Qualitative approach malicious
Very unlikely	Less than 0.05%	No specific indications; inconceivable
Unlikely	0.05 to 0.5%	No specific indications; somewhat conceivable
Somewhat likely	0.5 to 5%	No specific indications; conceivable
Likely	5 to 50%	Indications; very conceivable
Very likely	More than 50%	Specific indications that scenario is going to happen

4.1 Overview of risk categories with a high likelihood

The table below shows the risk categories with a high likelihood of occurrence (D or E). The risk categories and their possible manifestations are further discussed below.

Cyber threats: digital sabotage and cyber espionage
The analysis shows that one of the scenarios concerning cyber threats has the highest likelihood class (very likely). This concerns the risk of digital sabotage through disruption by collateral damage, which has taken place several times recently. Examples are WannaCry and NotPetya (both in 2017). The likelihood that such an incident will take place again in the next 5 years is estimated at more than 50%.

The analysis also shows that, besides sabotage, cyber espionage is also a likely risk to national security. For example, a state actor could compromise the secure email system of a (public) organisation and subsequently monitor its email traffic. This type of espionage has occurred in the past. Here, an important question is how long the act of espionage has been able to take place undetected.

Table 7: Risks with high likelihood (score D or E)

Theme	Risk category
Cyber threats	Digital sabotage (disruption via collateral damage)
	Cyber espionage
Subversion of the democratic constitutional system	Subversive enclaves, both criminal as well as ideological
	Unwanted foreign influence (via hybrid operations) by different foreign actors with different purposes
	Unwanted foreign interference with a foreign actor influencing diaspora communities.
Threats to international peace and security	Instability on European borders with destabilisation of a North African country
Threats to public health and the environment	Animal disease and zoonosis, with an animal disease having a higher likelihood
	Human infectious disease, influenza pandemic
Natural disasters	Extreme weather
Disruption of critical infrastructure	Disruption of critical infrastructure, such as power supply failure
Violent extremism and terrorism	Terrorism, violent loner
Financial and economic threats	Threat to hub function and supply lines of the Netherlands (flow security)
	Trade contraction/ disruption of international trade, shock to system of international trade

Subversion of the democratic system and open society

It is also likely that risks analysed in relation to the subversion of the democratic system will occur. Subversion can take place from the inside as well as the outside. From the inside, this can be done through the formation of an enclave, which can have different origins, for example, criminal groups actively pursuing the creation of 'no-go areas'. Parallel communities can also be formed on an ideological basis. In time, this could affect the authority of the Dutch government.

Scenario Subversion by state actors via hybrid operations

After two major cyber hacks affecting the payment of unemployment benefits and causing a power outage, Dutch citizens are very concerned about cyber safety. This has affected the authority of the Dutch government. Russia takes advantage of the increased polarization and whips up the unrest on social media.

Foreign state actors can subvert our society in different ways. There is a constant international competition going on in which covert hybrid operations are increasingly used. Hybrid operations exploit vulnerabilities in our social and political system. There are also signs that unwanted foreign interference with diaspora communities in the Netherlands is taking place (in various forms) and could do so in the future.

Instability on the borders of Europe

From the perspective of international security, there is political instability in countries surrounding the European Union. Taking current tensions and fragility into account, it is likely that countries on the borders of the EU will further destabilise. This could be accompanied by conflicts, migration, crime and violent extremism in (certain countries in) Europe. The cohesion of the EU, and in particular the Schengen system, could be (further) compromised. The question is whether the Netherlands and the EU could cope with such a crisis with political tensions on a national and European level.

Infectious diseases and animal disease
Based on the number of (serious) influenza pandemics during the last 100 years and their frequency, it is likely (5 – 50 %) that there will be an influenza pandemic in the next couple of years. It is however unknown whether this will be a severe or a mild type of influenza. In case of a severe influenza type, the number of victims will be very large. There will be major pressure on the medical sector and daily life will be totally (catastrophically) disrupted. Societal consequences will be especially large if a high portion of the population becomes ill.

An animal disease outbreak (like Foot-and-Mouth Disease (FMD) or African swine fever) remains likely in the Netherlands, despite precautionary measures. This is due to the large number of (domestic) animals and global animal transport. The impact will be of a mainly economic nature with the potential of severely affecting a specific sector.

Extreme weather
There are different kinds of extreme weather, such as black ice, hail, a snowstorm or a very severe storm. Extreme weather conditions are likely to occur. Snowstorms and hail will take place less frequently due to climate change whilst the opposite applies to (very) severe storms.

Disruption of the power supply
Given the current situation, it is likely that the power supply will be disrupted in the coming years. Our current energy supply relies strongly on fossil fuels. Sustainable alternatives are emerging, but it is not yet clear what this means for the reliability and safety of our future energy supply. The production of electricity will, for example, be more vulnerable to extreme weather if the number of wind turbines and solar cells increases. Subsequently, a disruption can become more likely.

Extremism and terrorism
A variety of actors with different manifestations (transnational networks, organisations, small cells and loners) could commit both small and major terrorist attacks in the Netherlands. At the moment, the greatest threat originates from jihadist terrorism. There are (still) people in the Netherlands who are involved with terrorist activities based on jihadist ideology. A potential threat for the coming years is the release from prison of jihadists who persist with their ideology. A terrorist attack in the Netherlands is seen as very likely and there are (some) indications that it might occur (in different forms). It cannot be excluded that other politically or ethnically motivated forms of terrorism will become more important in the coming years besides attacks inspired by a jihadist ideology.

Scenario Disruption of critical infrastructure

In a large part of Europe (also in the Netherlands), the power supply fails because of a decrease in frequency. Due to complications it takes 24h before the system works again. The impact on organizations and citizens is high, because different processes are (partly) out of order (such as public transport (train, tram, subway), medical home equipment, payment services, fuel stations, communications (fixed, mobile, internet), shops are closed).
The assumption is that most parts of the vital infrastructure (using emergency power systems) is not disrupted.

Financial and economic threats
It is likely that in the coming years a shock to the system of international trade or a decrease in trade volume will occur, taking into account previous cases in combination with the current financial-economic context and developments. The duration of such a shock is an important factor. The financial damage and consequences for the vitality of the system will be very serious if it takes a long time to recover.

In addition, international tensions can lead to a disruption of the supply lines of the Netherlands in the coming years, for example, by blockading strategic waterways. The Iranian threats to blockade the Strait of Hormuz have for some time led to international concern.

4.2 Reflection

The above shows that almost all the themes contain risk categories with a high degree of likelihood. Only the Major accidents theme is an exception. Events that may impact national security within the theme of Major accidents have a low likelihood of occurrence (very unlikely).

The risk categories which are mentioned here do not for the most part represent the largest risks in terms of impact within their respective themes. On the other hand, risks with a very high impact, such as floods, are very unlikely. In general, risks with a very serious or catastrophic impact are not very likely. There are however exceptions. A very severe influenza pandemic (human infectious disease) is likely as well as disruptive to society.

Chapter six looks at the combination of impact and likelihood.

5 Connecting links and interdependencies

The previous chapters have described the main results of the analysis of the themes and risk categories considered in this risk assessment. This was done from both the perspective of impact on the national security interests (chapter 3) and the likelihood of occurrence (chapter 4). In order to gain better insight into the risks, however, it is important to look beyond solely an overview of risks most seriously affecting interests and risks most likely to occur. Therefore, this chapter describes the results of the analysis from an integrated perspective. The most important interdependencies and links within and between themes and risk categories are described in the following paragraphs.

5.1 Risks with physical impact

Risk categories that fall within the themes Major accidents, Threats to public health and the environment, and Natural disasters, predominantly manifest themselves in terms of physical impact. Unsurprisingly, such risks can in particular severely affect the national security interests Physical safety (deaths, injuries; sick; basic needs). Territorial security can be impaired and daily life disrupted, especially in the case of serious nuclear disasters or floods. Furthermore, as is the case for all risks that have been analysed by the ANV, (serious) economic damage may occur when an incident occurs.

An important link between the previously mentioned risk categories are the reciprocal cascading effects, i.e. the effects of one risk can cause or aggravate another risk. For example, it is conceivable that installations could fail due to natural disasters (such as extreme weather). The failure of a nuclear power plant in Fukushima, as a result of a natural disaster, is an extreme example of this. Similarly, a concurrence of different circumstances can lead to certain risks reinforcing each other. For example, when peak discharge from the major (Dutch) rivers coincides with a western storm, the risk of a river flood increases.

There is also a clear relation between the aforementioned themes and the theme Disruption of critical infrastructure. For example, a natural disaster or a major accident can damage or disrupt critical infrastructure. This also has effects on the impact scores per national security interest. The type and magnitude of the impact of such incidents are related to the very nature of the disrupted vital processes. For instance, certain vital processes are strongly linked to the availability of basic needs (energy, drinking water) and continuity of daily life. In the same way, a disruption of critical infrastructure could cause or aggravate the effects of a major accident or natural disaster. For example, a disruption of the vital process of managing water quantities could result in a flood. Due to the digitalisation of vital processes, digital sabotage is also an aspect to take into account in analyses.

5.2 Cyber threats and critical infrastructure

The themes Cyber threats and Disruption of critical infrastructure have a different nature, as they can be both goals and means. Furthermore, in contrast to the aforementioned themes that predominantly emanate from accidents, risks within the Cyber threats and Disruption of critical infrastructure themes can manifest themselves as a result of both non-malicious and malicious behaviour. Disruption of critical infrastructure, for example, can be caused by technical failure (complexity in the system), but also as part of a cyber-attack (when systems are hacked). There is also a strong link between the two themes, in particular due to the far-reaching digitalisation of society. It is clear that critical infrastructure can be disrupted digitally (cyber-attack or technical disruption of digital systems). On the other hand, disruption of critical infrastructure can have an aggravating effect on risks within the cyber domain.

Complexity, interrelatedness and digitalisation of critical infrastructure can pose additional risks. Since critical infrastructures are often interdependent, the (technical) failure of one facility can lead to a variety of cascading effects. The possible consequences within these increasingly complex systems can be unforeseen. This complicates decision-making about mitigating measures when defects are identified, since intervening in the process may increase rather than alleviate the impact. The digitalisation of critical infrastructure also creates risks in terms of sensitivity to digital sabotage and cyber espionage. In this regard, it is also important to take into account aspects of Economic security. There are increasing concerns about the extent of dependency on foreign suppliers of hard and software used in critical locations of our infrastructure.

When we link the issues described in this section to cybersecurity and the risks of hybrid warfare, additional aspects arise. If an actor intends to damage national security, cyber capabilities can be a means to disrupt society, for example, via sabotage, criminal activities, espionage or dissemination of disinformation. It is difficult to determine who is behind an attack and thus to attribute it to a specific perpetrator. Therefore, thresholds for using cyber as a means are low. Although a cyberattack may trigger article 5 of the NATO Statute, the deterrent function of this is limited. Furthermore, not only may a targeted cyber action on the Netherlands cause damage, but cyber actions elsewhere in the world may have (random) effects on our country as well (collateral damage).

5.3 Risks of a malicious nature

Many (other) risks can be exacerbated in hybrid operations, especially if a crisis is ongoing. Hybrid operations often respond to existing societal discussions or crisis, such as public debates, elections, tensions within the EU, and economic developments. Within the cyber domain, dissemination of disinformation is a suitable means to do so. Technological developments in the cyber and information domains ensure that such means of subversion are very accessible. Hybrid activities are difficult to control by the initiating actor though. They can lead to increasingly escalating negative developments, such as increased polarisation or extremism.

Polarisation and extremism are breeding grounds for (a number of) other risks and threats that may manifest themselves as a consequence of malicious behaviour. Both state and non-state actors can initiate incidents. This applies in particular to risk categories within the themes Violent extremism and terrorism, Subversion of the democratic constitutional system, and Threats to international peace and security. An impact on the democratic constitutional system can be expected, including its underlying and shared values, but the International system of norms and rules and our Territorial security (in particular our international position and territory of our allies) may be impaired as well.

There is a clear link between ‘malicious risks’ and the themes Disruption of critical infrastructures and Cyber threats. For example, extremists and terrorists could aim to destroy critical infrastructure as part of their (subversive) activities. Within the cyber threats category, cyber should mainly be seen as a means in this regard. Extremists and terrorists are very active in the cyber domain. They use the digital infrastructure to communicate with each other and to disseminate their hatred and undemocratic messages. Furthermore, they choose cyberattacks as their weapon of choice, which potentially cause physical and/or economic damage (as well).

Increasing polarisation within society could undermine an open society and, at the same time, be a breeding ground for both non-violent and violent extremism and even terrorism. As stated above, several (non-)state actors may respond to such developments. They may or may not use hybrid operations to do so. Rather than it being an issue affecting the Netherlands alone, developments that facilitate polarization are an international phenomenon. The formation of anti-government sentiments is correlated to such developments. Anti-government extremism is also seen in relation to the EU and other (international) institutes. Certain decisions and changes in these institutes may influence the (extent of) extremist activities. On the other hand, large-scale extremist or terrorist actions can endanger international peace and security and thus lead to an international (political) response.

Several links between the risks and threats that emerge from an incident resulting from a malicious act can be identified as well. The first concerns the relation between undermining of the democratic constitutional system and international developments in which tensions between the great powers and within security institutions increase. Within the (international) competition for power, means are deployed that undermine sovereignty and the position of power of states. These may arise, for example, as 'long arm' activities or hybrid operations. In time, this can lead to (rising) tensions between population groups. Recent analyses emphasize the (digital) threat emanating from state actors. This threat focusses on the subversion of democratic constitutional society, on acquiring strategic information via espionage and disruption, or even on sabotage of critical systems. Furthermore, the interests of individual countries (and the norms and values on which their societies are based), are considered to be increasingly important. This is one reason why multilateral, institutional collaboration is coming under pressure.

5.4 Internal and external security

Within the framework of the internal-external security nexus, a connection between cyber and hybrid warfare clearly stands out in this national risk assessment. This connection could be amplified if a military threat evolves into a military conflict, especially if the Netherlands is somehow involved. For example, if a military conflict arises between a NATO member state and another state actor, via Article 5 of the NATO treaty (collective defence), other member states would become involved as well. It is likely in such a case that other hybrid instruments, including cyber, will be deployed in addition to traditional military activities. A tense situation could also occur if international conflicts escalate to the extent that Article 5 is not yet, but could be invoked. It is conceivable that the Netherlands, being a transit country for other NATO member states, is considered an important (cyber) target early on in such conflicts.

International tensions may also lead to internal tensions and the reinforcement of differences of opinion within security institutions such as NATO and, considering the instability around Europe, the EU. For example, if an 'Article 5 situation' arises, this would raise the question of which actions NATO would undertake. This also applies to situations where NATO or EU member states are challenged by short-term operations of foreign actors. Further examination of the internal-external security nexus reveals tensions between great powers, such as disputes relating to the South China Sea. International, political and economic tensions (such as an escalating trade conflict between the United States and China, which also affects the EU and thus the Netherlands) can impair national security (Economic security and International system of norms and rules). Another manifestation of international tensions concerns pressure on agreements relating to the non-proliferation of weapon systems.

Although financial and economic threats predominantly affect the national security interest Economic security (both costs and vitality), it is possible to identify a link with the Threats to international peace and security theme. Due to the international character of the financial and economic threats, manifestations of international tensions (such as an escalating trade war or tensions in the EU) may have consequences for both financial and economic risks and the International peace and security theme. Disruption of the world trade system could impact on international peace and security, especially if conflict resolution systems established to resolve issues are not used or respected. On the other hand, states announce trade barriers and pursue protectionism under the guise of 'national security'. In the case of increasing tensions, trade barriers are frequently used means of exerting pressure. This poses a threat to the international financial-economic system.

5.5 Reflection

Chapters 3 (impact on the national security interests) and 4 (likelihood of occurrence) together form a risk assessment of the most important risks related to various disasters, crises and threats with a potential disruptive effect on our society. Although cascading effects are implicitly considered, in particular causal consequences in the case of a risk actually occuring, the text in this chapter also reveals the existence of strong links and interdependencies between different risks. This implies that changes in threats related to one area can also have consequences on another area. Some threats that have been considered separately also form the trigger for the occurrence of other risks. In particular, cyber dependencies and critical infrastructure play a part in virtually all scenarios in one way or another. Hybrid operations also contain aspects that influence or aggravate almost all other risks. This all occurs against a backdrop of increasing international tensions.

6 Conclusion

Commissioned by the National Coordinator for Security and Counterterrorism (NCTV), the National Network of Safety and Security Analysts (ANV) has performed a National Risk Assessment to provide insight into the most important risks for Dutch national security in the coming five years. The results provide input for the development of the National Security Strategy (NVS).

During risk mapping, both the chance of occurrence (likelihood) and the possible consequences (impact) of particular risks have been taken into account. The six national security interests and their various impact criteria have been used to indicate the impact of risks. In addition to impact and likelihood, relevant links and interdependencies have been taken into account.

Table 8. Overview of risks with greatest impact per security interest

Territorial security	Physical safety	Economic security	Economic security	Social and political stability	International legal order
• Floods • Nuclear disaster • Digital sabotage • Cyber espionage • Unwanted foreign influence (hybrid operations) • Military threat (NATO) • Tensions within security institutions	• Floods • Major accidents (nuclear disaster, chemical incidents, transport accidents) • Infectious diseases (influenza pandemic, bird flu) • Terrorism (large scale) • Disruption of critical infrastructure • Extreme weather • Wildfires	• Floods • Nuclear disaster • Disruption of critical infrastructure • Destabilisation of the financial system • Trade contraction/ disruption of international trade • Criminal interference	• Floods • Wildfires	• Floods • Disruption of critical infrastructure • Human infectious diseases (influenza pandemic) • Criminal interference • Cyber espionage • Violent extremism • Non-violent extremism • Creation of enclaves • Unwanted foreign interference • Terrorism (large scale) • Security institutions under pressure • Unwanted foreign influence (hybrid operations)	• Military threat • CBRN proliferation • Unwanted foreign influencing (hybrid operations) • Instability of European borders • Terrorism (large-scale) • Trade contraction/ disruption of international trade • Security institutions under pressure

6.1 Risks: impact, likelihood and the combination of impact and likelihood

In the analysis, risks with the greatest impact on the national security interests (chapter 4) and risks with the highest likelihood of occurrence (chapter 5) have been described separately. Here, the results of both are briefly reiterated before the combination of impact and likelihood is described.

Risks with a great impact on national security

The analysis describes to what extent the impact criteria are affected by the various risks. By describing the results from the perspective of the criteria, it becomes clear which risks can affect one or more national security interests.

Table 8 provides an overview of the risks with the greatest impact per national security interest. This is an enumeration, not a ranking. It is clear that the risks with the greatest impact vary per security interest.

Concerning risks that seriously affect multiple interests, physical risks appear to have the greatest impact on overall national security. For example, floods or influenza pandemics can have a disruptive effect on society because they affect multiple interests. Such disasters can cause a large number of victims, may result in part of the territory being unavailable to use for a long(er) period of time, lead to a lack of basic necessities of life and seriously disrupt daily life. The table below provides an overview (top 8) of the scenarios that can most seriously affect national security.

Risks with a high likelihood

As described in chapter 4, an important observation is that the risks with the greatest impact also have a (very) low likelihood of occurrence. An influenza pandemic is the exception, because a serious variant is both likely and may have a very serious impact on national security.

The table below provides an overview (top 8) of the scenarios with a relatively high likelihood of occurrence.

Table 9. Scenarios with the greatest impact on national security

Risk category	Scenario
Flood	Flood – severe (sea)
Human infectious disease	Influenza pandemic - severe
Disruption of critical infrastructure	Cascading effects of power supply failure
Trade contraction/ disruption of international trade	World trade system shock
Nuclear disaster	Nuclear disaster in the Netherlands
Pressure on security institutions	Internal tensions in the EU
Flood	Flood (river)
Military threats	Annexation of a NATO member state

Table 10. Scenarios with a high likelihood of occurrence

Risk category	Scenario
Digital sabotage	Cyber disruption – collateral damage
Cyber espionage	Cyber espionage (affecting government)
Instability of European borders	Destabilisation of a North African country
Unwanted foreign influence	Hybrid operations by Russia
Unwanted foreign interference	Influencing diaspora communities (long arm activities)
Subversive crime	Subversive enclaves
Threats to the hub function and supply lines of the Netherlands (flow security)	Strategic strait blockade
Animal disease and zoonosis	Animal disease outbreak (foot and mouth disease)

Table 11. Risks on the basis of impact and likelihood of occurrence

Risk category	Scenario
Human Infectious diseases	Influenza pandemic - severe
Unwanted foreign influencing	Hybrid operations Russia
Digital sabotage	Cyber disruption – collateral damage
Trade contraction/ disruption international trade	World trade system shock
Subversive crime	Subversive enclaves
Unwanted foreign interference	Influencing diaspora communities (long arm activities)
Instability on European borders	Destabilisation North African country
Extreme weather	Extreme weather
Disruption of critical infrastructure	Cascading effects of power supply failure

The risks with a high likelihood are mainly those with a malicious character: cyber threats, subversion, unwanted interference and influence from foreign powers. Risks related to international developments that can affect our national security, such as instability on the borders of Europe or economic disruption of the world trade system, have a high likelihood of occurrence. These risks predominantly affect national security interests that are linked to the democratic constitutional system and the way this system is set up as well as the International legal order.

Risks: combination of impact and likelihood
Both impact and likelihood need to be taken into account in order to make assumptions about the greatest risks for our national security. From the analysis, it follows that the scenarios in table 11 are the ones posing the greatest risks when impact and likelihood scores are combined.

6.2 Links and interdependencies

In addition to the categorisation of risks based on impact and likelihood, links and interdependencies between risks also play an important role in identifying dangers which can disrupt society.

The most important links and interdependencies between risks have been analysed to gain more insight into the relationships between the various risks. It can be concluded that Disruption of critical infrastructure, Cyber threats and Hybrid operations contain aspects that influence or have an aggravating effect on almost all the other risks. Disruption of critical infrastructure, for example, can aggravate risks such as floods or major accidents. On the other hand, forces of nature or a cyberattack can also cause a critical infrastructure disruption. There is a strong interrelatedness between the risks to critical infrastructure and the other risks. Furthermore, vital processes are ever more dependent on each other and interrelated, and networks are getting increasingly complex. This implies that it is not always clear which and where cascading effects may occur during a disruption. Digitalisation also brings with it vulnerabilities and dependencies. For example, risks of digital sabotage, infiltration and (cyber) espionage.

Cyber can be deployed to achieve sabotage, criminal activities or espionage. The use of cyber within hybrid operations also emerges from the analysis. Via hybrid operations, existing societal discussions or crises (such as public debates, elections or tensions in the EU) can be exacerbated in an attempt to influence and subvert society. The analysis shows that (covert) interference and influencing activities from foreign powers (via hybrid operations) occur and have the potential to seriously disrupt the political and social system of the Netherlands. Furthermore, increasing international tensions have an impact on multiple risk categories that can affect national security. This also emphasizes the strong interdependencies between internal and external security, which is most clearly manifested in the theme Threats to international peace and security.

6.3 Greatest risks to national security

The question regarding the greatest risks to national security in the next five years can be answered in different ways, depending on the importance attached to different issues. Based on the national risk assessment, the following can be stated:

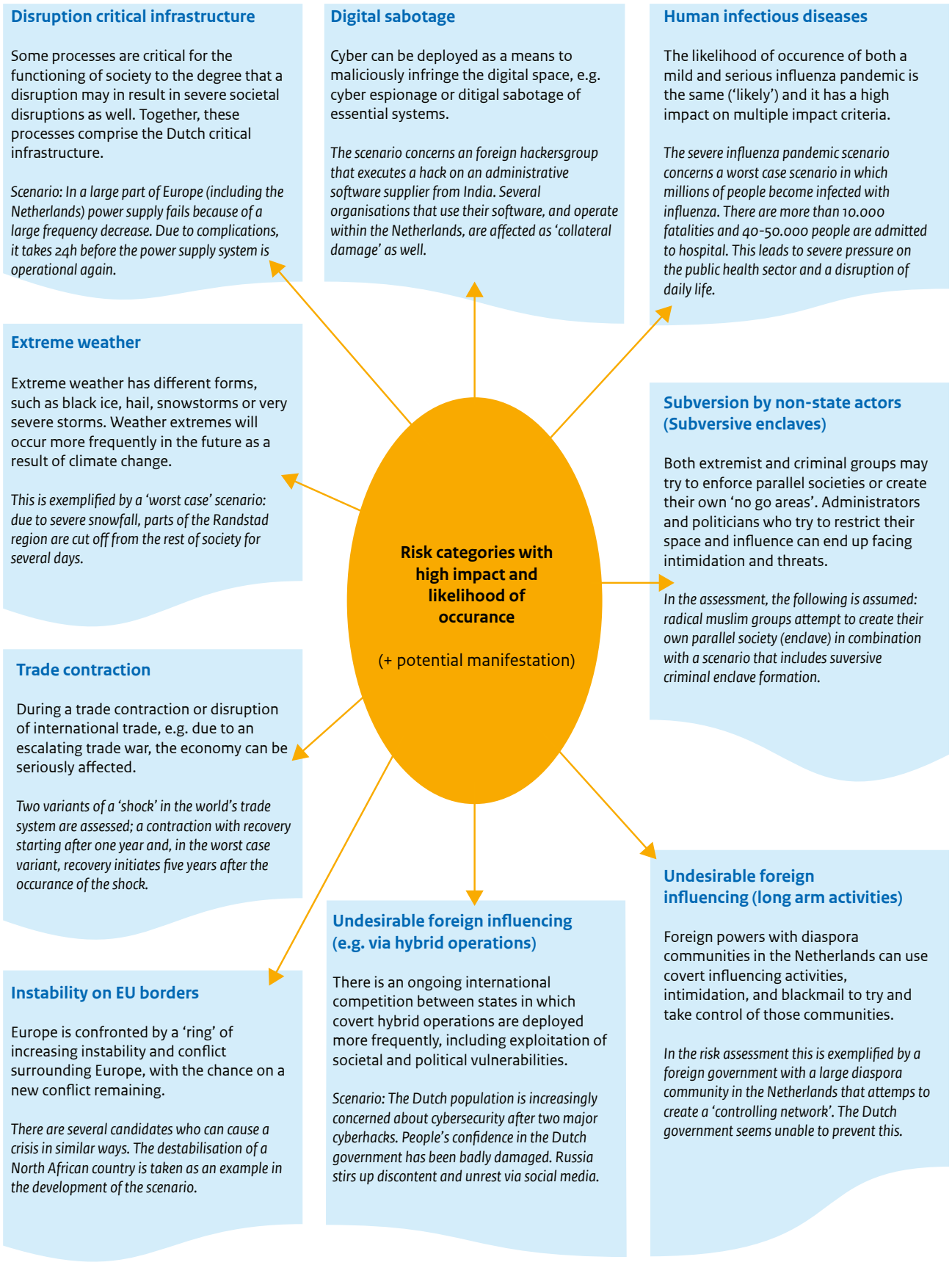
- *Impact*. Physical risks, such as a flood, have a very serious impact on several security interests and thus on our national security. These risks predominantly have an effect on Physical safety (fatalities and injured), disruption of daily life and economic costs. There is also a clear connection with the disruption of critical infrastructure. The likelihood of such large-scale physical disasters is low.

- *Likelihood*. "Malicious threats" related to cyber security, subversion of the democratic constitutional system and international peace and security deserve attention. The occurrence of these risks is (very) likely and in some cases (there are signs that) they are already happening. However, the impact of such risks is lower than the aforementioned physical risks. Means are being deployed to destabilise and undermine our society. Furthermore, current international developments are putting security institutions, such as NATO and the EU, under increasing pressure, both from outside and from within.

- *Interdependencies.* Cyber threats, hybrid operations and the increasing digitalisation and complexity of critical infrastructure influence other risks and can, therefore, have an aggravating effect on threats to national security.

- *Combination of impact and likelihood*. Based on the results of the analysis, an overview was made of risks that have both a high impact and a high likelihood. Figure 3 on the next page schematically depicts and briefly explains the top 9 risks based on impact score and high likelihood. The threats that have the most interdependencies with other risks are also (partly) included in this scheme.

Figure 3 Schematic overview of top 9 risks based on impact and likelihood of occurrence



7 References

ANV (2016). National Risk Profile 2016.

ANV (2018). Horizon scan Nationale Veiligheid 2018. [Horizon scan National Safety and Security 2018]

ANV (2018). International Legal Order as the sixth National Security Interest.

ANV (2019). Leidraad Criteria Geïntegreerde risicoanalyse. [Guideline Criteria National Risk Assessment]

Overview of theme reports (that include further references)

- Theme report Threats to public health and the environment
- Theme report Cyber threats
- Theme report Financial-economic threats
- Theme report Violent extremism and terrorism
- Theme report Threats to internationale peace and security
- Theme report Natural disasters
- Theme report Subversion of the democratic constitutional system and open society
- Theme report Disruption of critical infrastructure
- Theme report Major accidents

Annex 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. Since then, the ANV has been tasked by the Ministry of Security and Justice with the drawing up of the annual National Risk Assessment on behalf of the National Steering Committee for National Safety and Security (SNV). In 2014, the ANV was tasked with producing the National Risk Profile.

The ANV consists of a permanent core of six organisations surrounded by a network (the Ring) of organisations, such as knowledge institutions, research agencies, civil services, safety regions, critical infrastructure sectors, private companies and consultancy firms, which are engaged in the production of the NRP and underlying studies, depending on the knowledge requirements. The permanent core consists of:

- The National Institute for Public Health and the Environment (RIVM)
- The Research and Documentation Centre (WODC), Ministry of Security and Justice
- The General Intelligence and Security Service of the Netherlands (AIVD)
- The Netherlands Organisation for Applied Scientific Research (TNO)
- The Netherlands Institute of International Relations 'Clingendael'
- The International Institute of Social Studies (ISS) of the Erasmus University Rotterdam

The core organisations possess wide-ranging, multi-disciplinary expertise and therefore, collectively span the National Security work field. This structure guarantees the NRP's All Hazard approach as well as the uniformity of the methodology and cross-disciplinary analysis.

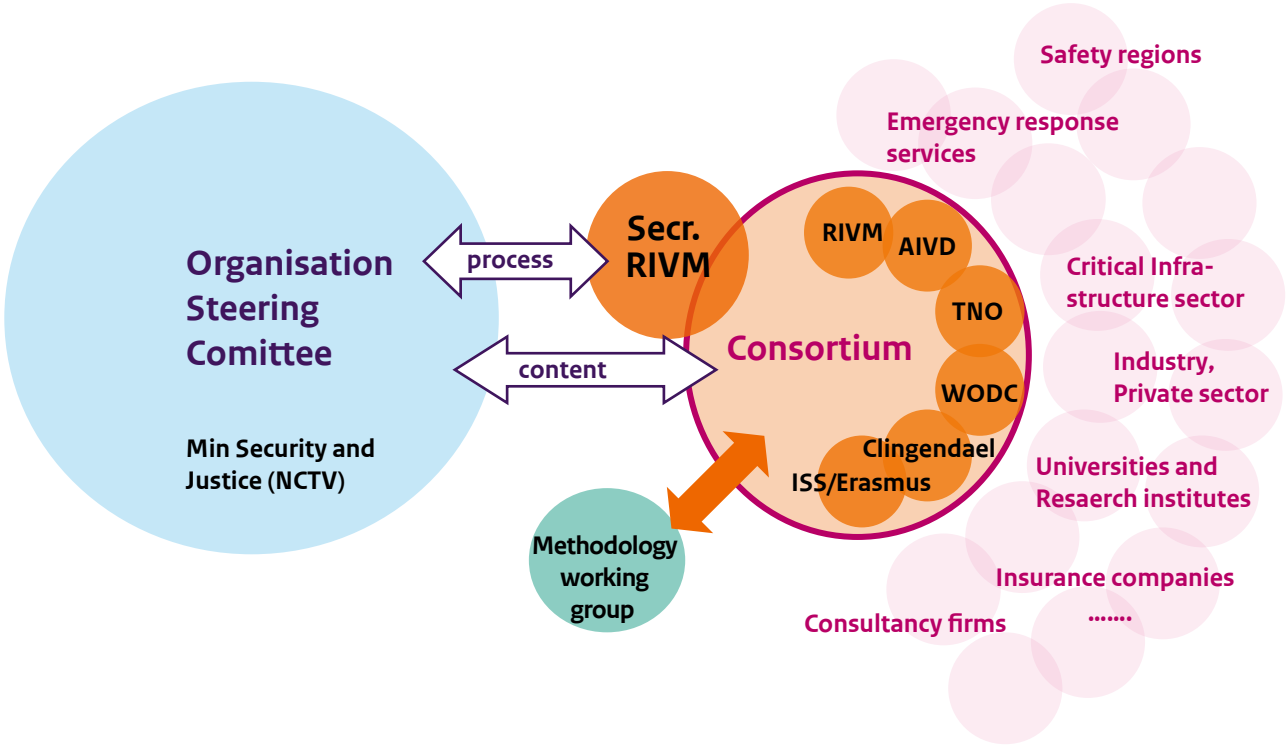
The six core organisations, united in the Task Group, share responsibility for the quality of the contents of the NRP and other products. Specific, supplementary expertise is provided by the other organisations in the network. The organisations in the core and the network ensure that experts and analysts are made available to sit on working groups, which are temporarily convened to undertake the various activities. There is also a supporting secretariat (the ANV Secretariat) made up of a general secretary, working group coordinators, and project support personnel, who provide process management, progress monitoring, and support for the creation of the NRP and other products. The ANV Secretariat acts as the fixed point of contact for the SNV, the IWNV (Interdepartmental National Security Working Group), and the associated departments and also supports the Task Group and the working groups, and directs and monitors the process. The ANV Secretariat is housed within the RIVM.

The methodology working group was set up in 2007. This working group has developed and maintained the NRA methodology. During the production of the NRA 2019, members of the working group have been involved in the development of several new impact criteria and facilitated several expert sessions.

A diagram of the organisational structure is shown in figure 4.

Figuur 4 A diagram of the organisational structure

National Safety and Security Analyst Network



The National Network of Safety and Security Analysts (ANV)

Published by:

The National Institute for Public Health and the Environment (RIVM)
Research and Documentation Centre (WODC)
General Intelligence and Security Service of the Netherlands (AIVD)
The Netherlands Organisation for Applied Scientific Research (TNO)
The Netherlands Institute of International Relations 'Clingendael'
Erasmus University Rotterdam, Institute of Social Studies (ISS)

July 2019

011559