National *Risk Profile* 2016

An All Hazard overview of potential disasters and threats in the Netherlands

The National Network of Safety and Security Analysts

National Risk Profile 2016

An All Hazard overview of potential disasters and threats in the Netherlands

The National Network of Safety and Security Analysts

Colophon

The National Risk Profile (NRP) has been compiled by the National Network of Safety and Security Analysts on the instructions of the National Steering Committee for National Safety and Security (ANV).

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)

Published by:
National Institute for Public Health and the Environment
Postbus 1 | 3720 BA Bilthoven
The Netherlands
www.rivm.nl

Contents

Summary

The National Safety and Security Strategy and the National Risk Profile

The National Risk Profile (NRP) provides an overview of the risks of various disasters, crises and threats with a possible destabilising effect on the Dutch society. The NRP is part of the National Safety and Security Strategy which the government uses to investigate which disasters, crises or threats can jeopardise our national security and what can be done about them.

The NRP also describes the capabilities which are available to manage the risks and identifies the link and the mutual effects between various risks. As a consequence, the NRP constitutes a basis for the next step, which is the capability analysis. The capability analysis involves an investigation to establish which capabilities may have to be strengthened or developed and what kind of measures are required. That falls outside the scope of the NRP.

Societal disruption exists if one or more of the five national security interests is seriously compromised:

In order to determine the seriousness (impact) of a potential disaster or crisis, these national security interests have been developed into a number of criteria. In the case of, for example, 'physical safety', attention is paid to the number of fatalities, seriously wounded and chronically ill and the lack of basic needs such as food, drinking water and power. An assessment is made for each type of disaster or threat as to how likely it is that it will occur.

Due to the fact that the risks of various sorts of disasters, crises and threats are assessed in the same way, the risks can be compared. Consequently, the NRP places the risks in a comparative perspective.

The insight into, and the overview of, the risks from the NRP enables the government to equip Dutch society more effectively to deal with (the threat of) potential disasters and crises and also choose the right priorities. The most important target group of the NRP is therefore the ministries, which are united in the National Steering Committee for National Safety and Security, and the national cabinet. However, the disasters and threats described also have consequences at regional and local level and can affect various organisations and sectors. The NRP analyses and the regional risk profiles drawn up by the security regions more or less cover a continuum from national to local scale.

The five national security interests	
Territorial security:	'The unimpeded functioning of the Netherlands as an independent state in the widest sense, or the 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.'

The basis of the NRP: eight different themes

In the NRP eight different themes are analysed, based on desk studies, consultation with experts from the fields of science, practice and policy and expert meetings, wherever possible composed of a variety of disciplines and organisations. The findings of these analyses are processed into separate theme reports. The most important risks from these analyses, in other words the types of disasters, threats and crises which can lead to societal disruption, are included in the NRP. These types (referred to in the NRP as *risk categories*) are summarised below per theme.

- **Natural disasters:** In addition floods (both from the sea and rivers), extreme weather events (heavy storms, snowstorms, black ice), wildfires and earthquakes can have serious consequences for society.

- **Threats to public health and the environment:** Due to the possible destabilising impact, the main focus of the NRP is on the risks of a large-scale outbreak of an infectious disease, such as a flu pandemic, a zoonosis outbreak and animal disease crises. Although relevant, the potential impact of a food crisis and an environmental disaster is estimated as being lower.

- **Major accidents:** This theme covers all accidents which can result in social destabilisation, such as radiological accidents (nuclear power stations), large-scale chemical incidents and transport-related accidents. Although the chance of such accidents occurring is estimated as being extremely low, if they occur the impact can be significant.

- **Disruption of critical infrastructure:** the emphasis is on the possible vulnerabilities of critical infrastructure and the potential impact of failure. The focus in this theme is on the impact of the disruption of the infrastructure (e.g. power, ICT, (drinking) water), irrespective of the applicable circumstances and the reason for the failure. That is explored in the other themes. The failure of several critical processes (as a consequence of cascading effects) has the greatest impact.

- **Cyber threats:** are focused on disruption of digital systems and disruption of internet (capacity), as well as cyber espionage and cyber crime. Cyber incidents can cause both indirect and direct damage and destabilisation (for example due to a substantial data leak or the corruption of key systems).

- **Subversion, extremism and terrorism:** This theme covers various types of social threats. The focus is on large-scale disorder, subversive practices which threaten, among other things, our open society, and (possible) consequences of extremism and terrorism. Insidious processes play a role in this which sometimes and often unexpectedly manifest themselves in incidents such as disorder or an attack.

- **Geopolitical threats:** relate to the effect of geographical factors on (international) political issues. More specifically: the battle to control land, sea and air space in order to define borders and spheres of influence. The Netherlands can become involved in various ways in threats or conflicts which can have a destabilising effect in the event of escalation. An increasing concern is the phenomenon of hybrid threat.

- **Financial-economic threats:** this means potential incidents or crises which can occur within the financial-economic system. This in particular means 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.

Risks in perspective

In order to gain an insight into the relative seriousness (or impact) and likelihood of all risks, fictitious scenarios have been developed, as an illustration, which describe a possible disaster, threat or crisis. These have been used to assess the impact and likelihood, so that these risks can be placed in a comparative perspective. A standard scoring methodology is used for the assessment which has been specifically developed as part of the National Safety and Security Strategy. The NRP also describes, per theme, the most important developments and capabilities so that the developed scenarios can be placed in the right context.

The figure below shows the total impact of the various scenarios which has been calculated on the basis of the individual impact scores (the sum of the impact on territorial security, physical safety, economic security, ecological security and socio-political stability). The scale goes from *limited to catastrophic*.

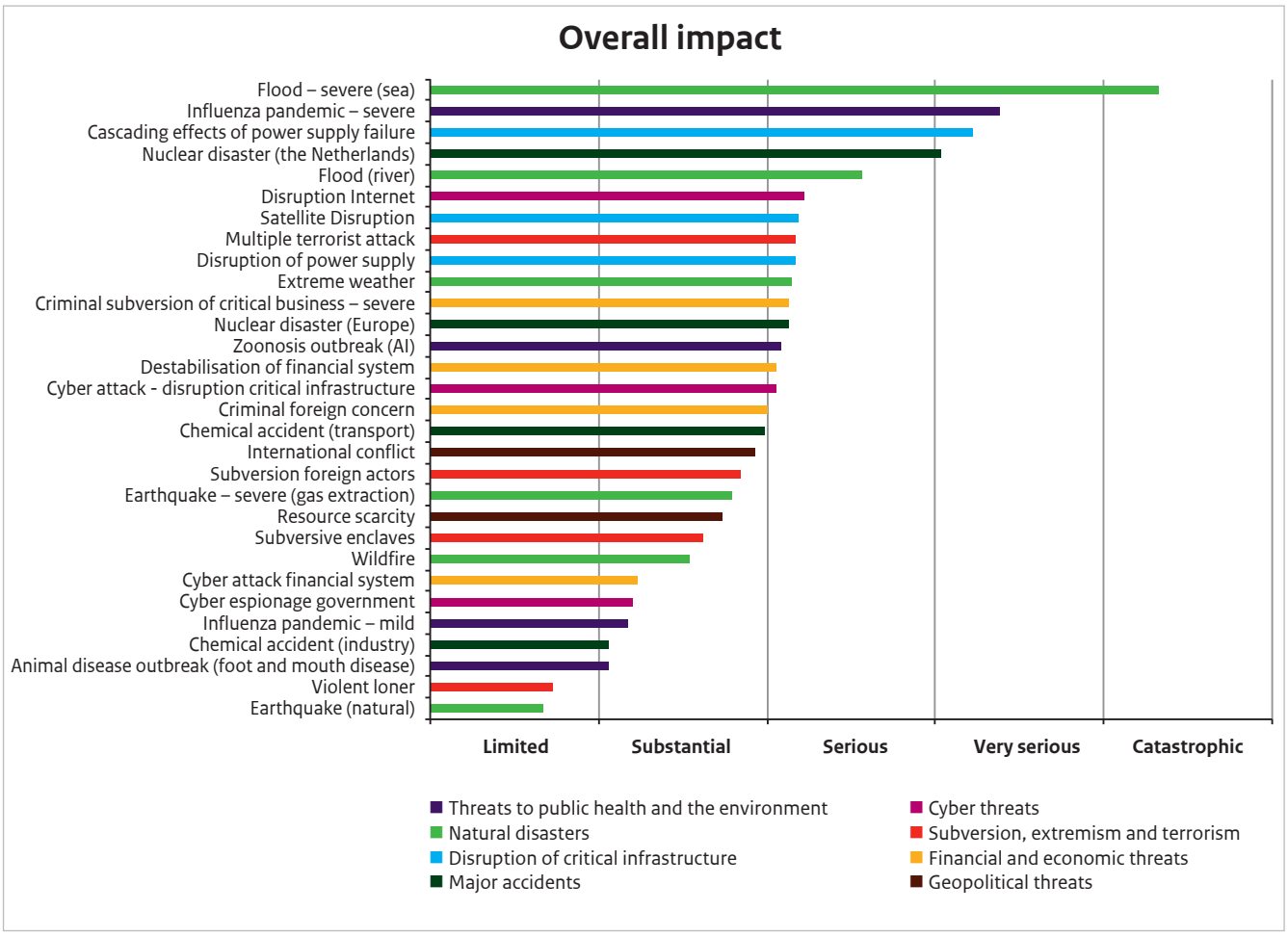
From this figure it can be deduced that numerous scenarios have an identical overall impact score, namely 'serious'. Five scores **stand out** more than others:

- Flood (caused by the sea)
- Severe influenza pandemic
- Cascading effects of power supply failure
- Nuclear disaster (the Netherlands)
- Flood (caused by rivers).

When these disasters occur they have an impact on a national scale and (very) seriously compromise several national security interests.

However, in addition to the impact, likelihood of occurrence is important as well. The probability of occurrence of 'physical disasters', such as a nuclear disaster (disaster involving a nuclear power station), a catastrophic flood (flood in the western part of the Netherlands) is extremely low. The same applies to 'worst case' disasters like a severe earthquake (with more than 100 fatalities) and major chemical accidents.

Figure 1 Overall impact.



The findings relating to these types of disasters are supported with examples of disasters which actually occurred, such as the flood as a consequence of the Hurricane Katrina, which affected New Orleans and the surrounding area in 2005 and the nuclear disaster at Fukushima in 2011. In both disasters the impact was partly determined by cascading effects, which occurred as a result of the failure of various critical infrastructure.

The score of the cascading effects of a power supply failure scenario clearly shows that the impact of this failure is also, in itself, already high, irrespective of the cause. Because such a failure may have various causes, the likelihood of this type of scenario is higher than that of a serious flood, even though the possibility of failure including serious destabilisation is still small.

The impact of chemical accidents is lower because, unlike in the event of a flood or nuclear disaster, it does not result in a large area being unusable or inaccessible for a prolonged period of time and neither does any large-scale evacuation take place. Nevertheless, there may be numerous victims, damage and social and psychological consequences, as demonstrated by the disaster in Tianjin (2015) and, on a smaller scale, the fireworks disaster in Enschede (2000).

A severe influenza pandemic scenario is characterised by both a relatively large impact and a relatively high likelihood of occurrence. This high impact differs in terms of some aspects from that of the 'physical disasters' discussed above. For example, a pandemic (a global infectious disease crisis) is, by definition, an international disaster (outside threat) that can hamper disease control and measures to limit the consequences. A serious pandemic is also characterised by numerous fatalities and ill people with the potential consequence of large-scale incapacitation of personnel, which in turn can lead to economic damage, failure of critical infrastructure and the functioning of society.

The categories and scenarios shown in the **lowest part** of the figure have a limited impact on a national scale. However, the majority do have a relatively higher likelihood of occurrence. For example, outbreaks of animal diseases, such as foot and mouth disease, swine fever, and attacks by violent loners occur quite regularly. Animal disease outbreaks can have a destabilising effect at regional level and livestock sectors, however, the total impact will be limited on a national scale. Attacks by violent loners may hold society in their grip temporarily, but do not lead to long-term disruption of national security interests. Cyber espionage and activities which subversive the functioning of the democratic system and its institutions have not yet manifested themselves on a (very) serious scale. However, there are indications that these risks are increasing and vigilance is therefore needed.

A relatively large group of types of risks do, if they do occur, affect national security (substantial to serious impact), but do not affect all national security interests to a high degree. This group includes scenarios relating to the disruption of critical infrastructure (with the exception of a disruption with long-term cascading effects), various cyber threats, a major terrorist attack, threats of a geopolitical and financial-economic nature, criminal interference in the economy, a zoonosis outbreak and several variants of natural disasters (extreme weather, wildfire) and accidents. Due to the increasing complexity of society, the interconnectedness of critical and digital systems and the development of hybrid threats, a number of these risks (in particular geopolitical and cyber threats and disruptions to critical infrastructure) may increase.

A closer look at the impact

Increased insight into the various national security interests which are compromised makes it possible to examine measures more specifically in order to make the Netherlands more resilient. If we then zoom in more closely on the impact per national security interest, this reveals the following picture:

Territorial security

This interest can be affected in two ways. For example, the consequence of a flood and a serious nuclear disasters is that part of our territory will be unusable or inaccessible for a long period of time. On the other hand, an international conflict and interference by undesirable parties in the business community can, for example, seriously damage our country's international position, either at a political-administrative level or economically, as well as threaten our autonomy.

Physical safety

We interpret the impact of this interest by the numbers of victims (fatalities, seriously injured and chronically ill including psychological disorders) and a lack of basic needs. Large numbers of victims come about primarily in the event of natural disasters, major accidents and threats to health, such as a pandemic. In addition, a major (multiple) terrorist attack can cause a substantial number of victims, whether they are committed with firearms, explosives or CBRN agents. The scenarios which fall under the theme of 'Disruption of critical Infrastructure', including a cyber disruption of critical processes, as well as some natural disasters, can create a

major shortage of basic needs, such as drinking water or energy (gas/electricity).

Economic security

It is evident that the scenarios which fall under the theme of 'Financial and economic threats', such as interference in the business community, affect economic security. In such instances there is both a violation of the vitality of the economy (large unemployment, failing sectors, decreasing confidence in the economy and financial system) and financial damage. Economic damage in terms of high to very high costs occurs in almost all risk categories.

Ecological security

Of all scenarios in the risk diagram, only a major flood and a wildfire cause a (serious) violation of nature and the environment. A number of global, often insidious developments, such as climate change and the reduction in biodiversity, can have negative effects on nature and the environment with possibly greater consequences for ecological security.

Social and political stability

The 'Social and political stability' interest has to do with disruptions to the daily life of the population, the violation of democratic institutions and standards and values and the destabilisation of the social climate in our society. The disasters that disrupt critical infrastructure, or which lead to a large area having to be evacuated, will quickly result in a serious disruption to daily life. This implies that large groups of people will not be able to participate normally in society (work, school, social activities) for a certain period of time.

The structural violation of the democratic constitutional system and the standards and values of our open society features in the scenarios that fall under the themes of 'Geopolitical threats', 'Subversion, extremism and terrorism', 'Financial-economic threats' and the 'Cyber espionage' risk categories. Scenarios in other risk categories will, at most, lead to a short-term disruption to the functioning of institutions. However, this will not lead to a structural violation.

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 the social climate. In particular, situations in which a large degree of uncertainty dominates the further continuation of events, in which there is a feeling of culpability towards institutions or companies, or which result in various opposing groups (based on different interests or viewpoints), can lead to outbreaks of violence (riots or revolts, as well as looting) or a structural violation of the social cohesion.

Developments and possible threats for the coming years

In addition to the theme analyses, we also carried out an assessment of developments which, by themselves, do not constitute an immediate threat to national security, but may have an effect on certain risks or which may lead to new risks. In particular developments, processes and trends which exist for the medium to long term and often on a global scale. These developments largely lie outside the direct sphere of influence of an individual organisation or a single country. This is partly the reason why the necessary capabilities with regard to such new risks have not always been clearly and properly defined. The (new) risks which result from these developments are beset with major uncertainties. Numerous scenarios are conceivable for such risks, and these scenarios are being characterised by a high degree of complexity, uncertainty and ambiguity, whereby the likelihood and consequences cannot be quantified. Several examples are clarified below.

Climate change increases the risk of natural disasters (floods, extreme weather, wildfires), large-scale epidemics and disruption of critical infrastructure. In our country work is being carried out using various approaches on the basis of a climate adaptation strategy with a view to control the consequences of climate change. For instance, the local effects of extreme weather incidents clearly show that climate adaptation requires permanent attention. The effects of climate change on a global scale are expected to be substantial. In various parts of the world the number and the impact of natural disasters may increase and there will be more frequent shortages of food and (drinking) water. These phenomena may indirectly lead to an increase in migration, conflicts between groups and countries, and to a 'battle' for raw materials and natural resources. They will therefore constitute a threat to our national security in the longer term. It is currently impossible to predict when this threat will occur and on what scale.

A trend which might be detrimental to the social cohesion in society is that of the **widening gap between social groups** regarding income, health, employment opportunities, well-being and socio-cultural views. What follows is that we can also highlight a number of **trends within the socio-cultural domain**: the individualisation (and the focus on individual interests), the decreasing confidence in the government and the authority of science and institutions, the increasing feeling of 'great discontent', the growing segregation and pressure of information, the influence of social media, the pressure on the welfare state and the increasing polarisation between various social, religious, ethnic, and political groups.

From a geopolitical perspective, the perception is that there are changes leading from a multilateral to a multipolar world order. This is accompanied by greater fragmentation within the international system, **a shifting balance of power**, more difficult relationships between great powers and other emerging countries, and a **growth in tensions**, (the threat of) conflicts and **increasing regional instability** in the world. The Netherlands could be dragged into a conflict due to its relationships with its allies. It should be noted, however, that the likelihood of an armed confrontation between great powers or a threat of a global conflict as in the Cold War, is extremely small. In contrast, regional conflicts can be expected to have indirect effects, like the aforementioned migration flow. As far as geopolitical developments are concerned, specific attention should be focussed on the phenomenon of **hybrid threat**. The term 'hybrid threat' is used to describe a conflict between states, usually below the level of armed conflict, involving the integrated use of conventional and unconventional means, open and covert activities, military, paramilitary and civil actors and resources to create ambiguity and exploit an opponent's vulnerabilities in order to achieve geopolitical and strategic goals. The use of manipulated information and deception are important aspects of hybrid tactics.

An important characteristic of such conflicts is often the deception, ambiguity and denial which accompanies the actions and which hamper attribution and response. An increase in this type of conflict has been observed.

For a number of sectors **globalisation** and increasing **centralisation** can constitute a threat to the international economy. Centralisation in, for example, the chemical industry and among producers of medicines and vaccines, is creating greater dependency, which implies risks for, among other things, the availability of essential substances and resources. The increasing complexity and interconnectedness of systems and the financial world hamper adequate control of risks and any crises that may occur.

Technological innovations are also having an effect on national security risks. The emergence of the Internet of Things (IoT) is creating **increasing connectivity and mutual dependency between systems**, as a result of which the failure or manipulation of critical infrastructure due to, for example, a cyber attack can have increasing consequences. Technological innovations can set social transitions in motion which are **difficult to control**. The speed of such developments and the difficulty of timely predicting potential risks makes it difficult to implement adequate supervision and legislation or regulations. In addition, knowledge and technologies are becoming more accessible for a broad audience and this is increasing the risk of **negative side-effects** of both their use and **misuse**.

Closing remarks

By describing the context and features of the different risk themes, the assessment of the risks and the underlying (impact) analyses, the NRP offers the possibility of viewing various potential disasters, threats and crises which could disrupt our society in a comparative perspective.

In addition, the results provide input for the capability analysis. The NRP presents an overview of the risks, based on the current situation, including what the Netherlands are already doing to manage the risks and eliminate threats (read: the existing capabilities). It also describes trends and developments which, in the future, may lead to a change in the current risks or cause new risks to arise. The capability analysis will reveal whether the current capabilities are considered sufficient, or whether certain capabilities have to be reinforced or developed.

The most important observations based on the results are the following:

- It is clear that a number of disaster types, namely a large-scale flood, a nuclear disaster, a pandemic and a long-term electricity outage (including cascading effects) are more destabilising than others (given their high impact). For this reason it is obvious to put effort in prevention of these disasters to occur wherever possible. The analyses show that the Netherlands are already doing a great deal to manage these risks and that, partly for this reason, the likelihood of such disasters is extremely low.

- Various other risks such as cyber threats, disruption of certain critical infrastructure, manifestations of extremism and terrorism, geopolitical threats, criminal interference in the economy, some types of natural disasters (such as extreme weather) and zoonosis outbreaks have a lower overall impact, but can have a serious detrimental effect on specific national security interests such as physical safety, or social and political stability. Those specific interests can provide a relevant basis to strengthen capabilities.

- A number of types of disasters and threats have a relatively high likelihood and a limited impact. It is important to determine what the possible triggers or developments might be that would exacerbate the impact (in the future) of these types of disaster. For

example, cyber espionage and activities which affect the functioning of the democratic system and its institutions have not yet manifested themselves on a (very) serious scale. However, their impact may be greater if certain developments continue. Some of these risks may be less disruptive on a national scale (compared to other threats), but may still be regarded as very serious incidents at regional level. Taken the capability analysis into account, the challenge is to achieve proper coordination with the security regions.

In addition to these results, analysis of (autonomous) developments, their mutual relationship and their possible influence provide insight on national security. We can illustrate this using the following two important increasing risks:

- The increasing connectivity and mutual dependency between systems can lead to the more rapid occurrence of (greater) cascading effects. Besides the mutual interconnectedness of various critical infrastructure, the focus is on digitisation with accompanying cyber threats.

- Based on international and geopolitical developments, the hybrid threat phenomenon has emerged as a relevant risk to our country.

Such developments can increase certain risks in the long term, or introduce new risks, and this can be taken into account during the continued development of, among other things, the capability analysis.

Foreword

We are proud to present the National Risk Profile (NRP) 2016, a periodical All Hazard overview of the risks of various disasters, crises and threats which may can jeopardise our society.
The NRP has been published as part of the National Safety and Security Strategy which has existed since 2007 and which consists of three steps:

1. The identification and analysis of various sorts of disasters, crises and threats: 'What is threatening us and how bad is it?'
2. The assessment of the capabilities that are required and need to be developed in order to prevent disasters or limit the consequences: 'What are we already doing and what can and must we do additionally?'
3. The implementation of capabilities to be developed and strengthened in policy and measures.

The NRP is a first step and therefore forms the basis for the National Capabilities Programme (NCP), that includes the second and third steps of the National Safety and Security Strategy.

The NRP replaced the National Risk Assessment (NRB), which was published up until 2014 and which analysed a number of types of disasters and threats each year in the form of scenarios which were then assessed using a fixed scoring methodology. Since the National Safety and Security Strategy started, a total of approximately 50 scenarios have been developed on a large number of themes.
In 2014 the National Steering Committee for National Safety and Security decided to develop the NRB into the National Risk Profile. The NRP contains an All Hazard overview of the most important risks to national security and is published every 4 years. The overview describes not only thematic analyses but also technological, social and international developments which may form a threat to national security and also indicates how the risks may develop in the medium term. The All Hazard overview presents the correlation, mutual effects and vulnerabilities, meaning that the individual analyses together form a single whole. After all, the increasing dependency of critical processes and the complexity of our modern society mean that disasters may have a destabilising effect in several areas and that, in turn, increases the demands placed on risk management.
The NRP explicitly describes which capabilities we have at our disposal to manage the risks.
The types of disasters and threats described in the NRP also have consequences at regional and local level and can affect various organisations and sectors. For that reason the security regions and critical sectors were explicitly involved in development of the NRP, with the aim being to ensure that the analyses for the NRP link up with those of the Regional Risk Profiles, so that they more or less create a continuum from national to local scale.

The production of the NRP involved continuing to build on the knowledge which has been developed in the successive NRBs during the past few years. This means that knowledge used for the development of the scenarios and execution of the theme analyses and for the methods and models used. Parallel to the creation of the NRP, the method for risk assessment was also reviewed. That resulted in a number of changes and additions. For example, a second assessment criterion for economic security (namely violation of the vitality of the economy) was added to the scoring methodology, a number of criteria were refined on the basis of the experiences with the NRB and the risk assessment was broadened in order to provide insights into not only the scenario analyses, but also specific developments, capabilities and historical cases.

The NRP has been compiled by the National Network of Safety and Security Analysts (ANV) on the instructions of the National Steering Committee for National Safety and Security. The ANV is a knowledge network that was set up in 2010 and, since then, has produced the annual National Risk Assessment and performed other national security studies for the government. The ANV core consists of six organisations (the National Institute for Public Health and the Environment (RIVM), the Netherlands Organisation for Applied Scientific Research (TNO), the General Intelligence and Security Service of the Netherlands (AIVD), the Netherlands Institute of International Relations 'Clingendael', the Institute of Social Studies and the Research and Documentation Centre (WODC) and an affiliated circle of organisations

such as knowledge institutions, security regions and other government departments, companies and consultancy firms. Annex 2 contains a description of the ANV.

The NRP is going to be published every 4 years. This way we are able to keep track of the effectiveness of national security policy, of developments and changes in the risks and the emergence of new risks and threats. Insights provided by the NRP will be used to prepare our country as well as possible for disasters, threats and crises, either by preventing them or by reducing their consequences.

1 Introduction

1.1 The National Safety and Security Strategy and the National Risk Profile

The government wants to prevent society from becoming destabilised due to a disaster or crisis, either by preventing such a disaster or crisis from happening, or by limiting the consequences as much as possible should they occur. For that reason the government is using, among other things, the National Safety and Security Strategy to establish which threats may jeopardise national security and what we can and should do about it. The National Safety and Security Strategy has existed since 2007 and consists of three steps:

1. The identification and analysis of various sorts of disasters, crises and threats: 'What is threatening us and how bad is it?'
2. The determination of the capabilities that are required and need to be developed and strengthened in order to prevent disasters or limit the consequences: 'What are we already doing and what can and must we do additionally?'
3. The implementation of capabilities to be developed and strengthened in policy and measures.

Details of the identification and analysis are contained in the National Risk Profile (NRP). The NRP is a periodical All Hazard overview of the risks related to various disasters, crises and threats with a potentially destabilising effect on society. The term 'destabilisation' applies if one or more national security interests are seriously or very seriously compromised. Those interests were established when the strategy was drawn up in

The five national security interests	
Territorial security:	'The unimpeded functioning of the Netherlands as an independent state in the widest sense, or the territorial integrity in a narrow sense.' *This concerns both the physical territory and corresponding infrastructure and the image and reputation of our country.*
Physical safety:	'The unimpeded functioning of people in the Netherlands and its surroundings.' *This concerns people's health and well-being. The criteria are numbers of fatalities and seriously injured people and a lack of basic needs such as food, power, drinking water and adequate accommodation.*
Economic security:	'The unimpeded functioning of the Netherlands as an effective and efficient economy.' *This concerns both economic damage (costs) and the vitality of our economy (for example a serious increase in unemployment).*
Ecological security:	'The unimpeded continued existence of the natural living environment in and around the Netherlands.' *This concerns violations of nature, the environment and ecosystems.*
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.' *This concerns violations of freedom to act, the democratic system, the core values of our society, and the occurrence or otherwise of large-scale social unrest and accompanying emotions (fear, anger, grief).*

2007 and can be measured using a number of criteria to determine the impact (seriousness) of each potential disaster or crisis. These criteria are used in the risk assessment, which is explained in more detail in Chapter 2.

The NRP analyses the risks of various sorts of disasters, crises and threats and places these in a comparative perspective. However, disasters do not occur in isolation. Due to the increasing dependency of critical processes and the complexity of our modern society, a disaster or serious incident can have destabilising consequences at various levels. Examples are cascading effects of a nuclear disaster (radioactive contamination of crops on a large scale can have serious detrimental consequences for the agricultural sector), or the consequences of a large-scale failure of the financial system due to a coordinated cyber attack. The complexity and dependencies impose demands – sometimes in addition to regular tasks – on the management of the risks by governments (at various levels), emergency and security services, critical sectors and the business community. An additional aspect is that for good risk management, technical and organisational measures are important, however, social factors such as perception, acceptance of risks and measures, risk awareness, uncertainties, controversies and other social aspects must be taken into account as well.
In the NRP we not only describe and analyse individual disasters, but also present an overview of the correlation, mutual effects and vulnerabilities in a way that the individual analyses together form an integral part that serves as a basis for the National Capacities Programme (NCP) which constitutes the second and third step of the National Safety and Security Strategy. The NRP is published every 4 years. This way we are able to keep track of the effectiveness of national security policy, of developments and changes in the risks and the emergence of new risks and threats.

If a society is well prepared to cope with the type of disasters and threats described in the NRP, it will also be well prepared for other major calamities.

1.2 Themes and risk categories

In order to stimulate a systematic and consistent approach, a decision has been taken to classify the various types of disasters, crises and threats into a number of threat themes, referred to below simply as themes. We distinguish between:
- Natural disasters
- Threats to public health and the environment
- Major accidents
- Disruption of critical infrastructure
- Cyber threats
- Subversion, extremism and terrorism
- Geopolitical threats
- Financial and economic threats

We examine a number of different risk categories for each theme. In the Natural disasters theme, these include floods, extreme weather, heat and drought, wildfires, earthquakes and solar storms. The complete list can be found in Annex 1.
The classification is based on differences and similarities in the nature of the risks, the causes and the underlying factors, as well as the types of consequences (impact). Other classifications are possible, for example on a natural, technical and wilful basis. The chosen classification fits well with practice, provides the best connection to the National Capabilities Programme, and is attuned to the theme classification used by security regions to facilitate a smooth transition between the NRP and the Regional Risk Profiles (RRP).

To a certain extent a classification into themes and risk categories is arbitrary, all the more so because all kinds of risks from the various themes are linked together. It is important to realise that the NRP is not intended to provide a complete description of all possible disasters in all possible manifestations, including consequences and cascading effects. The thematic analyses in the NRP aim to provide as comprehensive a picture of the spectrum of types of disasters, crises and threats that can lead to societal disruption. That picture is the basis for the NCP.

The analyses of the themes and the risk categories they cover are described in a number of separate reports, with the most important findings being summarised in this NRP. The analyses have been carried out in accordance with the fixed methodological approach which is described in Chapter 2.

In order to gain an insight into the relative seriousness and likelihood of all risks, scenarios have been developed for each risk category. These have been used to assess the impact and likelihood of each risk, so that these risks can be compared. For the sake of clarity, a maximum of two scenarios per risk category are included in this NRP (see Chapter 2).
The selection of risk categories which are detailed in the NRP is based on the criterion that we – in accordance with the point of departure in the National Safety and Security Strategy – use the term 'destabilisation' if one or more national security interests are seriously or very seriously compromised, supplemented with a number of qualitative arguments.

The criteria used as a basis to determine which risk categories are included in the NRP

1. The violation of at least one national security interest must be serious in at least one of the scenarios in the risk category. Serious corresponds to score class C according to the NRB method (see Chapter 2).
2. If two or more risk categories substantially overlap as regards their nature and the related capabilities, one will be selected and the other will not (for the more detailed risk assessment please refer to the theme analyses).
3. Other qualitative reasons, such as the topicality of a strongly emerging risk with regard to which too little knowledge is available, or there is a suspicion that the capabilities fall short.

In addition to the theme analyses we have also explored trends and developments which may lead to new risks. The risks in question are generally beset with substantial uncertainties and are often also linked to developments in other fields. Numerous scenarios are conceivable for such risks, and these scenarios are being characterised by a high degree of complexity, uncertainty and ambiguity, whereby the likelihood and consequences cannot be quantified. In addition, the necessary capabilities with regard to such new risks have not always been clearly and properly defined. In the case of these risks it is sufficient to describe the most important developments and provide a brief definition. The development of these new risks will have to be continually monitored, supplemented with regular exploratory analyses.

1.3 To whom is the NRP intended?

The management of the risks of potentially destabilising events is not the responsibility of a single (type of) actor. Various organisations at various levels can use the NRP and the underlying analyses by asking themselves the question:
'To what extent will my organisation, ministry, municipality, security region, company or sector be affected by events described and analysed in the NRP? Are we sufficiently prepared for this?'
The analyses for the NRP focus, in the first instance, on potentially destabilising disasters and necessary capabilities on a national scale. The most important target group of the NRP therefore consists of the ministries, united in the National Steering Committee for National Safety and Security and the cabinet. However, the types of disasters and threats described also have consequences at regional and local level and can – due to their complexity and mutually dependent factors, consequences and vulnerabilities – affect various organisations and sectors: not only national and local authorities and the emergency and security services they are responsible for, but also critical sectors and companies. In addition, comparable disasters may also occur on a more local scale (in which case we usually refer to incidents). The scenario analyses in the regional risk profiles of the security regions take place primarily at that level, although most RRPs also include supra-regional and national disasters. The NRP and the RRP analyses developed by the security regions more or less cover a continuum from national to local scale.

Although the National Steering Committee for National Safety and Security and the ministries represented in this committee are the primary target group for the NRP, regional and local authorities, companies and other organisations can also use the NRP analyses.

1.4 How did the NRP come about?

The National Risk Profile is a product of the National Network of Safety and Security Analysts (ANV) and was commissioned by the National Steering Committee for National Safety and Security.
The ANV is a knowledge network that was set up in 2010 and, since then, has produced the annual National Risk Assessment and performed other national security studies for the government. The ANV consists of a permanent core of six organisations (the National Institute for Public Health and the Environment (RIVM), the Netherlands Organisation for Applied Scientific Research (TNO), the General Intelligence and Security Service of the Netherlands (AIVD), the Netherlands Institute of International Relations 'Clingendael', the Institute of Social Studies and the Research and Documentation Centre (WODC) and an affiliated circle of organisations such as knowledge institutions, civil services, security regions, companies and consultancy firms which are engaged in the various analyses whenever a relevant topic arises. Annex 2 contains a description of the ANV.

The National Steering Committee for National Safety and Security is an interdepartmental body that advises the government about national security issues. The Steering Committee monitors the execution of the National Safety and Security Strategy and the related activities. The fact that all the ministries are represented in the Steering Committee means that a joint, government-wide approach is guaranteed.
The Ministry of Security and Justice is responsible for the coordination of strategy and is the authorised principal of the ANV.

The production of the NRP firstly involved a detailed study for each theme in which all the steps per theme, as described in Chapter 2, were detailed on the basis of desk research and consultation with a broad group of experts, policy officers and experts in the field. The results of each study and the scenarios which have been developed for each theme have been submitted to a panel in an expert meeting, after which the findings of this meeting were processed in the aforementioned theme reports which constitute the basis for this NRP. Theme experts and specialists in various impact criteria were involved in the analyses and in the panels, with the latter being involved primarily in the assessment of the scenarios according to the method described in Chapter 2. In addition, the aim when compiling the panels was to create an optimal mix of experts from science, practice and policy and of representatives from various organisations involved in the theme.

1.5 Overview of the document

The NRP is structured as follows: Chapter 2 describes and provides reasons for the method used. This is followed by eight chapters which describe the main elements of the threat themes:

- Natural disasters (Chapter 3)
- Threats to the public health and the environment (Chapter 4)
- Major accidents (Chapter 5)
- Disruption of critical infrastructure (Chapter 6)
- Cyber threats (Chapter 7)
- Subversion, extremism and terrorism (Chapter 8)
- Geopolitical threats (Chapter 9)
- Financial and economic threats (Chapter 10).

An underlying theme report has been drawn up for each threat-related theme.

After that, Chapter 11 assesses the autonomous developments across the themes. The results, conclusions and observations are contained in Chapter 12 which also includes the overall risk diagram and the scores of the impact criteria.

2 Methodological rationale

2.1 The concept of risk

The National Risk Profile is an All Hazard overview of the risks related to various disasters, crises and threats with a potentially disrupting effect on society. Consequently, the NRP is about risks.
Various definitions and approaches exist with regard to the concept of risk, which are used in risk analyses in various fields such as economics, finance, mathematics, engineering, security, medicine and social sciences.
A common approach is to regard risk as the product of the possibility of an event and the scope of the consequences (damage) of that event. More recent approaches also take into account the vulnerability of an organisation, system or structure in this quantitative approach to risk. Social science research has shown that, when assessing risks and related behaviour, qualitative aspects such as the degree of (supposed) voluntariness, fairness, manageability or the familiarity with, and the social utility of a risky activity also play and important role. Risk is therefore a multidimensional concept which can be both subject to 'objective' calculation as well as interpretation as a 'social construct'.

2.2 Risk assessment and National Security

In essence, risk has to do with what might happen in the future and it is therefore, by definition, linked to uncertainty. In a general sense it concerns the question of whether a certain undesired event (incident, disaster or crisis) will take place and what its consequences will be. For the analyses contained in the NRP we regard the concept of risk as the interplay of impact (the totality of the consequences) and likelihood (the expectation concerning the occurrence of a disaster or crisis or the development of a threat). The traditional approach of 'risk is probability times impact' is deliberately avoided in the NRP because this suggests too much of a strictly quantitative interpretation of the concept of risk and because the reduction of 'risk' to a single number obscures its two inherent dimensions. Furthermore, it can be asserted that, in our experience of risk, impact and probability are not always weighted equally, which is what the aforementioned formula does assume. Given the main objective of the National Safety and Security strategy – to set priorities to strengthen capabilities to prepare our country properly for potentially disrupting disasters and threats – aspects such as vulnerabilities, manageability, perception and acceptance by administrators, the general public and other stakeholders are also of importance for the assessment of risk.

The NRP covers a wide range of threats in various fields, concerning which the most important characteristics are:

- They are calamities which occur very infrequently, meaning that only limited use can be made of (historic) data, statistics and models.
- The consequences of the types of calamities studied cover various fields, varying from effects on health and the environment to those on the economy and social and political stability.
- There is a substantial difference in dynamics and time frame between the various types of disasters, threats and crises.
- Disasters, crises and threats which have the potential to lead to disruption on a national scale are, by definition, of a complex nature. One of the reasons for this is the involvement of multiple an impact on often different fields.
- When assessing risks in the NRP, subjective elements such as perception, interpretation, the experience and acceptance of a risk, also play an important role.

A comprehensive approach

Due to these characteristics a comprehensive, more procedural approach is used in the analyses performed for the NRP. For these analyses, not only a wide range of knowledge and methods from various disciplines are used, but also expert opinions and information drawn from consultations.
Regarding knowledge and methods, it concerns the following aspects:

- data collection (historical cases, indices, practical experience, expert knowledge, etc.)
- the process of analysis (models, multi-criteria analyses, processing input from experts)
- risk presentation (impact and likelihood scores, diagrams, descriptions)
- determination of uncertainties, where we distinguish between ignorance, uncertainty, ambiguity and indeterminacy.[1]

Due to the usually limited availability of data and models, the assessment of both impact and likelihood is largely based on estimates by experts. Experts specialised in both the field of the themes and risk categories as well as in the various national security interests (read: impact criteria) and methods of risk analysis are involved in the analyses. On the one hand the aim is to assess risks as objectively as possible by using a robust classification according to – wherever possible objectively measurable – categories for both impact and likelihood. On the other hand the subjective element plays an important role, for example when choosing the themes and scenarios and when assessing the national security interest of 'social and political stability', which includes social and psychological aspects.
A protocol was developed in order to process expert opinions, based on three points of departure:

1. The assessment of the scenarios and theme analyses will be done during sessions attended by all experts.
2. The opinion of every expert participating in a session counts.
3. Experts may have different opinions which are taken into account in the uncertainty of both impact and likelihood.

The transparency of the process and the use of knowledge and methods from various disciplines ensures that the results of the risk assessments in the NRP are widely supported and that the most important uncertainties concerning the results are highlighted as best as possible.

Bow-tie analysis, building blocks and scenarios

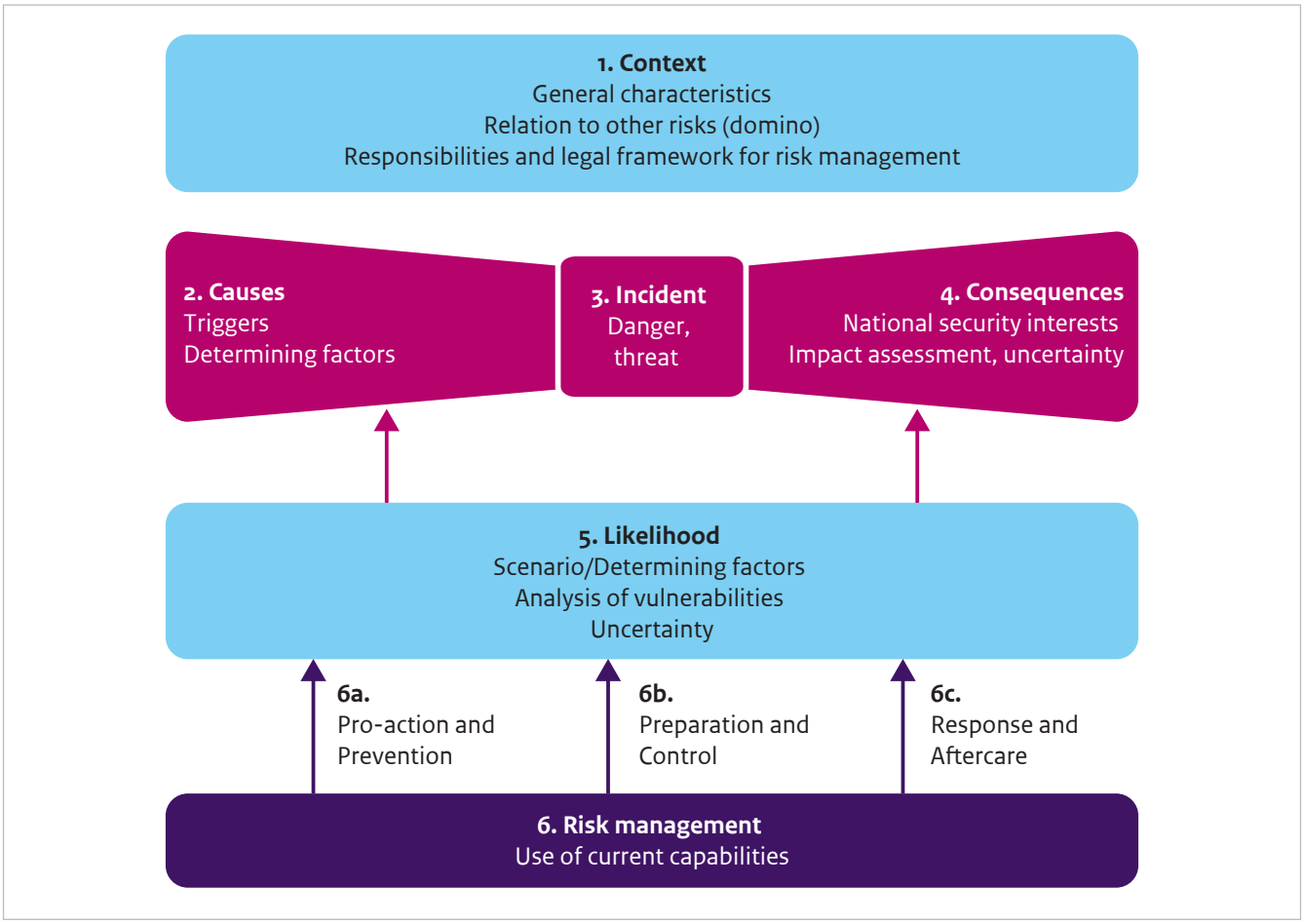
When compiling the National Safety and Security strategy in 2007, a methodology was developed which makes it possible to place risks of various, potentially disrupting disasters, threats and crises in a comparative perspective. This methodology, which is referred to as the NRB methodology, is based on scenarios which are placed in a fixed scoring methodology. The scenarios are narrative descriptions of disasters, threats and crises which are required to comply with a certain format in order to facilitate an adequate risk assessment using the scoring methodology. The scoring methodology, which is clarified in the next paragraph, was designed to determine the impact and likelihood of each scenario and the corresponding risk.

The format for the construction of scenarios according to the NRB methodology is based on the bow-tie model as shown in Figure 2.1.

The various elements in this bow-tie model (context; causes and triggers; consequences and possible cascade and cascading effects; mutual interdependence; vulnerabilities) are fixed parts of each scenario.
In the NRP – in contrast to the NRB – the risk assessment per risk category is no longer based on one detailed scenario description, but on an analysis of the entire spectrum of scenarios, derived from the building blocks and factors which together determine risk. These elements, as shown in the bow-tie model in Figure 2.1, provide the basis of the scenario spectrum and of the estimate of likelihood and impact including their bandwidth. In fact, risks do not manifest themselves in a single form, but in many forms with various likelihoods and impacts: from small opportunity – major consequence to major opportunity – small consequence and everything in between. It is also important to gain an insight into the determining factors which cause a disruption to arise or escalate, and into the consequences and related (cascading) effects: 'Where are the tipping points in the cause and effect chain?', and 'What makes an incident or crisis score higher or lower on the impact criteria?'
The risk assessment also examines the existing capabilities and possible vulnerabilities in the field of pro-action, prevention, preparation, repression (response and effect control), aftercare and recovery.

[1] By ignorance we mean: insufficient knowledge (gaps) and insight. Uncertainty refers to a lack of data, inaccurate models, representativeness, etc. Ambiguity relates to subjective aspects such as controversies and differences in acceptance. Indeterminacy stands for boundlessness, meaning that there is no visible 'end point' concerning the developments or consequences.

Figure 2.1 Schematic representation of the bow-tie model showing the various elements of the assessment per risk category.



In order to place the various categories of risks in a comparative perspective – one of the most important goals of the NRP – two scenarios are selected per risk category on the basis of the bow-tie analysis and the building blocks, generally speaking a normative and a conceivable worst-case scenario.[2] The scenarios are short narrative descriptions of a disrupting event including causes and effects, intended to outline a common image for experts, policymakers and professionals, and to determine impact and likelihood by way of the scoring methodology. This way an indication and bandwidth of each risk category is acquired. The selected scenarios serve as illustrations for the risk categories.

In the NRP the assessment of risks is based on the range of possible scenarios related to a particular type of disaster, threat or crisis.

2.3 The scoring methodology: risks in a comparative perspective

In the NRB each scenario is assessed against a fixed scoring methodology. This scoring methodology was designed in 2007, at the outset of the National Safety and Security strategy, in order to determine the impact and probability of each NRB scenario and the corresponding risk. The same scoring methodology is used for the scenarios contained in the NRP.
Over the years, the scoring methodology has been adjusted several times on the basis of experiences with its application in the successive National Risk Assessments. The framework is described in detail in the Guidelines on working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy[3].

A short clarification is provided below.

The scoring methodology which is used to assess risks to national security has been designed in such a way that the effects of very wide-ranging types of disasters, threats and crises can be placed in a comparative perspective.

The term '**impact**' is interpreted as the consequences or effects on the five national security interests, as defined in the National Safety and Security Strategy. This impact is operationalised in eleven 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 to catastrophic, and based on either quantitative data (such as the number of fatalities or costs), or a qualitative assessment (such as the degree to which institutions are no longer able to function). The figure below shows the general division into classes including two examples. For the full description please consult the aforementioned Guidelines.

Likelihood is an indicator for how often a described disaster, threat or crisis takes place within a certain period of time and is based on available knowledge. In the NRP a timespan of 5 years is used as a basis.
the determination of the likelihood of a scenario depends on the type of scenario and the available information. Generally speaking, three different characterisations are used for the classes of probability:

- quantitative scales for risks that can be analysed statistically or probabilistically;
- qualitative scales for threats of a malicious nature (based on aspects such as predictability, indications and vulnerabilities); and
- qualitative scales for other risks.

In a few instances a combination of two or three of these approaches are used.
Wherever possible likelihood is determined on the basis of historic cases, (historical) data, probabilistic models, chances of failure and calculations with the help of event trees. If these are not or only partially available, expert assessments will be used.
As is the case with impact, the scales used for likelihood will be divided into five classes.

[2] In general additional scenarios to those included here have been developed and assessed per risk category in accordance with the NRB method. For the sake of clarity it was decided to use a maximum of two scenarios per risk category in the NRP that are used to provide as good an insight as possible into the bandwidth of the risk. The difference between the scenarios is not always determined by their severity ('worst case' versus 'normative'), but sometimes also on the basis of variation in determining factors. The scenarios merely serve as illustrations and are, for example, not intended as a standard or model for which the Netherlands should prepare.

[3] The applied methodology is described in the Guidelines on working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy (2013) of the Ministry of Security and Justice and the working document entitled 'Guidelines on the method used for the National Safety and Security Strategy – revised impact criteria – working document 24 Feb 2016', in which the modifications to the assessment criteria are described. In the context of the revision, mention was made of 'cultural heritage' as an additional interest and an initial step was taken to include 'digital space' as a criterion. Further elaboration is required in both cases.

The impact criteria, related to the five national security interests	
Territorial security:	1.1 Encroachment on the territory and digital environment 1.2 Infringement of the international position of the Netherlands
Physical safety:	2.1 Fatalities 2.2 Seriously injured and chronically ill 2.3 A lack of basic needs (physical suffering)
Economic security:	3.1 Costs 3.2 Violation of the vitality of Dutch economy
Ecological security:	4.1 Long-term violation of nature (flora and fauna) and the environment
Social and political stability:	5.1 Disruption of daily life 5.2 Violation of the democratic constitutional system 5.3 Societal impact

Class	Example criterion: Number of fatalities	Example criterion: Violation of democratic system
Limited	Less than 10	Limited violation of the functioning of a couple of institutions[4]
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[5]
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

Class; general qualitative approach	Quantitative approach	Qualitative approach malicious
Very unlikely	Less than 0.05%	No specific indications; not conceivable
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] This concerns political representation, public administration and civil servants connected to it, public order and security systems and the independent judiciary.

[5] This concerns freedoms and rights as laid down in both the constitution and legislation (freedom of religion, expression, association, suffrage, etc.).

An understanding of the factors which determine likelihood is important in order to identify the degree to which it can be (positively) influenced by the strengthening or use of new capabilities.

An important aspect when determining likelihood and impact concerns the **vulnerability** or **resilience** of society. We interpret resilience as the capacity of society to continue functioning undisturbed in the event of (the threat of) exposure to the consequences of an incident, disaster or crisis.

2.4 Presentation of risks

The presentation of the results of the risk assessment is related to the objective of the NRP, namely to better equip Dutch society to deal with (the threat of) potential disasters and crises and to choose the right priorities whilst doing so. In this context important questions are:

- Which types of risk constitute the greatest threat, as regards impact and likelihood?
- Which national security interests are affected most concerning one or more risk categories?
- Which of the analysed risks constitute a possible current or perceived threat?
- Which capabilities are already being deployed per risk category and what is their quality and scope?
- What are the uncertainties (types, scope) in the results of the risk analysis and to what extent can these be taken into account in decision-making?

With regard to uncertainties, a distinction can be made according to the representativeness of the scenarios for the entire spectrum, the chosen models and variables, available knowledge and data (or the lack thereof) and subjective aspects such as perception, experience, acceptance and ambiguity.

We wish to point out that questions relating to the development and reinforcement of capabilities and decision-making belong in the National Capabilities Programme and not in the NRP. However, they are of importance when it comes to the objectives of the National Safety and Security Strategy.

The results of the risk analyses using the scoring methodology are presented in the theme chapters and in the All Hazard discussion in Chapter 12.
In the theme chapters the impact and likelihood scores of each of the selected scenarios are shown in the tables. In addition, each theme chapter contains a **thematic risk diagram** which presents the overall impact and likelihood of the selected scenarios.

Chapter 12 contains the **All Hazard risk diagram** with which the risks of various themes and risk categories can be placed in a comparative perspective. The meaning of the diagram is also clarified in more detail in this chapter.
In order to answer the aforementioned questions, an understanding of the severity with which the various national security interests are affected is important, both per risk category and as a whole. This is also described in Chapter 12.

2.5 Overview of the various aspects per risk category

The objective of the scenario assessment is to place the risks related to various themes in a comparative perspective. However, the analysis of the various risk categories in the NRP contains more than just the scenarios. The following aspects are presented for each risk category.

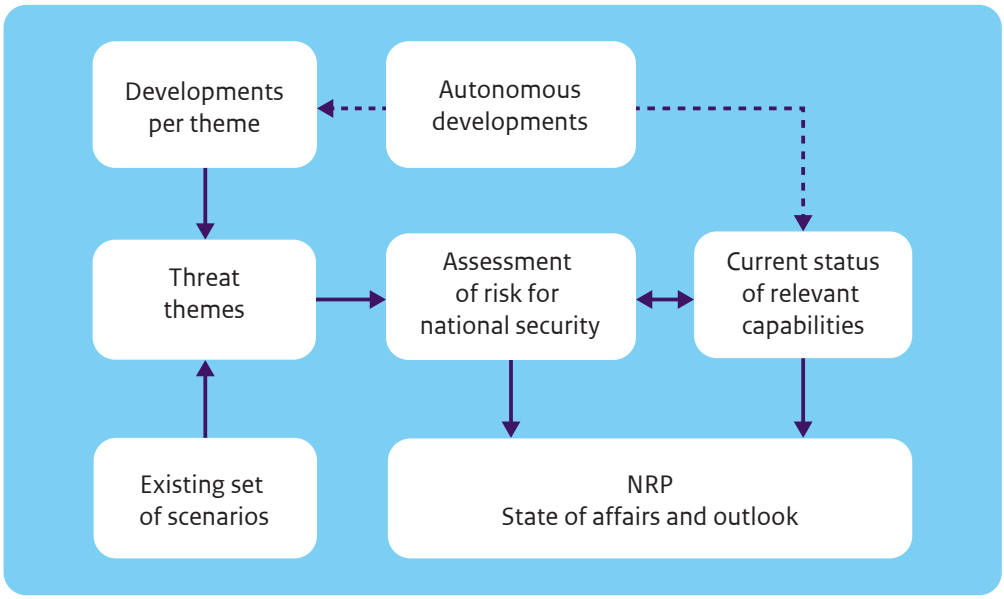
- A description of *general characteristics of the type of risk* and the possible varieties in which it can appear. An indication is also given as to which regulations and legislation are applicable and which parties (government, as well as business community, for example the critical sectors) are involved with this theme, including their responsibilities.
- An overview of the most severe incidents and disasters in relation to the risk category which have occurred during the past decades (in the Netherlands and worldwide). These *historic cases* provide useful information for the risk assessment.
- An overview of *current and future developments* relating to the risk category and any consequences thereof for the particular risk.
- An overview of the consequences of *autonomous developments which may have an impact on the risk*. We interpret the term ‘autonomous developments’ as developments in the medium to long term which are not, in themselves, a threat, but can have an indirect influence on national security. The next paragraph contains a more detailed description of the term 'autonomous developments' and the way in which we have taken these into account in the risk analyses.
- A general description of *existing capabilities* ('What are we already doing as regards risk management?'), using the five links in the crisis management cycle as a guide, supplemented with the aspect of knowledge ('Is knowledge on the risk in every way what it should be, or are there any blanks?')[6].

[6] The crisis management cycle is a standard approach to determining capabilities and vulnerabilities of a system or sector.

- An overview of previously constructed *scenarios from the National Risk Assessments* (2008-2013).
- Some of these scenarios or elements from them have been used for the scenario assessment in the NRP, as described in the previous paragraphs.
- An overall overview of *scenarios from the Regional Risk Profiles*, insofar as available[7].

The various elements are illustrated in Figure 2.2.

Figure 2.2 Elements of the theme analysis.



[7] The safety regions have produced scenarios for a number of themes and risk categories (referred to as crisis types in the RRP; see Annex 1). Compared with the NRP scenarios, the regional scenarios are more operational in nature and more limited as regards the consequences and impact.

2.6 Analysis of autonomous developments

Autonomous developments mean processes and trends which, in themselves, are not a direct threat for national security, but which can have an influence on certain risks and threats. The term 'autonomous' indicates that it concerns
developments which lie outside the sphere of influence of an organisation or government and which will occur irrespective of the risk management choices which individual organisations of authorities make. Examples are climate change which, over time, has consequences for, among other things, the risks of floods and extreme weather and threats to public health.
For the NRP we made a systematic analysis of autonomous developments by carrying out a literature review of leading explorative studies, trend analyses and scenario analyses by planning agencies, think tanks and renowned international institutes, supplemented by a number of expert meetings.
We distinguish between five categories of autonomous developments:

- Ecological developments
- Demographic-societal developments
- International-political developments
- International-economic developments
- Technological developments.

The analysis of autonomous developments serves two goals.

1. The first is to assess the influence that developments have on the risks in the individual themes and risk categories.
2. The second is to identify (new) risks and threats which do not come to light if we only carry out the step referred to above. Examples are potential effects (threats as well as opportunities) of existing and emerging technologies and risks and threats which result from the correlation between various themes and/or autonomous developments.

The findings of step 1 are summarised in the underlying theme analyses and the chapters in which the risk categories are described. Chapter 11 describes the results of the analysis of autonomous developments and takes a closer look at new risks and threats which result from step 2.

3 Natural disasters

3.1 Risk categories

In the case of the Natural disasters threat theme the focus is on (potential) disasters caused by forces of nature, concerning which we limit ourselves to natural disasters in the Netherlands with effects in the Netherlands. Such a disaster often has natural causes, but can also be caused (directly or indirectly) by human actions. Despite this qualification we use the term 'natural disasters' for the threat-related theme, given that this clearly refers to forces of nature. The following risk categories are considered[8]:

- Flood
- Extreme weather (black ice, (snow)storm)
- Drought/heat
- Wildfire
- Earthquake
- Solar storm

The possible consequences of a natural disaster go beyond the amount of victims alone. To show that economic damage can also be extensive, we provide, before examining the categories referred to above in more detail, an overview of the consequences of the ten 'most expensive' natural disasters in Europe in the period 1980-2010.

Table 3.1 The ten 'most expensive' natural disasters in Europe in the period 1980-2010 according to data from Munich Re NatCatSERVICE database (adopted from NMI, 2013).

Time	Type of natural disaster	Affected area	Direct economic damage (€ million)	Number of fatalities
August 2002	Floods	Central Europe	16,800	30
July-August 2003	Drought + heat	Central Europe	12,300	70,000
November 1980	Earthquake	Italy	11,800	2,900
December 1999	Storm (Lothar)	Northwest Europe	11,500	110
October 2000	Floods (and landslides)	Italy, Switzerland, France	10,000	38
January 2007	Storm (Kyrill)	Northwest Europe	7,800	49
November 1994	Floods	Italy	7,500	68
January 1990	Storm (Daria)	Northwest Europe	5,900	94
July-August 1997	Floods	Central Europe	5,500	118
September 1997	Earthquake	Italy	5,400	11

[8] A decision was made to give the risk categories very clear and self-explanatory. By doing so we deviate from the classifications used in this specialist field, which refers to meteorological, hydrological, climatological and geophysical disasters. This is explained in more detail in the theme report.

3.1.1 Flood

Due to the possible catastrophic consequences it is essential to include floods as a risk category in the NRP. A major flood leads to social disruption and will have an effect on all national security interests.

As regards capabilities, a lot of measures are being implemented in the Netherlands now and in the coming decades to protect the country against flooding and to keep the resulting damage caused by floods to a minimum. The so-called multilayer security approach is a key point of departure in this respect. According to this approach the land behind the dykes is protected from (the consequences of) flooding by investing in three layers: strengthening flood defences (layer 1), a water-robust spatial lay-out (layer 2) and adequate disaster management (layer 3). The main focus of layer 1 is to limit the possibility of a flood, while layers 2 and 3 are intended to limit the consequences, should a flood occur after all.

In order to create a better understanding of flood risks, it was decided to analyse both a 'worst-case' scenario and a 'normative' scenario. A flood originating from the sea, flooding a large portion of the Randstad conurbation is used as a 'worst-case' scenario. The 'normative' variant concerns a flood originating from rivers[9]. See also paragraph 3.2.

3.1.2 Extreme weather

In order to gain an understanding of the risks related to extreme weather, such as a snowstorm, hail, black ice or a severe storm, it suffices to assess just one 'extreme weather' scenario. The different variants ultimately have to do with the same types of impact, with disruption of daily life being the main one. Furthermore, the capabilities necessary to deal with the consequences of these disasters are generally identical, such as the accessibility of people requiring assistance and medical facilities, the supplying of supermarkets and the continuity of critical infrastructure.

For the 'worst-case' variant of the 'extreme weather' scenario the assumption is that it occurs in the Randstad conurbation. See also paragraph 3.3. It also the case that, as far as national security is concerned, there is no point including a 'normative' scenario, given that impact will remain limited and consequences are more likely to be regional.

[9] We use the term 'normative' in the NRP to indicate a representative scenario. In the case of flooding, normative has a different meaning and relates to a flood in conjunction with a 'normative high water level', which is the water level in conjunction with the normative probability as laid down in the law.

3.1.3 Drought and heat

Because the total (combined) impact of drought and/or heat on the five national security interests is 'limited', this risk category is not developed in further detail in this main report. In this context we would still like to point out that particular attention needs to be paid to the number of fatalities in relation to premature deaths of elderly and chronically ill people during heatwaves.

With regard to capabilities, however, heat and drought are of importance for national security and when also taking into account climate change, it is a good idea to focus on them. The phenomena of heat and drought have various knock-on effects regarding required capabilities:

- In the case of heat, capabilities in the field of healthcare are particularly important. A relevant aspect is the premature death of elderly people during a heatwave, particularly within the context of changes in healthcare and the trend that vulnerable groups of elderly people are continuing to live at home more often and for a longer period of time.
- In the case of drought the emphasis is mainly on capabilities required for providing fresh water. Another factor that requires attention is the impact on the power supply. If restrictions apply to the discharge of cooling water, this may result in power stations that are (or have to be) shut down. This can lead to cascade effects, for instance in the ICT sector (see also the disruption of critical infrastructure threat-related theme). However, it has to be pointed out that, over time, the dependency on cooling water from rivers will decrease.

3.1.4 Wildfires

Similarly to flooding, a decision was made to examine the effects of a serious wildfire in the case of the wildfires risk category. In the event of an out of control wildfire it is important to, in addition to trying to get the fire under control, limit its consequences by, for example, evacuating the exposed population. These are relevant aspects belonging to capabilities. See also paragraph 3.4.

3.1.5 Earthquakes

On the basis of publicly available sources the earthquakes risk category has been developed in detail for the NRP. This is described in paragraph 3.5.

3.1.6 Solar storm

When a solar storm occurs, it may result in satellite failure, in turn affecting communication systems. That is why this aspect is discussed in the disruption of critical infrastructure theme and not examined in greater detail here.

3.2 Flood

3.2.1 Risk

In the Netherlands a lot of attention is and has been and paid to water safety and the risk of flooding. An example can be found in the form of the Delta Works and the current Delta programme. The great flood of 1953 has been a major driving force behind this policy. This was a major flood originating from the sea, but flood risks also originate from rivers, as demonstrated by high water levels in 1995.

In order to provide an impression of the consequences of (near) flooding, the table below contains a number of key numbers concerning a few (near) floods in the Netherlands, Central Europe and the United Kingdom.

Because the flooding risks can be seen as a threat from the sea as well as a threat from the rivers, a choice was made for a 'worst-case' scenario in the form of a flood originating the sea and for a 'normative' scenario from the rivers. For both scenarios we revert to available scenarios from the NRB.

3.2.2 Capabilities

Legal and regulatory framework and policy

Delta Programme

The Delta programme has resulted in a number of 'Delta decisions' aimed at protecting the Netherlands more effectively against (the consequences of) flooding and to safeguard the provision of fresh water for the coming few decades (Delta programme, 2015). Important elements of the Delta programme are, in addition to the content-related proposals, the Flood Protection Programme [Hoogwaterbeschermingsprogramma], the Delta Act [Deltawet] and the Delta Fund [Deltafonds] which provide the legal foundation and financing of the (implementation of the) Delta decisions.

National Water Plan

In December 2015, the Minister of Infrastructure and the Environment and the State Secretary of Economic Affairs adopted the National Water Plan for 2016-2021 (NWP). The NWP contains the main elements of the national water policy and the corresponding aspects of the national spatial planning policy for the coming 6 years and looking ahead to 2050.

Prevention and preparation

New flood defence standards

The main focus of the Water Safety Delta Decision are new standards for water safety. These new standards were created by way of a risk-based approach: Standards are not only related to the possibility of a flood, but also to the consequences of a flood. The magnitude of the consequences determines the level of the standard. The new standard is aimed at the year 2050 and concerns the primary flood defences, namely those along the coast, major rivers and large lakes. Expected climate change and soil subsidence as well as possible socio-economic developments are taken into consideration concerning this standard.

Space for rivers

Thanks to a large number of river-widening measures, the discharge capacity of the Rhine and Meuse in the Netherlands has increased in recent years. Most of these measures have involved a modification of the rivers (a deeper winter riverbed, stronger/higher dykes). However, Space for Rivers also includes a number of measures which only apply in extreme circumstances, such as the diversion and temporary storage of river water in the downstream stretches of the Rhine tributaries and the Meuse.

Table 3.2 Key figures of a few (near) floods. Amounts are not scaled. (Source: PBL Social disruption due to floods, 2014)

Catastrophe	Year	Damage (euros)	Number of fatalities	Number of people affected
Storm surge	1953	680 million	1835	600
High water in the River District	1995	900 million	1	250
Elbe flood (Germany)	2002	9 billion	27	330,108
Elbe flood (Czech Republic)	2002	2.4 billion	18	200
UK flood	2007	4 billion	7	340
Dyke failure at Wilnis	2003	unknown	0	1,500

Multilayer security
In this concept the land behind the dykes is protected from (the consequences of) flooding by investments in three layers: strengthening flood defences (layer 1), a water-robust spatial layout (layer 2) and adequate disaster management (layer 3).

Risk assessment
A European Floods Directive has been effective since 2007. In specific terms the Floods Directive obliges member states to draw up a provisional risk assessment, flood danger and flood risk maps (see *www.risicokaart.nl*) and *flood risk management plans* (see National Water Plan).

Planning
Various plans have been drawn up to limit the possibility of a (major) flood, to manage the possible consequences of a flood and to facilitate the recovery from these consequences after a flood. A number of examples of these plans are, at national level, the National High Water and Floods Protocol, at the level of the safety regions, the Regional Flood Coordination Plans, and for a regional cross-border flood (threat) the Coordination Plan for Dyked Area 14-15-44 (the area of the worst imaginable coastal flood).

Risk communication
The State, the water boards and the Delta programme inform citizens about the flood risk in the areas in which they live and work via the *www.overstroomik.nl* website.

Permanent dyke monitoring
The water boards initiate dyke monitoring once the water has reached a certain level. Monitoring is carried out by a large number of volunteers. This dyke monitoring is a 'fixed' element of the water boards' prevention policy.

Response

Large-scale evacuation
In recent years a number of projects and plans have been initiated and developed in relation to large-scale evacuation. For example, the National Operational Evacuation Plan - Waterproof [Landelijk Operationeel Plan Evacuatie – Waterproef] (LOPE-W) of 2009 was followed up by the Large-Scale Evacuation Framework [kader Grootschalige evacuatie] (2014), a Water and Evacuation [Water en evacuatie] project is being implemented by the Safety Consultation Council [Veiligheidsberaad], the Ministry of Security and Justice, the Association of Water Boards [Unie van Waterschappen] and the Directorate-General for Public Works and Water Management [Rijkswaterstaat] and in mid 2016 the Great Flood Evacuation Module [Module Evacuatie Grote Overstromingen] (MEGO) project was completed, including advice about the role of the main national infrastructure in the event of flooding.

International assistance
At a European level the Emergency Response Coordination Centre (ERCC) is in operation. This is an EU initiative aimed at rapidly offering emergency assistance in the event of disasters in Europe and elsewhere through the coordination of resources made available by the 31 countries affiliated to this initiative.

Information and alert systems
The provision and exchange of information between various actors (authorities, relief organisations) in the event of crises is being organised more and more in a central and uniform manner.

The setting up of the Netherlands Water Management Centre [Water Management Centrum Nederland], which is part of Directorate-General for Public Works and Water Management [Rijkswaterstaat] means the systems (models) used to calculate expected high water on the coast, rivers and the great lakes and to communicate the findings to stakeholders have been combined at a single location. In addition, information and warning processes related to the various flood threats (water systems) are now more uniform than they used to be.

Emergency measures
Water boards can take emergency measures to stabilise a dyke (for example by placing a bank of sand against the dyke on its land side) or by either preventing or slowing down the passing of water through the dyke (boxing in areas through which water is passing).

Aftercare
Since 2012, Dutch citizens have been able to take out insurance against damage due to flooding. Since 2015, this insurance has been referred to as 'flood insurance'.

The Disasters and Major Accidents (Compensation) Act [Wet tegemoetkoming schade bij rampen en zware ongevallen] (WTS) provides a structural arrangement through which the State can provide a payment to people who have suffered material damages due to flooding.

Knowledge
By way of a website on *climate adaptation services* (*www.climateadaptationservices.com*) access is provided to products and services of Dutch knowledge institutes, with a view to taking action on climate adaptation. In addition, via the New construction and restructuring

[Nieuwbouw en Herstructurering] subprogramme (Delta programme) and the Knowledge for Climate [Kennis voor Klimaat] research programme, a website on spatial adaptation has been developed (*www.ruimtelijkeadaptatie.nl*) which provides users with know-how on climate adaptation.

3.2.3 Determining factors and impact

When a flood occurs, its eventual impact depends on various factors, such as the source of the flood (originating from the sea, the IJsselmeer, a river), the affected area and with it the number of people affected.

Concerning impact, the possibility of evacuation is an essential factor as regards the number of victims and is linked to the speed of development as well as the predictability of a flood. In the analyses this is combined in the percentage of the affected population that can be evacuated. In general it is the case that the evacuation percentage in the case of a flood originating from the sea is low and high in the case of a river flood, due to the time available for evacuation.
These differences are the result of variation in the predictability of potential flooding, weather conditions and the degree to which an area can be evacuated (road capacity). However, this does not apply in all cases. As demonstrated by the normative scenario, the element of surprise can also have a major effect in the event of a river flood.
What also plays a role in this respect is the combination of the predictability of high water (which is much more predictable in the case of rivers than in the event of a threat from the sea) and the predictability of dyke failure. The scenarios have been developed on the basis of the evacuation percentages used in the NRB.

The NRB details a number of different flood scenarios. In order to present a picture of the bandwidth of the impact of flooding, a decision was taken to analyse both a 'worst-case' scenario and a 'normative' scenario. The 'normative' variant concerns a river flood (Lek Dyke). A flood originating from the sea, resulting in a large portion of the Randstad conurbation being flooded, is the 'worst-case' scenario.

Normative scenario: river flood

This scenario is based on a breach of the Lek Dyke near Nieuwegein, causing the flooding of part of the Lopiker and Krimpenerwaard and, following this, the flooding of a section of the Central Holland dyke ring. The scenario involves a river flood that cannot be easily predicted because the dyke can be considered to be weak even at low water levels. There is, therefore, a significant 'element of surprise' with little time to evacuate. In this scenario, horizontal evacuation is not, or hardly, possible due to the surprise dyke failure which takes place shortly after the decision to evacuate.

For the likelihood of a flood in the selected area in the manner as described in the scenario, a bandwidth was chosen on the basis of calculations of the failure probability of dykes in the area (within the National Safety Analysis for the Netherlands [Veiligheid Nederland in Kaart] (VNK)) programme, of 1/100 to 1/500 per year (NRB score 'somewhat likely').

Worst-case scenario: Flood from the sea

A flood of the western coast is very extreme but still conceivable as a consequence of an extreme storm/ hurricane. Flood defences will fail in several places, the assumption in the scenario for the West Coast is a water level with a likelihood of occurrence which is smaller by a factor of 10 than the normative water level related to the statutory level of protection. The probability of the occurrence of the water levels as used in the calculations is 1/100,000 per year. The many dyke failures and the duration of the storm surge in the scenario for the West Coast (and that of Dyke Ring 14) result in a probability that is considered as being less than 1/100,000 per year.

As stated, we are in line with the worst credible flood scenarios included in the NRB. Nowadays, the water sector uses 'maximum possible flood' as the upper limit, in addition to the 'worst credible flood'.

The 'maximum possible' coastal scenario consists of several scenarios (northern coast, western coast and IJsselmeer area), leading to a(n) (even) larger impact (as regards the flooded area and number of victims). Because the scores of the existing NRB scenario are already extreme (several 'catastrophic' criteria), we have linked with this already existing scenario.

These days the water sector uses 'maximum possible flood' as the upper limit. However, because the scores of the existing NRB scenario are already extreme (several 'catastrophic' criteria), we have linked with this already existing scenario.

The following tables show the impact estimates for both scenarios.

Table 3.3 Normative scenario – flood (river).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.				○			Based on the probability of failure of dykes in the area.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory				◉		Concerns an area of 600 km² with a duration of longer than 6 months.
	International position	○					
Physical	Fatalities			○			Several hundred fatalities (bandwidth 326-625 fatalities).
	Seriously injured and chronically ill people			○			Several hundred injured
	A lack of life's basic necessities		○				More than 100,000 will not have any water and food for several days.
Economic	Costs				◉		The total damage is estimated at 12 billion euros.
	Violation of vitality	◉					
Ecological	Violation of nature and the environment	○					
Socio-political	Disruption to daily life				○		A total of 325,000 affected people are in the area, experiencing the consequences in the fields of education, employment, etc.
	Violation of constitutional democratic system	○					
	Societal impact				○		There is temporary social unrest.

○ average to considerable uncertainty; ◉ minor uncertainty

Table 3.4 Worst-case scenario – flood – severe (sea).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	**Explanation**
Likelihood of the scenario occurring between now and 5 years.		◉					Based on the probability of failure of dykes in the area.
Impact assessment							
Security interest	**Criterion**	Limited	Substantial	Serious	Very serious	Catastrophic	**Explanation**
Territorial	Territory					○	Concerns the Western Netherlands (Randstad conurbation); 4,340 km² being out of bounds for an extended period.
	International position		○				Normal activities of embassies and international visits are hampered.
Physical	Fatalities					○	More than 10,000 fatalities.
	Seriously injured and chronically ill people					○	
	A lack of life's basic necessities					○	In total more than a million people affected and a failing drinking water supply in the affected area, taking months to a year to restore.
Economic	Costs					◉	damage estimated at 121 billion euros.
	Violation of vitality			○			Increasing national debt ratio due to various causes (breakdown of international trade, interruption of production, costs of government initiated evacuation measures, etc.). Furthermore, there are consequences for employment, both directly and in the medium term (due to the flood risk).
Ecological	Violation of nature and the environment					○	Several nature reserves affected for an extended period.
Socio-political	Disruption to daily life					◉	It concerns a large area in which all aspects of daily life are disrupted for an extended period.
	Violation of constitutional democratic system		○				The violation primarily concerns public order and security services, although other institutions will also be affected.
	Societal impact			○			A flood like this will lead to widespread social anxiety.

○ average to considerable uncertainty; ◉ minor uncertainty

3.2.4 In perspective

Concerning the development of flood risk in the Netherlands, a distinction is often made between two autonomous developments: climate change and socio-economic development.

Socio-economic developments refer to a combination of demographic, social and economic developments, such as the growth, composition and lifestyle choices of the population as well as changes in prosperity. The impact of flooding will increase due to population growth and increased concentration in certain areas (such as the Randstad conurbation), as regards both population density and economic activities.

Climate change has consequences for sea levels. Soil subsidence is also of importance for the relative increase in sea level (the rise in sea level compared to the land). Both developments are included in the determination of the new security standards for primary flood defences. In addition, the discharge of water through the rivers is also relevant. The expectation is that peak discharges will increase this century and that high water levels will occur more frequently. The management of peak discharges of rivers will probably be the greatest water safety challenge in the Netherlands in the coming years. Between now and 2050 river dykes will have to be reinforced in order to comply with the new standards (see the Water Safety Delta Decision [Deltabeslissing Waterveiligheid]). In the long term (between now and 2100) the expectation is that more space will be required for the rivers in order to cope with higher peak discharges.

Findings

The main findings are that both climate change and socio-economic developments (such as population growth and increased prosperity) will lead to an increase in flood risk, with the rivers representing the greatest challenge. At the same time a lot of measures are being implemented in the Netherlands now and over the coming decades to protect the country against flooding and to keep the damage caused by floods to a minimum, ensuring that the new standards are complied with. These standards take both an increase in the threat as well as the growth in the value of economic production and in the numbers of residents into account.

3.3 Extreme weather

3.3.1 Risk

Extreme weather comes in all shapes and sizes, such as black ice, hail, a snowstorm or a very severe storm. Black ice and a snowstorm are closely related. They are both linked to a weather front (transition from hot to cold air) and in terms of impact the affected area is isolated for several days. This mainly has consequences for daily life, for example traffic and logistical standstills as well as disruption to power supplies and telecommunication. A very severe storm is usually shorter in duration (a number of hours), resulting in a smaller impact. This is based on the assumption that the flood defences continue to function in the event of a very severe storm.

In the NRB the scenarios for black ice, a snowstorm and a severe storm are based on events that have already taken place. In 1987 the northern part of the Netherlands was covered in a thick layer of ice for a number of days. As regards snowstorms, the snowstorm of 1979 is regarded as one of the most serious in recent decades. At the time the northern part of the Netherlands experienced heavy snowdrifts for approximately 90 hours, resulting in the formation of snow dunes some of which were between 3 and 6 metres high. One of the last very severe storms to hit the Netherlands occurred in January 1990. One of the last occasions that Northwest Europe was affected by a hurricane was on 26-28 December 1999 when two storms raged across France and Central Europe in quick succession.

To give an idea of the impact extreme weather could have these days on urban areas such as the Randstad conurbation, a few characteristics of serious black ice in Toronto (2013) and snowstorms in Boston (2015) are summarised below.

As already stated, the decision was made to base the NRP on a 'worst-case' scenario for extreme weather, with an impact in the Randstad conurbation. A 'normative' scenario is not included in the NRP because its impact is expected to be more regional in nature.

Black ice in Toronto in 2013 as an example

A number of figures relating to the impact of very serious black ice in Toronto in 2013:

- The black ice lasted for 3 days and covered the ground with a 30 mm layer of black ice.
- This resulted in large numbers of broken electricity cables, with well over 1 million people being without electricity for 3 days and tens of thousands for more than a week.
- Economic damage: $106 million for the city of Toronto and $200 million for insurance companies.
- There was a breakdown of public transportation and traffic lights. Two hospitals had to switch to emergency power.
- There was concern about the accessibility of vulnerable groups.
- Health effects: breakdown of heating systems, falling blocks of ice, slippery roads, eating food that had gone off, danger of electrocution and danger of carbon monoxide poisoning due to electricity generators and barbecues being used in enclosed spaces.
- 1,000 people spent Christmas in emergency accommodation.

Snowstorms in Boston in 2015 as an example

A number of figures relating to the impact of the snowstorms in Boston in 2015:

- Public schools were closed for 9 days
- There were 3 fatalities.
- 150 roofs and buildings collapsed.
- For a period of one month shops generated 24% less turnover. For restaurants this was even 50%.
- The state of Massachusetts missed out on approximately 1 billion dollars of income.

3.3.2 Capabilities

Prevention and preparation

Because the underlying causes of extreme weather cannot be eliminated, the focus is on prevention and preparation. A number of important capabilities are:

- According to experts the power supply and ICT/ telecom infrastructures can cope quite well with a severe storm. High-voltage cables can cope with hurricanes (wind force 12 Bft) and, should damage arise, it can be repaired within 24 hours. However, we wish to point out that repair efforts are dependent on the accessibility of the locations in question, which that can be problematic in the event of extreme weather. The consequences of blown over trees pulling out ground cables that are primarily felt at local level. However, black ice can cause considerable damage to high-voltage cables.
- In this context we also wish to refer to the salt depots as a capacity, with which agreements have been made about the purchase, storage and distribution of salt stocks for/between various authorities.
- The Royal Netherlands Meteorological Institute (KNMI) issues general weather warnings for fifteen regions: The provinces, the IJsselmeer area, the Wadden Sea and the Wadden Islands. In addition to general warnings, separate wind and storm warnings are issued for shipping.
- The possible consequences of extreme weather are taken into account in the preparations for large-scale events.

Response and aftercare

Several parties are involved in this phase. The State and the local authorities have gritters, snowploughs, etc. at their disposal. The safety regions (fire brigade, Regional Medical Assistance Organisation (GHOR)) have the resources needed to save people. Critical sectors have taken measures to ensure that emergency power is available in the event of an electricity outage. At a European level the Emergency Response Coordination Centre (ERCC) is in operation.

The damage caused by extreme weather can, in general, be insured. If this is not the case, compensation be can be claimed under the Disasters and Major Accidents (Compensation) Act [Wet tegemoetkoming schade bij rampen en zware ongevallen] (WTS).
The usual capabilities related to major disasters are available to provide care for victims (such as hospitals that are specially prepared for calamities).

Knowledge

At an international level, a great deal of knowledge is available concerning the possible impact of extreme weather on (critical) infrastructure. However, the question is to what extent this knowledge can be accessed and used in the Netherlands. In the Netherlands there are calls for a Community of Practice in which knowledge about the risks and mutual dependencies of different sectors is shared. This concerns, among other things, knowledge of the effects of extreme weather on critical infrastructure, which can be used to prepare for extreme events, particularly at a local (municipalities) and regional level (safety regions).

3.3.3 Determining factors and impact

There are various factors which determine the impact of extreme weather, such as the duration and the number of people affected. We have taken as a basis a snowstorm which lasts several days and which affects more than a million people.

From the analysis of the NRB scenarios (black ice, snowstorm and heavy storms) it can be concluded that the impact of a snowstorm is the highest. That is why the worst-case scenario for 'extreme weather' is linked to this variant.

The NRB scenario was linked to the North-eastern part of the Netherlands. In this report, however, it was decided to have this scenario take place in the Randstad conurbation. This means that we base the scenario on a snowstorm taking place in the Randstad conurbation.

The impact estimate for this scenario is as follows (table 3.5).

3.3.4 In perspective

As far as the likelihood of extreme weather is concerned, we must differentiate between two expected developments related to climate change. On the one hand the expectation is that snowstorms / black ice will take place less frequently as time goes on. On the other hand very severe storms are expected to occur more often. At the end of this century, the number of heavy storms in the Netherlands could be 20-30% higher than at the end of the previous century and storm damage is also expected to increase. However, it should be noted that there is considerable uncertainty about expectations as regards the future situation surrounding storms in the Netherlands.

In addition, tropical storms may constitute a serious threat for Western Europe in the future. This is because the part of the Atlantic Ocean where the seawater is at least 27°C (the threshold value for the creation of tropical cyclones) is extending eastwards, as a result of which cyclones will retain more of their original power than the 'current' cyclones which need to cover a longer distance before reaching Europe.

The influence of socio-economic developments on the risk of extreme weather can only be estimated in a qualitative manner. Relative to the events on which the NRB scenarios are based (such as the snowstorm of 1979), dependency on electricity and ICT and the use of transport infrastructure have increased. This could have consequences for the disruption of daily life.

Flooding due to extremely heavy rainfall has not yet been included in the list of scenarios for extreme weather. This is because these events occur locally and are consequently regarded as unsuitable for inclusion in a national risk profile, but rather in the regional risk profiles instead. A combination of serious flooding events can, however, lead to damage at national level.

Table 3.5 Worst-case scenario – extreme weather (snowstorm).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					○		Based on historical cases the occurrence of extreme weather is 'likely'. In the NRB black ice, snowstorm and severe storm are all estimated as 'likely'.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities	○					Several deaths (<10).
	Seriously injured and chronically ill people		○				Several dozens of wounded.
	A lack of life's basic necessities				○		The area (Randstad conurbation) home to a large group of people is isolated for several days.
Economic	Costs			○			Damage is estimated at slightly more than 1 billion euros.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life				○		In the area the daily life of more than one million people has been completely brought to a standstill for several days (education, work, shops, etc).
	Violation of constitutional democratic system						Not applicable.
	Societal impact	○					In addition unrest there will also be a sense of community spirit.

○ average to considerable uncertainty; ○ minor uncertainty

3.4 Wildfire

3.4.1 Risk

In the Netherlands there have been various large wildfires in recent years. Examples are the dune fires at Bergen/Schoorl in the province of Noord-Holland (late summer 2009, April 2010 and April 2011), on the Strabrechtseheide in Noord-Brabant (July 2010), in the Drentse Fochteloërveen (April 2011), the peatland fire in the Aamsveen nature reserve near Enschede (June 2011) (PBL, 2012b) and the forest and heathland fire in the Hoge Veluwe national park (April 2014).

The NRB describes one wildfire scenario. This 'Uncontrollable wildfire and large-scale evacuation' scenario analysis is linked with the heat/drought scenario. Similar to the heat/drought scenario, 1976 has been chosen as reference year because in that year a wildfire actually occurred close to Arnhem, at the Roozendaalse Veld. In the chosen scenario the fire brigade is able, at most, to manage the wildfire but not put it out. In total approximately 10,000 people have to be evacuated. The scenario is representative for areas such as the Veluwe, Utrechtse Heuvelrug and Sallandse Heuvelrug.

Because the NRB scenario can be regarded as normative, the upper limits of this scenario have been estimated for the NRP. This concerns the occurrence of cascade effects as regards critical infrastructure and a care institution. We regard this as the worst-case wildfire scenario.

3.4.2 Capabilities

Prevention

Nature conservation

Initiatives have been taken in various regions to limit the size of any wildfire through measures in the field of nature conservation: Replacing coniferous trees with deciduous trees, creating more wet areas and corridors in forests to ensure that a fire cannot spread. However, these can be counteracted by nature conservation measures with an opposite effect: the connecting of nature reserves via heathland areas (with a relatively high risk of fire) undertaken within the framework of the Ecological Main Structure increases the possibility of large-scale fires.

Risk communication

Wildfire Risk Index Cards [Risico Indexkaarten Natuurbranden] (RINs) are intended to prevent wildfires. The RIN instrument is used to divide nature reserves into square kilometre sections. For each section an assessment is made of wildfire risks, such as the combustibility of the vegetation, the chance that a fire will spread quickly, how quickly the fire brigade can be at the scene to combat the fire, the availability of water which can be used for firefighting, the accessibility of the terrain, etc. The implementation of this initiative is still at an early stage.

In periods of major forest fire risk citizens are warned to be careful with naked flames in nature reserves. A national communication strategy has been devised, referred to as the 'National Wildfire Message' [Landelijke Natuurbrand Boodschap] (2013), which is used as a uniform framework for preventive risk and crisis communication in the Netherlands.

Preparation

There are no specific plans related to combatting wildfires. Relevant aspects in this context are: cooperation and guaranteed advice, fire risk management, risk communication and the encouragement of self-reliance, and alarming/informing nature conservators.
A number of safety regions make use of wildfire risk maps. The level of preparation can be linked to a drought index.
There are excellent real-world examples of public-private partnerships in relation to wildfires, for example between the fire brigade, provincial authorities, entrepreneurs in the leisure industry and site managers in the Veluwe Wildfire Risk Management Committee [Commissie Risicobeheersing Natuurbranden Veluwe].

There are currently no specific evacuation plans for wildfires. Generic plans for (large-scale) evacuation or specific plans related to another threat (such as flooding) cannot be used for wildfires because, among other things, the response time in the event of a wildfire is extremely short and the people who have to be evacuated are often unfamiliar with the area where they are staying in.

Response

New possibilities are available for raising the alarm if a new fire is discovered, such as sharing information via mobile phones / social media, detecting changes in air quality and video detection. The systematic use of these resources is still in the development stage.

Additional fire-fighting resources can be made available via civil-military cooperation, for example in the form of a helicopter with firefighting capabilities.

Aftercare
Private parties, companies and authorities can take out insurance against wildfire damage. The usual capabilities related to major disasters are available to provide care for victims (such as hospitals that are specially prepared for calamities).

Knowledge
There are possibilities for European cooperation, with the international contacts of a number of safety regions in this field providing an interesting basis. Furthermore, results of international research can be used to create measures to reduce the risks of wildfires. However, this knowledge is still insufficiently accessible for planners, policymakers, the emergency services, site owners and entrepreneurs in the leisure industry. According to experts who participated in the sessions during which the NRB scenarios for natural disasters were discussed within the framework of this pilot, knowledge about (the prevention of) wildfires is often held by individuals.

3.4.3 Determining factors and impact
The table below summarises the determining factors for a wildfire. The elements of the wildfire scenario are highlighted in the table.

Wildfire scenario variant
This scenario variant builds on the existing NRB scenario, but the consequences are greater. The main elements are as follows. It concerns a fire in a large nature reserve (Veluwe) with tourists present at the various campsites. They can be regarded as less self-reliant because they do not know the area. People in several retirement homes on the edge of the nature reserve are also at risk. Due to the limited accessibility of the threatened areas for the purpose of evacuating citizens and tackling the fire ('accessibility and manageability') there are several dozen fatalities and seriously wounded. What is more, a substation for both electricity and the extraction of groundwater fails and road and rail connections are unusable.

3.4.4 In perspective
Due to climate change the risk of forest and peatland fires in Northwest Europe is likely to increase during the course of this century. In addition, there have been a number of specific developments. The grassing over of nature reserves has increased the chance of a wildfire breaking out (dry grass burns faster than bushes and trees). The fact that nature reserves have been linked together increases the possibility of major wildfires because the links are often created via heathland areas and experience has shown that heathland areas were often involved in major wildfires.
In this context we would like to point out that, although our elaboration is based on one major fire on the Veluwe, it is also conceivable that major wildfires may start simultaneously. This produces additional questions as regards capabilities, for example as to whether the various regions can or cannot support each other.

With regard to impact the development of tourism is of particular importance. In the coming decades the risk of wildfires may increase due to (foreign) tourists spending more time in nature reserves as a consequence of climate change (a longer period of nice weather during the summer), perhaps leading to increased numbers of campsites or holiday parks.

Table 3.6a Wildfire scenario variant.

Location of the wildfire	Size of the area	People affected	Vulnerable objects	Accessibility and manageability
Forest and heath (Veluwe, Utrechtse Heuvelrug, etc.)	< 10 km^2	<10,000	Campsite	High
Dune area (Bergen, etc.)	< 50 km^2	< 100,000	School	Medium
	>50 km^2	> 100,000	Retirement home	Low
			Prison	
			(critical) infrastructure (electricity substation, groundwater extraction)	
			Museum	

Table 3.6b Wildfire scenario.

Likelihood assessment						
	Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.			◎			Research shows that the probability is once every 25 years on the Veluwe with the probability being higher in years with lengthy droughts (once every two years). Due to the size of the fire a choice was made for 'somewhat likely'.

Impact assessment							
Security interest	**Criterion**	Limited	Substantial	Serious	Very serious	Catastrophic	**Explanation**
Territorial	Territory		◎				Based on a fire on the Veluwe.
	International position						Not applicable.
Physical	Fatalities		●				Several dozens of fatalities.
	Seriously injured and chronically ill people		●				Several dozens of wounded.
	A lack of life's basic necessities			●			In total 10-100,000 people are affected.
Economic	Costs		●				Remains limited (< 0.5 billion euros).
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment		●				It is assumed that some vegetation is lost forever.
Socio-political	Disruption to daily life			●			Daily life will be disrupted for several days.
	Violation of constitutional democratic system	◎					
	Societal impact		●				Citizens will be surprised that a wildfire can cause so many victims because they are relatively unaware of the risk. This leads to temporary social unrest.

● average to considerable uncertainty; ◎ minor uncertainty

3.5 Earthquakes

3.5.1 Risk

This risk category covers both natural earthquakes and earthquakes induced by people. Both of these have occurred in the Netherlands.

Tectonic earthquakes in Limburg

In the south of the Netherlands there are a number of active fault lines in the earth's crust, along which natural (tectonic) earthquakes can occur. The two largest fault lines in the Netherlands, the Feldbiss fault line and the Peelrand fault line, basically extend from Kijkduin (in the province of South Holland) to Kerkrade (in the province of South Limburg) and are primarily active from Uden (North Brabant) to beyond Roermond. The most severe earthquake in the Netherlands with a natural cause was the earthquake in Roermond in 1992 (see Table 3.7).

Induced earthquakes in Groningen

Long-term and large-scale commercial activities, in particular gas extraction, have resulted in earthquakes in primarily the North of the Netherlands. Natural gas extraction has caused movements in the sandstone layers, leading to fissures. The increasing tensions in these fissures cause earthquakes at relatively low depths (several kilometres). This type of induced earthquakes occurs regularly in the province of Groningen and the most severe one was in 2012 and measured 3.6 on the Richter scale (Table 3.7). The force of these induced earthquakes is relatively low (1-4 on the Richter scale). Recent reports by the KNMI, TNO and the National Mines Inspectorate [Staatstoezicht voor de Mijnen] have revealed that, as a consequence of gas extraction, earthquakes with a force of between 4 and 5 on the Richter scale are possible.

Earthquakes as a partial cause of other incidents

Mining activities in the past, in combination with (light) earthquakes, can lead to acute soil subsidence. An example of this is the collapse of part of the 't Loon shopping centre in Heerlen (South Limburg) in December 2011. The sudden soil subsidence was very likely due to a combination of various factors, namely an unfilled, shallow mineshaft under the shopping centre, the erosion of the limestone layers in between and the light natural earthquakes in the same area.

Historical cases

The table below shows an overview of the most severe earthquakes in the Netherlands.

Table 3.7 The four most severe earthquakes in the Netherlands with a natural cause (tectonic), or a non-natural cause (gas extraction). Not all earthquakes had their epicentre in the Netherlands.

Past earthquakes	Cause	Magnitude (Richter scale)	Damage and impact
Roermond, South Limburg (13 April 1992)	Tectonic	Fairly powerful: 5.8	The most powerful (tectonic) earthquake in the Netherlands up until 2016. Damage: € 77 million.
Uden, North Brabant (20 November 1932)	Tectonic	Fairly powerful: 5.0	Damage in the area around Uden and Veghel.
Alsdorf, North Rhine Westphalia, Germany (22 July 2002)	Tectonic	Average: 4.9	Felt in Voerendaal and Heerlen. Cracks in walls and dislodged roof tiles.
Goch, North Rhine Westphalia, Germany (8 September 2011)	Tectonic	Average: 4.5	Felt in Nijmegen and other parts of Gelderland. No reported damage.
Huizinge, Groningen (16 August 2012)	Gas extraction	Light: 3.6	The most powerful (induced) earthquake in the Netherlands up until 2016. 800 reports of damage.
Westeremden, Groningen (8 August 2006)	Gas extraction	Light	A total of 400 reports of damage (to the NAM).
Hellum, Groningen (30 September 2015)	Gas extraction	Light: 3.1	Reports of damage still being received.
Hoeksmeer, Groningen (24 October 2003)	Gas extraction	Light: 3.0	Minor material damage.

Earthquakes, measurement of magnitude and intensity

The Richter scale is the best-known scale for expressing the magnitude of an earthquake. This scale is logarithmic and runs from 1 to 12. The intensity of an earthquake is measured using the Mercalli intensity scale. This scale can be used to measure the effects on, for example, people, objects, buildings and the landscape and also runs from 1 to 12 but uses the Roman numerals I to XII.

3.5.2 Capabilities

The Ministry of Economic Affairs (EZ), the Ministry of Foreign Affairs (BZK), the National Mines Inspectorate (SodM) and the KNMI are the relevant actors as regards managing the risk of earthquakes and capabilities in the context of a response.

Prevention and preparation

As a society it is difficult to prepare for an earthquake. The safety regions in areas with an increased risk of earthquakes, such as Groningen and Limburg, have formulated a number of recommendations on how to act during an earthquake. Furthermore, the KNMI provides knowledge and technology and, via an extensive measurement network, measurements, data and prognoses.

The Ministry of Economic Affairs is responsible for policy related to gas extraction and determines the amount of gas extraction every year. As a preventive measure aimed at reducing the frequency of earthquakes due to gas extraction, the Minister of Economic Affairs has ordered a reduction in gas extraction in the Groningen gas field for the year 2015/2016 to 24 million m3.

In addition, the Minister of Economic Affairs, together with the 'Netherlands Standardisation Institute' (NEN) and the experts involved, drew up and published a Dutch Practical Guideline [Nederlandse Praktijkrichtlijn] (NPR 9998: 2015) in December 2015. The NPR can be used in conjunction with existing constructions to calculate whether the building adheres to the safety standard is subjected to the maximum expected load or, if not, whether reinforcing measures have to be taken. The National Mines Inspectorate (SodM) monitors compliance with statutory regulations which are applicable to the detection, extraction, storage and transportation of mineral resources. The SodM also carries out inspections and audits.

The National Coordinator for Groningen heads the Government Agency for Groningen and is responsible for the activities which are intended to improve the security and quality of life for people living in the province of Groningen. The Groningen Safety Region has set up an information number for information about what to do before, during and after an earthquake.

Incident response (repression)

In the case of earthquakes (and other natural disasters) the regular chain of emergency organisations will come into action and is therefore not included here. Concerning response, a number of specific recommendations have been made about, for example, looking for a safe place in your home during an earthquake.

The SodM investigates violations, accidents and hazardous situations in relation to mining or natural gas operations and takes measures as necessary.

Aftercare

The safety regions make sure that victims are taken care of via the relief chain and that safety checks are carried out on buildings and other critical infrastructures after an earthquake. At the beginning of 2016, the Minister of Economic Affairs submitted an amended bill for the reversal of the burden of proof related to earthquake damages in Groningen. As a result, affected residents would no longer have to demonstrate that damage to their home was a consequence of gas extraction. The National Coordinator for Groningen is going to produce a method for dealing with disagreements about compensation for damages. The independent implementing body known as Centrum Veilig Wonen (CVW) took over the responsibility for dealing with complaints from the NAM at the beginning of 2015. The Independent Adviser [Onafhankelijke Raadsman] deals with complaints about the way in which current compensation claims are being handled by Centrum Veilig Wonen and the NAM. He is also assisting in improving the way claims are processed by CVW.

3.5.3 Determining factors and impact

In order to create a better understanding of the building blocks relating to the risk estimate of earthquakes, the nature, cause, consequence, scope and impact of past incidents have been compared. This has resulted in the following building blocks:

Type of earthquake

Tectonic earthquakes have natural causes, originating from so-called plate tectonics. Induced earthquakes in the Netherlands are related to gas extraction.

Source

The hypocentre of an earthquake is the location under the earth's crust, between two or more tectonic plates, where a quake originates. The epicentre is the point on the earth's surface, immediately above the hypocentre (underground) of an earthquake.

Depth

Quakes in the higher layers of the earth's crust are often felt more than quakes that occur in deeper layers. They can also cause more damage.

Magnitude

The magnitude of an earthquake is often indicated on the Richter scale, a logarithmic scale which runs from 1 to 12. The magnitude according to the Richter scale is independent of the place on earth where it is calculated and is therefore a characteristic of the force of the earthquake itself.

Intensity

The intensity of an earthquake is indicated on the Mercalli intensity scale and is a measure for observations at a certain location. It is a measure of the effects on, for example, people, objects, buildings and the landscape. The intensity of an earthquake depends on the distance to the epicentre and on the type of substrate.

Exposure

Location

An earthquake in a densely populated area has a higher impact on society than one that occurs in a sparsely populated area. Furthermore, affected areas may experience secondary incidents, such as fires and explosions due to burst (gas) pipes, or flooding if dykes or quays are compromised.

Frequency

Normally 'frequency' is linked to the likelihood of the occurrence of a scenario.
In this case, however, a decision was made to refer to frequency as a factor for measuring the occurrence of all earthquakes. The focus is, therefore, not specifically on serious earthquakes which can lead to social disruption, but also on less serious earthquakes which can still have consequences for people in its vicinity. It has also been concluded that the number of times that people suffer damages due to quakes has an effect on their health. In particular residents who have experienced damage several times experience health problems more frequently.

Scenario variants

Depending on the way in which building blocks are combined (in the form of scenario variants) this will have an impact on physical safety (fatalities and wounded), economic security and socio-political stability (disruption to daily life and social unrest). In the case of the latter this concerns, among other things, the consequences of a high demand on the healthcare sector and cascade effects such as the failure of services and infrastructure due to large-scale damage.

Based on historical cases one can state that, in the Netherlands, the magnitude and intensity of earthquakes with a natural cause (tectonic), is higher than earthquakes with a non-natural cause (induced by, for example, gas extraction), although that may change in the future.

Normative scenario: earthquake (natural)

The severest earthquake with a natural cause was the earthquake in Roermond in 1992. This earthquake occurred at a depth of 17 kilometres in the Peelrand fault line and had a magnitude of 5.8 on the Richter scale and an intensity of VII on the Mercalli intensity scale.

In this normative scenario a natural (tectonic) earthquake is selected, with a slightly lower force (5.5 on the Richter scale), but an equal intensity. The hypocentre is at a depth of 10 kilometres in the Feldbiss fault line and the epicentre is a couple of kilometres to the south of the city of Sittard.
The earthquake results in startle responses and anxiety in the city and the surrounding area. The quake causes a number of water pipes in the centre to burst, as a result of which a number of streets flood and a shopping centre is temporarily closed due to flooding. The nearby industrial complex is more seriously affected and fires start at a number of companies on the complex which are subject to the Major Accidents (Risks) Decree [Besluit Risico's Zware Ongevallen] (BRZO). The earthquake also causes a number of small cracks in Motorway A76. Eventually there are 50 wounded and 1 fatality.

Costs relating to infrastructure and economic costs are estimated at several hundred million.

'Worst-case' scenario: earthquake – severe (gas extraction)

At the moment (2016) the frequency of induced earthquakes and the economic interests relating to the gas extraction in the North of the Netherlands play an important role in the debate on the possible safety risks for society.

Table 3.8 Normative scenario: earthquake (natural).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.				○			It has already occurred.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory	○					Functional loss of access to the area of the quake for a certain period of time.
	International position						Not applicable.
Physical	Fatalities	○					1 fatality.
	Seriously injured and chronically ill people		○				Dozens of wounded; also psychological problems.
	A lack of life's basic necessities						Not applicable.
Economic	Costs		○				Damage estimated at several hundred million.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life	○					Limited.
	Violation of constitutional democratic system						Not applicable.
	Societal impact		○				Temporary unrest and fear among the population.

○ average to considerable uncertainty; ○ minor uncertainty

Table 3.9 'Worst-case' scenario. Earthquake – servere (gas extraction).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.		○					Comparison with chemical accident, floods.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory		○				Earthquake area (< 100 km²) inaccessible for several weeks.
	International position						
Physical	Fatalities			○			Dozens to (slightly) more than 100 fatalities (105).
	Seriously injured and chronically ill people			○			Several hundred injured; psychological problems.
	A lack of life's basic necessities	○					Temporary; quickly rectified.
Economic	Costs			○			The repair of 1,100 homes and infrastructure (railway, road); health-related costs. A total of more than one billion euros.
	Violation of vitality						Not applicable (lost natural gas revenues fall outside scope).
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life		○				Several thousand people (< 10,000) who experience consequences for daily life for several weeks/months.
	Violation of constitutional democratic system		○				Affected population largely distrusts national government bodies. They feel ignored at every level. Administrative processes are hampered.
	Societal impact			○			There is a serious degree of fear, anger and apathy among the affected population.

○ average to considerable uncertainty; ○ minor uncertainty

In this 'worst-case' scenario the approach is similar to the one adopted by the safety region and a choice was made for an earthquake induced by gas extraction with a force of 5 on the Richter scale. The intensity of the earthquake is fairly high, namely VIII on the Mercalli intensity scale, because the earthquake takes place at a depth of 3 km in the gas extraction area.

The earthquake occurs in the north of the Netherlands, in the gas extraction area where the NAM is working in parts of the southern portion of the Groningen gas field. A powerful earthquake occurs, the epicentre of which is 3 kilometres under a village.
1,100 older houses are severely damaged, or collapse. The earthquake causes large cracks and holes in Motorway N33, reducing the accessibility of the village for external emergency services. Due to damages to the railway lines, the supply of relief (goods) by rail is also seriously limited.

The quake causes cracks in a number of water and gas pipes on the nearby industrial estate and a number of fires start at some of the commercial premises there. A total of 230 people are wounded, there are 105 fatalities and the financial damage is substantial. The material damage consists primarily of reconstruction work to buildings and local infrastructure.

Impact criteria

The scores of the likelihood and impact of the two scenarios are shown in the tables 3.8 and 3.9.

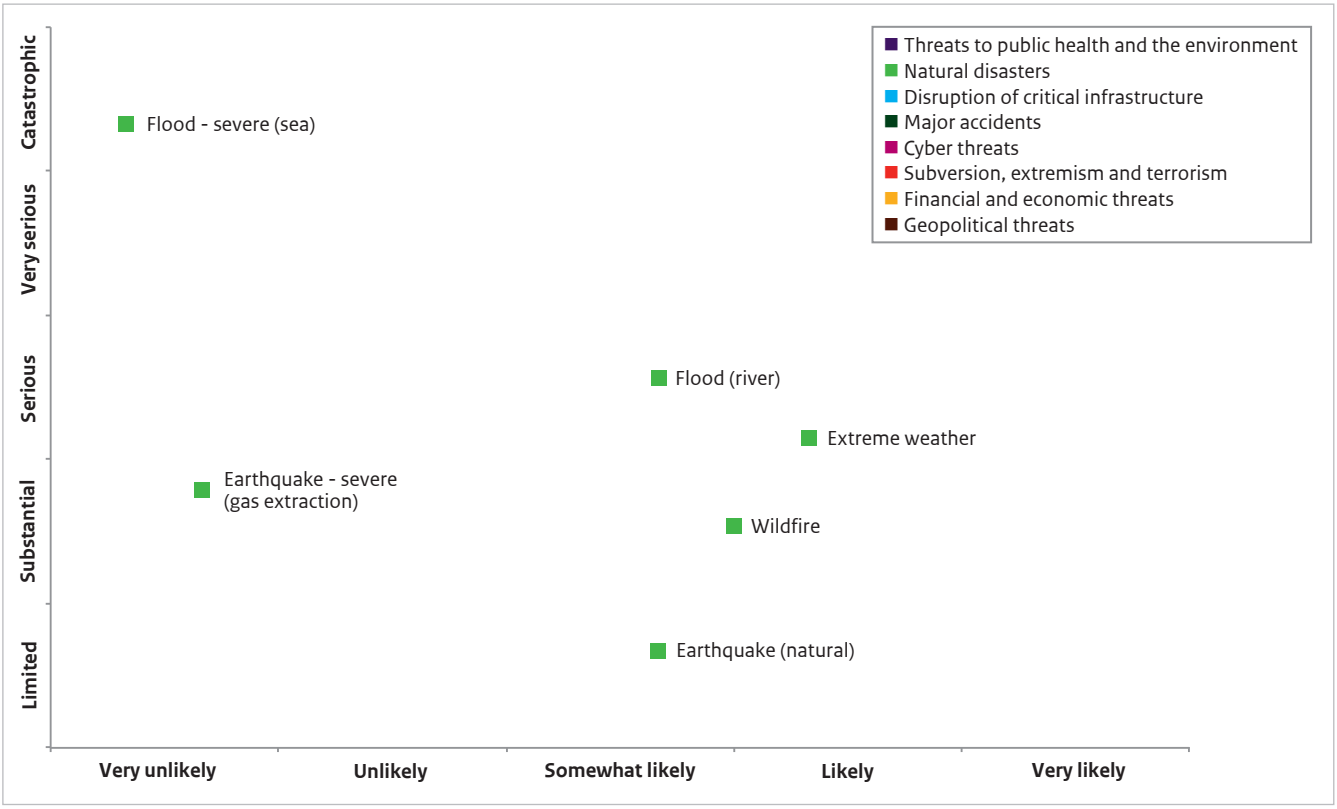
3.5.4 In perspective

Political and social discussions are taking place on the subject of natural gas extraction in Groningen in relation to safety risks, the reduction of, and the revenues from natural gas extraction. Studies are also taking place concerning measures to reinforce homes and buildings. In a slightly broader perspective the developments relating to power supply are important, as described in the disruption of critical infrastructure theme.

3.6 Conclusion and considerations

The results of the analyses of natural disasters are included in figure 3.1 below.

Figure 3.1 Natural disasters risk diagram.



4 Threats to public health and the environment

4.1 Risk categories

The Public health and Environment theme focuses on endemic and pandemic diseases, food crises and environmental disasters with a national impact. Within the National Risk Profile the accent is also on acute threats for public health and the environment which manifest themselves in the form of a crisis. Risk categories addressed within this theme include:

- Environmental disasters,
- Food crises,
- Antimicrobial resistance (AMR),
- Infectious diseases (human, animal diseases and zoonoses).

Many threats in the field of public health and the environment, such as air pollution, obesity, bee mortality, changes in ecosystems as a consequence of climate change, the effects of plastics in the ocean and the growth of greenhouse gas emissions are insidious developments which are high on the agenda of public health and the environmental policy. In time they can constitute a threat to national security – and are therefore included in the description of developments – but are not treated as a separate risk category.

4.1.1 Environmental disasters

Typical environmental incidents are oil spills and large discharges and leakages of chemicals into water, soil and groundwater. Explosions and the spread of toxic (gas) clouds fall under the 'major accidents' theme.

Many environmental incidents do not directly affect national security, but have a local or regional impact. An example where national security is jeopardised concerns an oil spill, whereby a large quantity of oil is released from an oil tanker and ends up in the sea or rivers. We regard this as a 'worst-case scenario'. In addition to financial damage for the company in question and unrest among the population, there will probably be a lot of environmental damage (national security interest of ecological security). The overall impact on national security will ultimately be limited, so this category is not developed in more detail in a separate chapter.

Developments

Despite the fact that they do not form an acute threat for national security, some developments within the environmental domain are relevant. As a first the environment is a theme whereby climate change and international relationships and developments are relevant. The agreements made during the climate summit in Paris reflect this and are intended to limit climate change by reducing emissions. This will have a knock-on effect via policy on, for example, industry and the energy sector. In addition, the (increase in) plastics in the seas and oceans (the 'plastic soup') is an international problem. The thematic in-depth assessment which the network of analysts carried out in 2013 describes the possible long-term impact via the food chain.

Environmental themes such as soil pollution, water and air quality are discussed in conjunction with various developments. Air quality is, for example, important for public health. Approximately 5% of the disease burden in the Netherlands is related to environmental causes, of which air quality in the form of particulate matter is the most important cause. This affects discussions on the maximum speed limit and low-emission zones in cities. Soil and (drinking) water quality feature in discussions of shale gas extraction and the underground storage of CO_2 or oil. Such examples are mainly relevant at regional level, but do lead to discussions at national level.

4.1.2 Food crises

In 2013 the network of analysts carried out a 'thematic in-depth assessment' for the theme of food security. This involved five scenarios being developed from a variety of perspectives. The scenarios jointly cover the range of possible causes where the food security

problem manifests itself, such as a deliberate contamination (STEC infections), a natural outbreak (Salmonella Typhi) and fraud (contaminated palm oil). Two process scenarios were also developed: (i) the development of acid-resistant micro-organisms and (ii) the long-term consequences of plastics in the oceans.

In the NRP we regard plastics in the oceans as one of the autonomous developments which may be relevant for national security in the long term (see under 'environmental disasters'). As far as the other food scenarios are concerned, the likelihood of occurrence is considered to be relatively high and this is in line with practical experience with regular food incidents.

The impact of these scenarios on a national scale is limited and is determined primarily by social unrest and fear. For example, food fraud has unpleasant consequences and citizens feel cheated. However, the impact on our national security interests is limited.
It can be deduced from the analysis that the food theme is important for the population. However, the expectation in the short term is that issues regarding food will not jeopardise national security. On the basis of the thematic in-depth assessment, the food theme is therefore, not treated as a separate risk category in the NRP.

Developments

A few autonomous developments could influence food supply and food security in the long run. For example, loss of biodiversity can lead to a significant impoverishment of natural environment and agriculture. Eventually this can lead to vulnerability, for example the Irish potato blight between 1845-1850 as a consequence of monoculture. Potato blight disease led to food scarcity and the death of more than a million Irish people.
A development like the increase in bee mortality can be linked to food supply with, among other things, possible consequences for fruit growing. Finally, climate change can cause food and water shortages elsewhere, which affect prices, and it can also lead to international tensions and migration flows.
Globalisation is relevant to the food sector. For example, a boycott of Dutch products has an effect on the sector. The same applies to international treaties, with the TTIP (Transatlantic Trade and Investment Partnership) being a current example. With regards to power relations within the food sector itself, one trend is that food production also centres around a few large actors.

4.1.3 Antimicrobial resistance (AMR)

Antibiotics are essential for the treatment of infectious diseases. However, using antibiotics has led to selection and the spread of resistant micro-organisms, which is a cause of concern. In some cases these resistant micro-organisms can cause infections which are difficult to treat. A 'thematic in-depth assessment' was also carried out for the Antimicrobial resistance (AMR) theme in 2013. It described eight scenarios which jointly cover the range of possible bottlenecks which can arise in the field of AMR cover and which were chosen from various perspectives (healthcare, environmental, veterinary) and differences in other issues (endemic/non-endemic).

The likelihood of the AMR scenarios is relatively high, but the direct impact on the national security is limited. Possible impact means the specific consequences for healthcare (emergency care, hospitals, the availability of medicines, sera and vaccines). The analysis also revealed that national security is only compromised in the situation in which the incidental events in the field of AMR are going to occur more frequently and simultaneously. The threat is therefore not in the various incidents themselves, but in the more frequent occurrence and coexistence/codevelopment of these incidents.

Because AMR only has a limited effect on national security, AMR has not been included in the NRP as a separate risk category. At the same time AMR can be regarded as a 'silent killer' and is therefore definitely important. AMR has now been recognised as an important issue and taken up by the authorities and policies are being intensively developed both internationally (WHO) and nationally.

4.1.4 Infectious diseases (human, animal diseases and zoonoses)

An infectious disease is caused by micro-organisms, such as bacteria, viruses, fungi and parasites which can cause symptoms if they enter certain areas of the body of person or animal where they do not belong.
A well-known example of an infectious disease is the common seasonal flu. Every year, on average of 820,000 people get flu and between 250 and 2,000 of people die as a result (or of its complications).

Infectious diseases can be categorised in various ways, for example on the basis of the transmission route, type of pathogen, or the organ where the illness primarily occurs.
Within the framework of this NRP analysis a distinction is made between 'animal diseases and zoonoses' and 'human infectious diseases'. The term ‘human infectious diseases’ covers the diseases which are transferred from

human to human. If transfer only occurs from animal to animal, we refer to animal diseases, while infectious diseases which can be transferred from animal to animal and/or from animal to humans are referred to as zoonoses. A recent example of a zoonosis is the Q fever outbreak among goats in the Netherlands which lead to sickness in people as well.

Both these risk categories ('animal diseases and zoonoses' and 'human infectious diseases') are explored in more detail below.

The conclusion that infectious diseases are the most important threats within this theme is in line with the regional risk profiles.

Within the public health and environment theme infectious diseases constitute the most important threats. This is in line with the regional risk profiles.

4.2 Animal disease and zoonosis

4.2.1 Risk

The Netherlands have an intensive agricultural sector, harbours a large number of (farm) animals and pets, and a high population density. In addition, the Netherlands are also a hub for the global transportation of people and animals. Animal diseases and zoonoses cannot be ruled out because of the intensive and global society of which the Netherlands are part. Even if extensive precautionary measures are taken and even in the event of an optimal response, incidents that can have an effect at national level are expected to continuously occur.

In recent years there have been outbreaks of animal diseases which required a national response. For example, an outbreak of swine fever occurred in 1997, a large-scale outbreak of foot and mouth disease in 2001 and the Netherlands were also hit by bird flu (H7N7) in 2003. The outbreaks of Q fever in the years between 2007 and 2010 also required a national response and a crisis management effort.

The consequences mainly affected the agricultural sector and in a few instances public health as well. Economic security was also affected because significant costs were incurred in combating the disease and there were direct consequences for the livestock population and the marketability of products. The economic damage varied from several million to billions of euros (swine fever in the Netherlands in 1997: 2.3 billion, foot and mouth disease crisis 2001: 1.2 billion euro in the Netherlands and 7.1 billion pounds in the UK). An outbreak of a zoonosis (infectious disease that can be transferred from animals to humans) may also have the potential impact on physical safety, given that people can become ill and may even die. In addition there is an increased possibility of disruption to the social and political stability due to unrest among the population. Culling may cause tension due to concerns about animal welfare and acceptance of the measure by the population and the farmers concerned. A number of agricultural sectors are currently under considerable financial pressure as a result of which an outbreak of an infectious animal disease may have an additional impact on a sector as a consequence of reduced resilience.

4.2.2 Capabilities

Recent developments and distribution of responsibilities

The capabilities have been recently revised, refined and set up based on earlier outbreaks such as the swine fever, foot and mouth disease and more recently the Q fever virus. The basis was the 'One Public health' approach which stands for an integrated human-veterinary risk analysis structure for zoonoses.

The ministerial responsibilities for the policy fields of public health and animal public health are clearly established. Combating zoonoses requires parties to share responsibilities. When considering whether a zoonosis has to be managed and which measures have to be taken, the focus is on the public health interest with the Ministry of Public health, Welfare and Sport having control. The shared human responsibility (municipality or Ministry of Public health, Welfare and Sport) and veterinary responsibility (Ministry of Economic Affairs) is specifically taken into account when setting up the crisis organisation.

Both the Netherlands Food and Consumer Product Safety Authority (NVWA) (veterinary) and the Municipality Health Services (GGD, human) are responsible for managing animal diseases. In the Netherlands the NVWA is responsible for supervision and law enforcement and is supported by various services and research institutions such as RIVM (National Institute for Public Health and the Environment), the GD Animal Health, the GGD (Municipal Health Service) and Wageningen Bioveterinary Research.

Pro-action, prevention and preparation

Surveillance of animal diseases is based on international cooperation. For example, the World Organisation for Animal Health (OIE), of which around 175 countries are members, provides clarity and transparency with regard to global animal disease and zoonoses.

Measures have been recorded (at national and international level) in the form of legislation, policy rules and protocols which reduce the possibility of introduction of dangerous animal diseases. Within the Netherlands general and specific crisis plans are available for certain types of diseases which enable the response organisation and other parties involved to prepare for an outbreak.

Response, crisis management

In 2011 the Ministries of Health, Welfare and Sport and Economic Affairs initiated an integrated human-veterinary risk analysis structure for zoonoses. This details the elements of a risk analysis structure, namely identification, assessment and risk management, types of partnerships, which are analogous to the way in which the risk analysis is organised in the context of human infectious diseases. The risk analysis structure has to make it possible to identify signals and possible infections (introduction) adequately and quickly, after which the response and any scaling up can be started on time.

The duty to report which is laid down in law with regard to a large number of animal diseases and zoonoses is an important element of this. The animal diseases which are not covered by the standard monitoring or a not notifiable may be detected and reported more slowly. Certain infectious animal disease can be a subject of mandatory management. This is the case when such a duty is laid down in a European Union directive or when it has been stipulated by the Minister of Economic Affairs. Well-known diseases for which there is mandatory management are foot and mouth disease, classic swine fever, African swine fever and avian influenza (also referred to as bird flu). The EU stipulates what a country must do as a minimum to manage an animal disease. Those EU directives are used as a basis to compile national policy protocols. These state what has to be done for each animal disease and who has to do it.

Guaranteed financing of the costs of managing an infectious animal disease or zoonosis is available from the Animal Health Fund [Diergezondheidsfonds (DGF)]. The DGF budget is derived from the business community, plus a contribution from the EU for management and activities and contributions from the government's general resources. Agreements are also in place relating to the use of specialised personnel, the availability of equipment and the capacity for processing dead animals.

Within the context of the human infectious diseases the generic key points have been identified for responses to infectious diseases, such as the availability of specialist care (respiratory equipment) and the possibilities for separate nursing (quarantine).

Aftercare

If a crisis occurs, an aftercare team is put together comprising representatives from the ministries involved, whose task is to develop a (general) action plan for the aftercare phase. After the crisis organisation has been scaled down, aftercare is often carried out within the framework of the regular policy responsibilities of the ministries and implementing bodies.

Knowledge

Sufficient knowledge is available in the Netherlands in the field of animal diseases and zoonoses. At most, the knowledge in specific specialist fields may temporarily be slightly narrow due to the changing focus and finances available for the various disciplines within this specialist field.

4.2.3 Determining factors and impact

After the initial infection the degree to which the infection can spread is one of the most determining factors for the scope and impact that can be expected. The variables and factors shown in Table 4.1 influence how an infection occurs and the extent of spread and they therefore form the triggers and determining factors (building blocks) for the creation and scope of an animal disease/zoonosis outbreak in the Netherlands.

The extent of spread is one of the important determining factors for the scope of the impact. Degree of spread is primarily determined by the question of whether the infection can be spread via the air transmission route and by the response time.

Table 4.1 General building blocks for impact of infectious animal diseases/zoonoses.

Cause	Origin	Type	Disease (human)	Transmission route	Location of introduction in risk area	Response time	Sector	Number of exposed people	Immunity
Natural	Int. transport (people and goods)	Animal-animal	Mild	Air	Yes	Days	Poultry	<100	Yes
Deliberate	Migrating birds	Animal-human	Serious (hospital)	Direct contact	No	Weeks	Cattle	100 -1,000	No
Technical	Vectors		Lethal	Food		Months	Pigs	1,000 -10,000	
				Water			Goats	10,000 -1,000,000	
				Vectors			Other (e.g. horse)	>1,000,000	

Scenario variants and their impact

An actual incident with an infectious animal disease consists of a combination of the building blocks described above. The type of danger of an infection determines, in particular, what kind of impact can be expected. For example, an infectious disease which spreads only among animals will mainly cause economic damage.
The scope of the impact is determined to a significant degree by the location of introduction, the pathogen transmission routes and the speed and effectiveness of the response (also determined by the speed of discovery and adequate response).

In order to provide a proper description of the scope of the possible impact of a crisis in relation to animal diseases and zoonoses, a 'normative scenario' and a 'worst-case scenario' have been developed and assessed.

Normative scenario: animal disease outbreak (foot and mouth disease)

A scenario for a 'normative effect' is created by an outbreak of an infectious animal disease which is restricted to the livestock population, which has spread for two weeks from a location where there are no extremely high densities of vulnerable animals and whereby the response is started directly (within one day) based on effective measures such as a transportation ban, culling and vaccination. As a normative scenario, a moderate to large outbreak of foot and mouth disease (FMD) has been chosen.
An overview of the combination of building blocks for this normative scenario are shaded in grey in the table below. These are the characteristics and effects which occur in the Netherlands.

Table 4.2 Building blocks for the normative scenario.

Cause	Origin	Type	Disease (human)	Transmission route	Location of introduction in risk area	Response time	Sector	Number of exposed people	Immunity
Natural	Int. transport (people and goods)	Animal-animal	Mild	Air	Yes	Days	Poultry	<100	Yes
Deliberate	Migrating birds	Animal-human	Serious (hospital)	Direct contact	No	Weeks	Cattle	100 -1,000	No
Technical	Vectors		Lethal	Food		Months	Pigs	1,000 -10,000	
				Water			Goats	10,000 -1,000,000	
				Vectors			Other (e.g. horse)	>1,000,000	

Table 4.3 Worst-case scenario building blocks.

Cause	Origin	Type	Disease (human)	Transmission route	Location of introduction in risk area	Response time	Sector	Number of exposed people	Immunity
Natural	Int. transport (people and goods)	Animal-animal	Mild	Air	Yes	Days	Poultry	<100	Yes
Deliberate	Migrating birds	Animal-human	Serious (hospital)	Direct contact	No	Weeks	Cattle	100 -1,000	No
Technical	Vectors		Lethal	Food		Months	Pigs	1,000 -10,000	
				Water			Goats	10,000 -1,000,000	
				Vectors			Other (e.g. horse)	>1,000,000	

Worst-case scenario: zoonosis outbreak (AI)

A combination of building blocks can, however, also lead to an even worst-case scenario relating to the type of impact and the scope in the event of an outbreak of a zoonosis (animal disease with transmission to and effect for people) with serious symptoms for humans which is introduced in a risk area for rapid spread, which is noticed after a long period and for which

effective measures cannot be taken quickly. The worst-case scenario chosen is an outbreak of bird flu with a variant of the H10 virus ('reassorted') which does not lead to very serious symptoms in animals (and is therefore not noticed) but which does have a considerable impact on public health. An overview of the combination of building blocks for this worst-case scenario are shaded in grey in table 4.3.

The following tables show the impact estimates for both scenarios.

A worst-case scenario, with a variant of avian influenza which does not lead to extremely serious symptoms in animals (and is therefore not noticed) but which does lead to extremely serious symptoms in people after a certain period of time, can lead to several hundred fatalities, thousands of ill people and a couple of billion in economic damage.

Likelihood of occurrence of scenarios

Given the precautionary measures taken and extra preparation, the possibility of a large outbreak as described in the normative scenario is expected to decrease in the coming five to ten years compared to the recent past but is still 'likely' with 20% to 50% probability of occurrence.

The possibility of an outbreak of a high pathogen avian influenza (bird flu) is substantial. This is partly caused by natural spread by migrating birds, which is difficult to control. In the context of preparations for calamities the assumption is that a new avian influenza infection will take place in the coming five to ten years. The probability that this will be an outbreak which can lead to a worst-case scenario is, however, smaller. For such an outbreak to occur there needs to be (1) an introduction of a reassorted H10 influenza type within Dutch poultry farming sector, (2) a high degree of spread within the poultry sector and (3) the possibility of a successful transfer via the environment to humans and to a location where it can then cause serious symptoms. The experts have assessed the total possibility of this worst-case scenario as 'somewhat likely'.

Table 4.4 Normative scenario – animal disease outbreak (foot and mouth disease).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					●		Experts estimate the probability now, given the precautions taken and extra preparation, to be between 20% and 50%.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory		◉				Restrictions, access area, transport, etc. (local) during 1 to 6 months.
	International position						Not applicable.
Physical	Fatalities	◉					No fatalities due to the foot and mouth disease crisis. Possibly an increased number of suicides.
	Seriously injured and chronically ill people	◉					No somatic illnesses as a consequence of the foot and mouth disease crisis, but some psychological effects.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			◉			1.6 billion (based on foot and mouth disease crisis).
	Violation of vitality	◉					The cattle industry suffers a loss, but is not entirely eradicated, nor does unemployment substantially increase. NB. For other animal industries (pigs) the financial pressure is so high that an outbreak of diseases may have extra consequences due to the reduced resilience.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life	●					Only a small group of affected people experience disruption.
	Violation of constitutional democratic system	●					In the case of unrest regarding wrong or contradictory decisions by the authorities.
	Societal impact		●				Sorrow, unrest and anger among affected people; dismay and indignation among part of the population.

● average to considerable uncertainty; ◉ minor uncertainty

Table 4.5 Worst-case scenario – zoonosis outbreak (AI, H10 virus).

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.				○			The possibility of a high pathogen Avian influenza outbreak is substantial, however, according to the experts, the combination of factors leads to 'somewhat likely' (B/C).
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory		◉				Restrictions on the grounds of access area, transport, trade, etc. (local) during 1 to 6 months.
	International position						Not applicable.
Physical	Fatalities			○			Several hundred fatalities based on expert estimate. Possibly increased number of suicides.
	Seriously injured and chronically ill people				○		More than 4,000 seriously ill people based on expert estimate.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			○			A few billion (of which 0.8 billion direct costs).
	Violation of vitality	◉					The poultry industry suffers a loss, but is not entirely eradicated, nor does unemployment substantially increase. NB. For other animal industries (pigs) the financial pressure is so high that an outbreak of diseases may have extra consequences due to the reduced resilience.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life		◉				Fewer than 10,000 affected people are unable to go to work, school, facilities, etc. for max. one month.
	Violation of constitutional democratic system	◉					In the case of unrest regarding wrong or contradictory decisions by the authorities.
	Societal impact			○			Considerable dismay and indignation among part of the population.

○ average to considerable uncertainty; ◉ minor uncertainty

4.2.4 In perspective

Scenarios relating to zoonosis and animal disease are also detailed in the regional risk profiles. Approximately half of the safety regions have included a zoonosis in a scenario and in most cases the Q fever outbreak from the 2007-2010 period is used as a basis, or a fictitious, more general variant thereof. Not surprisingly it is primarily the safety regions with very intensive livestock farming that have developed animal disease scenarios. The basis which is often used is a regional crisis caused by foot and mouth disease or swine fever.

The global developments in the field of vaccine production can be important for the capabilities. Globalisation and market forces have an influence on the control that can be exercised by government/the Netherlands on the availability of vaccines. The veterinary market in particular is sometimes of little interest to large vaccine producers. This may partially be related to the policy of not vaccinating against a number of infectious diseases. Centralisation is taking place and there are only a limited number of large producers on the global market. The choices made by these large companies can determine the availability of certain vaccines in the world.

4.3 Human infectious diseases

4.3.1 Risk

Although a relatively large number of people sometimes die from certain types of seasonal flu, the normal seasonal flu is not an infectious disease which causes social unrest or affects national security. The victims often die from a combination of the flu with other factors such as old age.

Examples of infectious diseases which have affected the feeling of social security in the (distant) past, but which are now under control (in the Netherlands) due to adequate treatment and improved health conditions, or which have been eliminated by vaccination programmes include the plague, tuberculosis and smallpox. However, there are still a number of very serious infectious diseases which can lead to a destabilisation of society in the Netherlands.

Diseases such as the 'Severe Acute Respiratory Syndrome' (SARS, 2003, China) and Ebola (West Africa, 2014) recently resulted in large numbers of victims and social unrest worldwide. With regards to influenza (flu) there have been several pandemics, for example the recent outbreak of 'Mexican flu[10]' (Mexico, 2009). In the 20th centuries there were three pandemics. The 'Spanish flu' (1918-1919) is often labelled as 'worst-case', with approx. 20,000 fatalities in the Netherlands. However, this pandemic took place at a time that medical science, care and resources were of a substantially lower standard than is now the case. The pandemics of 1957-1958 (Asian flu) and 1968-1969 (Hong Kong flu) resulted in fewer victims[11].

As soon as an infectious disease occurs in a higher frequency than normal, it is referred to as an epidemic. 'If an epidemic spreads across the world, it is referred to as a pandemic.

The scenarios in the NRP describe mild and serious influenza pandemics. Such a scenario is representative of the entire range of infectious diseases which can be a threat to national security with regard to causes, factors, mechanisms, consequences and capabilities. This choice corresponds to the regional risk profiles. Each safety region has developed one or more pandemic scenarios, whereby almost all safety regions take influenza (influenza pandemic) as representative of the scenario, with the scenarios from the NRB often being used.

An influenza pandemic is a good criterion for the causes, mechanisms and consequences which very serious infectious diseases can have on the scale of national security.

[10] Mexican flu, known officially as new influenza A (H1N1), is a flu virus that caused a pandemic in 2009. This type of virus came about due to an exchange of genetic material between a number of H1N1-flu virus variants, including human flu, bird flu and swine flu.

[11] CBS refers to a figure of 19,050 fatalities in the Netherlands due to Spanish flu and 1,230 fatalities as a consequence of influenza in the Netherlands in 1957. The pandemic of 2009 led to 63 fatalities in the Netherlands [NRB, 2011].

4.3.2 Capabilities

Spread of responsibilities

In the case of (the threat of) national crises, with a suspicion of an epidemic causing a threat to human health nationally, the Minister of Health, Welfare and Sport is responsible for tackling infectious diseases. Preventing and managing very infectious or serious infectious diseases in people is laid down in the Public Health Act [Wet publieke gezondheid] (Wpg) and the Animal Health and Welfare Act [Gezondheids- en welzijnswet voor dieren] (GWWD).

The GGD, GHOR and RIVM have an important role during the execution of all phases of the crisis management cycle (from pro-action to aftercare). RIVM's Centre for Infectious Disease Control [Centrum Infectieziektebestrijding] (RIVM-Cib), supports the (25) GGDs when it comes to controlling infectious diseases in the region. The Cib takes control, on behalf of the Minister of Health, Welfare and Sport, as regards tackling large-scale, cross-regional outbreaks of infectious diseases.

Pro-action, prevention, preparation

Surveillance and monitoring

For early surveillance of (new) infectious diseases, the Cib of RIVM has a national task to fulfil in the field of monitoring, surveillance, modelling and managing and improving the protocols. International epidemiological surveillance is organised via the WHO in order to identify and characterise new influenza variants.

Vaccination policy

Vaccination policy is an important aspect of prevention. Levels of vaccination among the Dutch population are high. Within the framework of the National Immunisation Programme children are given vaccinations against, for example, serious infectious diseases such as diphtheria, whooping cough, tetanus, polio, Haemophilus influenza type b and hepatitis B.

Preparation

In the weekly human infectious diseases alert meeting (SO), epidemics at home and abroad are discussed by experts from the Ministry of Health, Welfare and Sport (RIVM) and the Ministry of Economic Affairs (NVWA). In addition, experts from the veterinary and human domain come together on a monthly basis in the zoonoses alert meeting (SO-Z) to exchange information on signals in humans and animal at home and abroad.

The flu epidemic continuity plans also need to be mentioned here. Various social parties, such as government authorities, emergency services, healthcare institutions, critical sectors, educational institutions, as well as large companies have initiated these plans in response to the long-term and large-scale unavailability of personnel.

Repression and aftercare

In the Netherlands 43 infectious diseases (including zoonoses) have to be reported to the GGD. In the case of a (threatened) national crisis due to an infectious disease a national Outbreak Management Team (OMT) is formed, chaired by RIVM-Cib. This OMT provides advice during an Administrative Advisory Board [Bestuurlijk Afstemmingsoverleg] (BOA), which consists of national and regional administrators. The BOA then advises the Minister of Health, Welfare and Sport about management measures to be taken. If the infectious disease is a zoonosis, the zoonosis response team is activated.

Healthcare

The availability of specialist care (in particular the intensive care and respiratory equipment) can be a restrictive factor in the event of a serious influenza pandemic or other serious infectious disease. The same can also apply to the possibilities for separate nursing (quarantine) which will be required. Based on the capabilities, it is also important to note that upscaling via the military is an option for increasing the capacity for nursing.

Information

It follows from the report on the influenza pandemic in 2012 that advisory information produces dilemmas in the initial period of an incident, because it is not yet known what type of new virus is introduced and how serious the consequences can be. Wrong impressions can arise, partly due to the influence of social media and, in turn, lead to 'undesirable' behaviour with unintended side-effects. However, the government can use social media as well for communication about consequences and possible measures.

4.3.3 Determining factors and impact

The building blocks which determine the type of impact and the scope of the impact of a human infectious disease are shown in Table 4.6.
Depending on the way building blocks are implemented (in the form of scenario variants) an infectious disease outbreak will have an impact on the physical safety (fatalities and ill people), economic security and socio-political stability (disruption to daily life and social unrest).

Table 4.6 Building blocks of human infectious disease.

Cause	Origin	Pathogen	Transmission route	Response time	Infected people	Risk groups (yopi)	Immunity
Natural	Abroad	Influenza virus	Air	Days	< 100,000	Young	Yes
Deliberate	The Netherlands	Ebola virus	Direct contact	Weeks	100,000-1,000,000	Old	No
Technical		Coronavirus	Food	Months	1-5 million	Pregnant	
		...	Water		5-10 million	Immune compromised	
			Vectors		>10 million		

The latter concerns the effects of pressure on healthcare and cascading effects, such as loss of services and facilities due to large-scale unavailability of personnel.

Scenario variants and their impact

The NRB 2011 details two pandemic influenza scenarios: a mild and serious variant. These are used in the current analysis because they provide a good insight into the bandwidth of the impact of a human infectious disease crisis for the Netherlands. These two scenarios are based on a 'basic scenario' that is used as reference in NRB 2011. In this scenario 9.5 million people are infected, there are more than 18 thousand hospital admissions and more than 7 thousand fatalities. Consequently this ranges between mild and serious scenarios. The table below shows the routes of these two scenarios via the building blocks.

Both cases assume an influenza virus that originated abroad. Infection occurs abroad and is then spread in the Netherlands.
The two scenarios differ with regard to the number of infected people and the immunity (see difference between light and dark grey). These differences determine the eventual impact, in particular with regard to the number of hospital admissions and the number of fatalities.

In the case of the mild influenza pandemic the consequences are limited. This is different in the case of the serious variant. In addition to numerous fatalities and ill people (hospital admissions) there is mainly an economic and societal impact. This means the possible mass unavailability of personnel due to disease with consequences for work and education and considerable pressure on the public healthcare sector. These consequences are detailed in the estimate of the impact criteria as shown in the following tables.

Likelihood of occurrence of scenarios

in NRB 2011, probability of occurrence based on historical cases, was determined as one pandemic every 25 years. This means a likelihood of 20% during the coming five years.
The assumption was that the possibility of a mild or serious pandemic is equally divided. This assumption was stressed by the experts (March 2016). That leads to a probability of 10% of both a mild and a serious pandemic in the coming five years.

The probability of a mild or serious influenza pandemic occurring is the same. For both a mild and a serious influenza pandemic the estimate is 'likely'.

Table 4.7 Two scenarios for human infectious diseases.

Cause	Origin	Pathogen	Transmission route	Response time	Infected people	Risk groups (yopi)	Immunity
Natural	Abroad	Influenza virus	Air	Days	< 100,000	Young	Yes
Deliberate	The Netherlands	Ebola virus	Direct contact	Weeks	100,000-1,000,000	Old	No
Technical		Coronavirus	Food	Months	1-5 million	Pregnant	
		...	Water		5-10 million	Immune compromised	
			Vectors		>10 million		

Table 4.8 Normative scenario – influenza pandemic – mild.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					●		Based on the number of influenza pandemics in the last 100 years.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					Linked to the purchase of vaccines.
Physical	Fatalities			●			Approximately 200 fatalities.
	Seriously injured and chronically ill people			●			Several hundred hospital admissions.
	A lack of life's basic necessities	○					Scarcely relevant.
Economic	Costs	●					Only partially relevant.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life	○					Only partially relevant.
	Violation of constitutional democratic system	○					Not applicable.
	Societal impact	●					Based primarily on fear and uncertainty.

● average to considerable uncertainty; ○ minor uncertainty

Table 4.9 Worst-case influenza pandemic – severe.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					◉		Based on the number of (serious) influenza pandemics in the last 100 year.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					Linked to the purchase of vaccines.
Physical	Fatalities					◉	More than 14,000 fatalities.
	Seriously injured and chronically ill people					◉	Large number of hospital admissions (40-50,000); pressure on IC.
	A lack of life's basic necessities	○					Scarcely relevant.
Economic	Costs			◉			A few up to max. 5 billion euros, due to large-scale unavailability of personnel.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life					◉	Groups not going to work, school, facilities, ...
	Violation of constitutional democratic system	○					
	Societal impact			◉			Based primarily on broad social fear and uncertainty.

◉ average to considerable uncertainty; ○ minor uncertainty

4.3.4 In perspective

The likelihood of an influenza pandemic occurring is estimated as high. Based on several developments, the expectation is that the likelihood will significantly reduce. Due to climate change, in combination with globalisation (international transport and trade), 'emerging infectious diseases' may start occurring in the long run. A large and connected ecological network in Europe is increasing the possibility of the spread of infectious diseases (via vectors such as mosquitoes).

As far as social developments are concerned, urbanisation is, on the one hand, reducing the possibility of infectious diseases because people are coming less frequently into contact with nature and vectors which can spread diseases. On the other hand, urbanisation is actually making it easier for diseases to spread.
In addition, ageing is raising all kinds of issues related to healthcare in general. As far as this focus is concerned, ageing increases the size of the group of vulnerable people and that may have consequences for the number of ill people (hospital admissions) and fatalities in the event of a pandemic.

4.3.5 Conclusion and considerations

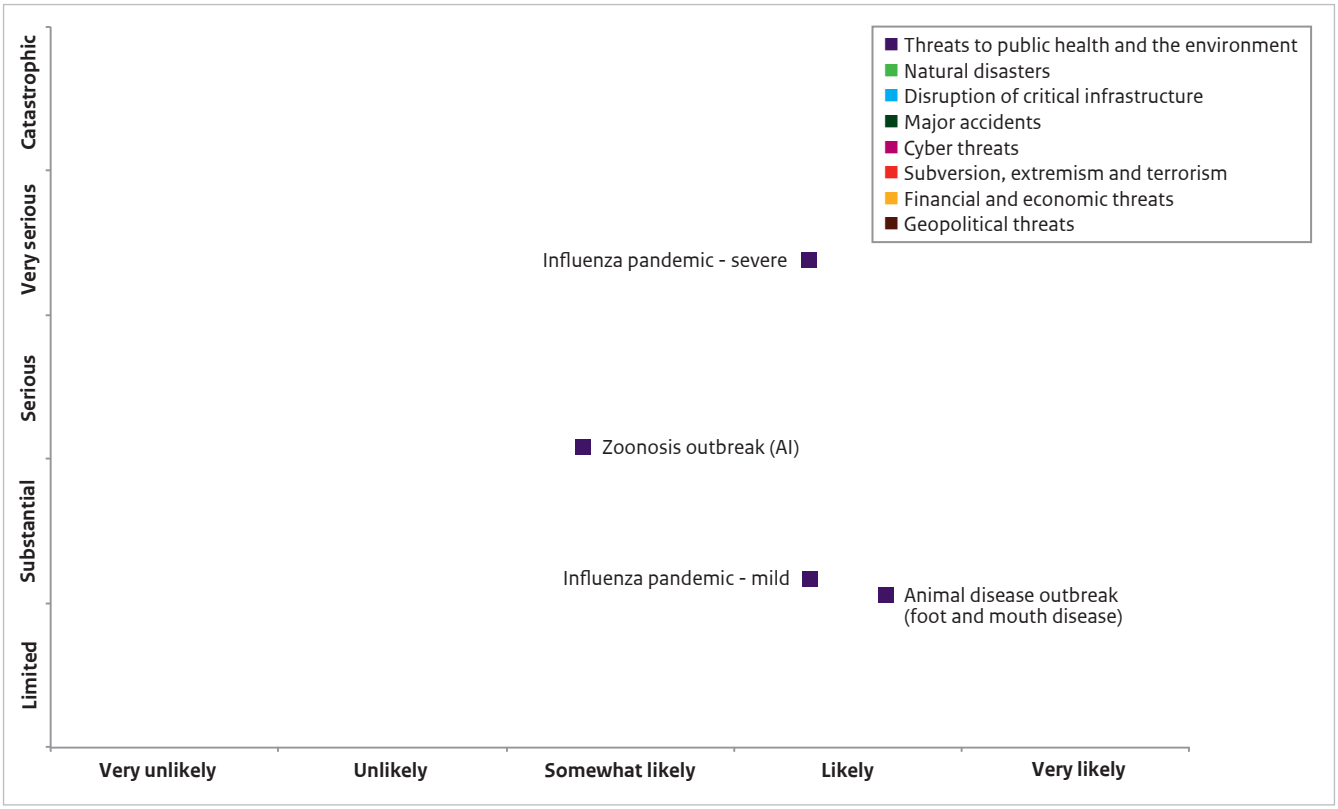
The risk categories of 'human infectious diseases' and 'animal diseases and zoonoses' are particularly relevant to the public health and the environment theme. The Netherlands are part of a global society. Consequently, infectious diseases represent risks which means that the proper preparation of a national response is essential.

The extent of spread is one of the important determining factors for the scope of the impact. The spread is primarily determined by the question of whether the infection can be spread via the air transmission route and by the response time. With regard to minimising response time it is particularly important to focus on the rapid 'discovery'/identification of an epidemic.

The capabilities for animal diseases and zoonoses have been recently revised, refined and organised according to the 'One Health' approach with an integrated human-veterinary structure. The focus is now on how the system works in practice and on refinement based on experiences in, for example, exercises. Well-known key points in the response are the availability of specialist care (in particular intensive care and respiratory equipment) and the possibilities for separate nursing (quarantine) which will be required. In addition, the security of supply and availability of vaccines has become more difficult to manage due to production now being in the hands of only a few players on a global market.

The risk diagram shows that the occurrence of almost all scenarios relating to infectious diseases is likely. Only the occurrence of the worst-case scenario for animal diseases is less probable (somewhat likely). The probability of occurrence in combination with the substantial impact which the scenarios have makes these risk categories important for national security and the subsequent capability analysis. The impact extends from, primarily, a 'serious' impact for the normative scenario relating to animal diseases and zoonoses to a catastrophic impact in relation to fatalities, seriously wounded and chronically ill people and the disruption of daily life for a worst-case influenza pandemic.

Figure 4.1 Public health and environment risk diagram.



5 Major accidents

5.1 Risk categories

The major accidents theme includes all accidents which may lead to large-scale social destabilisation. The term 'major accidents' is a collective term for events that are caused by system failure. In the case of system failure this means non-deliberate incidents and may be caused by (a combination of) technical, human or organisational failure. In addition, accidents can also occur as an effect of another event (such as, for example, a natural disaster). Within the major accidents theme a distinction is made into three risk categories:

- Nuclear disasters
- Chemical incidents
- Transport accidents.

The categories can be differentiated based on differences in risk nature, the effects and the necessary measures (regulations, expertise). Transport-related accidents, taken from the broader group of physical accidents, have been included in the National Risk Profile because, especially these can result in large numbers of victims and destabilisation. Other physical accidents are almost always on local and of a smaller scale, which means that they are included in regional risk profiles.

5.2 Nuclear disasters

5.2.1 Risk

In the case of nuclear disasters the focus is on the release of radioactive material into the atmosphere, soil or water. An incident with a (threat of) discharge of radioactive material can have serious social consequences. The focus is then on public health effects due to the direct exposure of people (inhalation of radioactively contaminated air), or due to indirect exposure (contamination in the food chain and drinking water). In addition to public health effects there may also be economic damage, ecological damage, reputation damage, social unrest in general (fear, dissatisfaction, anger) and loss of support for nuclear power and other applications of nuclear technology.

In the Netherlands there are 3 locations with nuclear reactors (the so-called A locations): the nuclear power station at Borssele (EPZ's KCB), the High Flux Reactor in Petten (belonging to NRG) and the Higher Education Reactor at the Reactor Institute Delft (RID). There are also a number of locations where radioactive material is processed, such as URENCO (production of lightly enriched uranium) in Almelo, COVRA (radioactive waste storage) in Nieuwdorp, as well as various laboratories and hospitals where certain quantities of radioactive material are located.
Finally, radioactive substances are sometimes transported (by rail, road, air and sea).

Incidents at nuclear power stations abroad also represent a risk of an impact on Dutch society.
A distinction can be made between the nuclear power stations just over the border in Belgium (Doel, Tihange) and Germany (Emsland-central in Lingen) which, in the event of incidents, may have a direct impact on the Netherlands (for example as a consequence of direct exposure of people) and incidents further away in Europe which may have an indirect impact on the Netherlands (for example as a consequence of safety measures relating to the food chain).

Historical cases

Luckily, large-scale radiation incidents do not occur very often. Nevertheless there have been examples in the past which illustrate the various types of incidents and possible consequences. One of the most well-known accidents is the Chernobyl disaster (1986). Steam explosion and fires led to more than 5% of the radioactive reactor core being released into the atmosphere. More than 30 people who worked at the site during the accident or who were involved in the incident control died immediately or within a few days. Approximately 200 other people suffered acute radiation syndrome. Although there were no cases of radiation syndrome outside the site, a large number of people were found to be suffering from thyroid cancer caused, in all likelihood, by the fall-out of radioactive iodine.

The more recent incident in Fukushima – which, in 2011, led to large-scale discharges from three out of six reactors into the air and the sea – and had various effects on humans and the surrounding environment. For example, large areas were evacuated (approx. 100,000 people will have to live elsewhere for many years) in order to reduce the radiation effects. The fact that these areas have become unusable for a considerable period of time has resulted in a serious impact on agriculture, livestock farming and fishery. In addition, there were more than 60 fatalities during the evacuation as well as a number of suicides. In addition to fatalities and disease, the incident also resulted in many people suffering long-term psychological problems.

Developments
The role of nuclear power in the worldwide energy mix is changing. In some countries steps are being taken to reduce the amount of nuclear power generated while, in other countries, nuclear power is actually regarded as a vital source of energy in the process toward sustainability (nuclear power does not cause CO_2 emissions).

Despite regular discussions about the issue in the media, for the time being nuclear power in the Netherlands is going to be kept at its current level. In the rest of Europe as well, the aim appears to be to keep total nuclear capacity stable, in any event for the coming 5 to 10 years.

At a technical level, research is being carried out into safe, small systems with buckyballs, the use of thorium and the combustion of long-life nuclides. As yet these are unproven techniques and they are not expected to be implemented in the coming fifteen years.

5.2.2 Capabilities

General picture and responsibilities
Security in relation to nuclear power is an important issue which is the subject of a lot of attention at national and international levels. There is a tradition of security thinking that translates into (legally) formalised capabilities in all links of the crisis management cycle. This tradition dictates that the facilities in the Netherlands have to function within the limits of the licence and that, just as in other countries, periodical security studies and inspections have to be carried out to provide a basis for further improvements in security. The Netherlands also have security ambitions and the Borssele nuclear power station has to become one of the 25% safest nuclear power stations in Europe, the United States and Canada (Borssele Nuclear Power Station Covenant).

Nevertheless, the security aspect of the nuclear power dossier is still developing. Recently there have been shifts in the organisational embedding and responsibilities. Since 1 January 2015 there has been a single body in the Netherlands which is responsible for policy and supervision in the field of nuclear security and radiation protection: the Authority for Nuclear Safety and Radiation Protection [Autoriteit Nucleaire Veiligheid en Stralingsbescherming[] (ANVS). As a result, expertise is now more concentrated. In the past knowledge about licensing and supervision of the nuclear sector used to be spread across a number of different bodies. In addition, the administrative responsibility for nuclear safety and radiation protection has been transferred completely from the Minister of Economic Affairs (responsible for energy policy) to the Minister of Infrastructure and the Environment (I&E). The generally existing processes and procedures therefore have to be embedded and arranged in the new situation.

A tradition of security thinking has been translated into a system of formalised capabilities. A new element of the policy context is the creation of a single Authority for Nuclear Safety and Radiation Protection and the transfer of political responsibility to the Minister of Infrastructure and the Environment.

Pro-action, prevention and preparation

Supervision and policy:
- The international nature of nuclear power (and the possible consequences in the event of calamities) means that many of the agreements relating to security and crisis response have been laid down and implemented internationally. The member states are also involved in their implementation. The International Atomic Energy Agency (IAEA) of the United Nations (UN) plays an important role in the coordination and harmonisation but also has implementing powers as regards monitoring authorities' compliance with the rules. For example, the IAEA is entitled to inspect nuclear installations in the member states.
- The Social Affairs and Employment Inspectorate [Inspectie SZW] and the Health Care Inspectorate [Inspectie voor de Gezondheidszorg] (the Ministry of Health, Welfare and Sport) are responsible for monitoring working conditions and the environmental burden within the Netherlands. RIVM carries out

supporting research on behalf of the Inspectorates.
- The ANVS monitors nuclear safety and security.
- The safety regions play an important role in ensuring coordination with the licensees at regional level.

Legislation and regulations:
- All applications relating to nuclear power and radiation sources are embedded in a system of licensing, supervision and enforcement. These are laid down in law and regulations such as the Nuclear Energy Act [Kernenergiewet] and the Radiation Protection Decree [Besluit stralingsbescherming].
- Refinement takes place where necessary (internationally and nationally). For example, the most recent European directives – the EU Basic Safety Standards (BSS) – must have been implemented in national legislation in the Netherlands by no later than the beginning of 2018. This is already being worked on and various points of the legislation and regulations are being adapted.

Response, after-care and evaluation

In the new division of administrative responsibilities the Minister of I&E has formal system responsibility for nuclear accidents and radiation incidents.
The Nuclear Emergency Response System [Responsplan Nationaal Plan Kernongevallenbestrijding] (NPK) is a subplan of the National Radiation Incidents Crisis Plan [Nationaal Crisisplan Stralingsincidenten] (NCS) and focuses on the response phase of radiation incidents. It describes the points of departure for dealing with radiation incidents in the Netherlands. The Safety Regions' Radiation Incidents Handbook [Handboek Stralingsincidenten veiligheidsregio's] was published at the beginning of 2016.

At the level of installations, safety regions, institutes (ANVS), countries and also internationally there are rules for alarms and information exchanges relating to nuclear accidents. In addition, systems have been arranged in the Netherlands, such as the National Radioactivity Monitoring Network [Nationaal meetnet radioactiviteit] which can ensure detection, additional measurement and analysis of incidents. The IAEA is responsible for international alarms and additional agreements are also in place between the Netherlands and its immediate neighbours regarding rapid alarms and information exchanges.

The response to a so-called category A-object (nuclear reactors) requires administrative coordination by central government in line with the agreements as described in the National Crisis Management Handbook [Nationaal Crisisplan Stralingsincidenten] and in the National Radiation Incidents Crisis Plan. An incident with a B-object is an incident with radioactive substances or applications with (possible) radiation consequences for the immediate environment which can lead to questions locally. Depending on the set GRIP level dealing with such incidents is the responsibility of the mayor or the chair of the Safety Region. Advice is provided by the Nuclear Planning and Advice Unit [Eenheid Planning en Advies nucleair] (EPAn), the Radiation Crisis Expert Team [Crisis Expert Team straling] (CETs), and/or the Radiation Duty Officer [Dienstdoend Ambtenaar Straling] (DDA Straling). A major nuclear accident is primarily tackled using general resources (fire brigade, police, medical). Other specific measures and capabilities are provided such as:
- The first response by a company emergency response team (via the licensee itself) that has the necessary resources, including cooling water and emergency generators.
- An emergency hospital with a capacity of 100 to 300 patients which functions primarily as a 'transit port' to regular hospitals.
- Agreements have been made with hospitals about caring for radiation victims.
- Iodine tablets are used to protect the population against contamination from radioactive iodine. With this in mind, iodine tablets have been distributed among the population at various locations (pre-distribution).
- The Institute of Physical Safety (IFV) is currently rewriting the Evacuation protocol. The safety regions have developed evacuation plans in consultation with third parties such as road operators and the military.
- The Netherlands have six large-scale decontamination units.

There are almost no capabilities available, specifically for recovery and aftercare following a radiological incident. Existing general capabilities for recovery and aftercare will be used. The generic policy relating to crisis response will therefore also serve as a guideline for aftercare following a radiation incident.

Knowledge

Specialist knowledge is required within this field of work and it is also important for sufficient experts and crisis managers to maintain an adequate level of knowledge.

5.2.3 Determining factors and impact

The radiation source (type and source term) in combination with, among other things, the weather conditions and the season, determines the type and degree of impact. Table 5.1 provides the details of all so-called determining factors for radiation incidents. A scenario consists of a combination of the building blocks. The coloured cells of table 5.1 show the scenario of an accident in the Borssele power station (see next paragraph for description of scenario).

Table 5.1 Determining factors for radiation incidents with the coloured cells showing the Borssele scenario.

Radiation source	Warning time	Cause	Source term	Rainfall in the Netherlands	Kind of weather	Time of day	Harvest time	Size of acute danger area (distance to source)	Size of affected area	People present (acute danger area)	People present (affected area)	Presence of critical objects in affected area (y/n)
Borssele Nuclear Power Station	None	Isolated incident	Zero/ Minimal	Dry	Summer conditions	Day	Yes	n/a	n/a	n/a	n/a	Drinking water supply
HFR Petten	6 hours	Chain effect as a consequence of an external incident	1 TBq	Downpours/ hotspots	Winter conditions	Night	No	Radius < 1 km	Radius < 5 km to the source	0	0	Power supply
HOR Delft	24 hours		10 TBq	Rain throughout the Netherlands	Normal			Radius between 1 km and 5 km	1% of the Netherlands	1 - 10	1 - 10	Water management
A-object just over the border	2 days		STC-CON1					Radius between 5 km and 10 km	10% of the Netherlands	10 - 100	10 - 100	Mainport Rotterdam
A-object further away in Europe			10 x STC-CON1					Radius > 10 km	Large part of /the whole of NL	100 - 1,000	100 - 1,000	Mainport Schiphol
A-object further away									Radiation from NL across the border	> 1,000	1,000 - 10,000	Other critical object
B-object											10,000 - 100,000	
Transport											100,000 - 1,000,000	
Uncontrolled source/contamination											> 1,000,000	

Scenario variants and their impact

In order to describe the scope of the possible impact of a radiation incident, the in-depth theme analysis details four scenarios which together cover the space with important characteristics of plausible scenarios which (may) have a national impact (see underlying report). These scenario variants form short scenarios which are only intended as an illustration. It concerns the scenarios of incidents:

1. 'Borssele': This concerns a nuclear disaster in the Netherlands involving the Borssele nuclear power station.
2. 'Just over the border': An accident with a nuclear power station just over the border at, for example, Doel or Emsland in conjunction with a wind blowing towards the Netherlands.
3. 'Further away in Europe': A very serious accident with a nuclear power station outside the Netherlands, within Europe (for example Germany, France or the United Kingdom), in conjunction with unfavourable weather conditions.
4. 'Transport': Transport accident in conjunction with the release of medical isotopes (molybdenum) during transportation.

The three scenarios involving nuclear reactors (scenarios 1 to 3) are different primarily as regards the type of effect that they could have. In the event of a radiological accident in the Netherlands or just over the border, consequences can be expected from both the direct exposure to radiation as well as the indirect consequences such as agricultural measures, image damage and the loss of trade (routes). In the event of an accident further away in Europe, there will only be indirect consequences. However, depending on the impact, these may be factors that determine certain aspects just as seriously or with even higher scores. The 'Borssele' scenario (nuclear disaster in the Netherlands) is detailed below as an example of an accident with direct and indirect effects plus the 'Further away in Europe' (nuclear disaster in Europe) scenario with only indirect effects. The 'just over the border' scenario is comparable with both these scenarios and is not developed in any more detail here, but is described in the theme reports. Although the possibility of an incident comparable with the 'Transport' scenario is greater than the other scenarios, the impact is so much lower that, as far as the impact scores are concerned, it

Table 5.2 Building blocks of 'Nuclear disaster in Europe' scenario.

Radiation source	Warning time	Cause	Source term	Rainfall in the Netherlands	Kind of weather	Time of day	Harvest time	Size of acute danger area (distance to source)	Size of affected area	People present (acute danger area)	People present (affected area)	Presence of critical objects in affected area (y/n)
Borssele Nuclear Power Station	None	Isolated incident	Zero/ Minimal	Dry	Summer conditions	Day	Yes	n/a	n/a	n/a	n/a	Drinking water supply
HFR Petten	6 hours	Chain effect as a consequence of an external incident	1 TBq	Downpours/ hotspots	Winter conditions	Night	No	Radius < 1 km	Radius < 5 km to the source	0	0	Power supply
HOR Delft	24 hours		10 TBq	Rain throughout the Netherlands	Normal			Radius between 1 km and 5 km	1% of the Netherlands	1 - 10	1 - 10	Water management
A-object just over the border	2 days		STC-CON1					Radius between 5 km and 10 km	10% of the Netherlands	10 - 100	10 - 100	Mainport Rotterdam
A-object further away in Europe			10 x STC-CON1					Radius > 10 km	Large part of /the whole of NL	100 - 1,000	100 - 1,000	Mainport Schiphol
A-object further away									Radiation from NL across the border	> 1,000	1,000 - 10,000	Other critical object
B-object											10,000 - 100,000	
Transport											100,000 - 1,000,000	
Uncontrolled source/contamination											> 1,000,000	

would not be included in the NRP and would be more suitable for inclusion in the regional Security Profile. In view of the central government's responsibilities for nuclear disasters and the sensitivity in relation to this type of incidents, this scenario has been included in the theme report, but then as the least serious variant.

Nuclear disaster in the Netherlands (Borssele) scenario variant

The Borssele scenario is an accident in the Borssele nuclear power station, leading to contamination outside the power station. The wind direction is extremely unfavourable, initially blowing towards the populated centres of Vlissingen/Middelburg and then changing, during the incident, towards the Port of Rotterdam area. There are several critical objects in the affected area: drinking water sources which may become contaminated, as well as primary flood defences and power supply facilities, with access to these being hampered, meaning that they cannot therefore be completely controlled. The Westerschelde tunnel will also be closed. Dutch airspace will also be closed for several days. The impact of the 'Borssele' scenarios is shown in table 5.3 on the next page.

Nuclear disaster in Europe ('Further away in Europe') scenario variant

The building blocks for this scenario are shown in colour in table 5.2. The 'nuclear disaster in Europe' scenario is an accident in a nuclear power station close to the Netherlands, but not just over the border, meaning that there are no direct consequences. However, it is still a very serious accident (10 times STC-CON1) in combination with wind direction causing the cloud to spread into the Netherlands. Then there is the unfortunate circumstance that it is hot, summer weather and that heavy, local rain showers are expected. Although the cloud is not a direct threat due to the distance, the locations at which the rain falls will become hotspot areas of contamination. Because it is difficult to predict where those rain showers will exactly fall and where they will result in contamination, agricultural measures will be instigated for a very large portion of the Netherlands. This is already having drastic (economic) consequences and is leading to unrest. The hotspot areas are temporarily unable to operate which can have significant consequences primarily in the case of densely populated urban areas (for example a hotspot in Rotterdam). The airspace is temporarily closed (in

connection with possible contamination of aircraft, etc.). Unrest occurs primarily due to the relatively long period of time which is necessary to take measurements at the rain shower locations.

Table 5.3 Impact of scenario – nuclear disaster in the Netherlands (Borssele).

Likelihood assessment						
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.	○					
Impact assessment						
Security interest / **Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial / Territory					○	An area of 100-1,000 km² becomes inaccessible for more than half a year (not functionally usable and uninhabitable), including some densely populated areas.
/ International position			◎			There is a decline in tourism and a significant decrease in exports of Dutch products and transport via routes through the Netherlands (e.g. Port of Rotterdam). There will not be any formal (political) boycott.
Physical / Fatalities			○			There will not be any direct victims as a consequence of radiation. On the basis of the estimated exposure (level and numbers of people) and an average possibility of death within 50 years in conjunction with a certain radiation dosage we have calculated that there will be approximately 500 fatalities due to cancer as a consequence of radiation in the long term. There may also be several dozen fatalities as a consequence of the evacuation or due to suicide.
/ Seriously injured and chronically ill people			○			On the basis of the calculated exposure (see 2.1) we believe that there will be several hundred chronically ill people, including a number of people with long-term psychological issues.
/ A lack of life's basic necessities	○					Depending on the accessibility of the area for the supply of emergency provisions and the degree of contamination, the expectation is that the people affected will be provided with basic needs within a couple of days.

◎ average to considerable uncertainty; ○ minor uncertainty

Table 5.3 Impact of scenario – nuclear disaster in the Netherlands (Borssele). *(continuation)*

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Economic	Costs				◉		Agriculture, exports and tourism will experience serious consequences. The Port of Rotterdam and Schiphol (in connection with the closure of Dutch airspace) will be out of operation for several days. The reputation of Dutch products will be compromised for a considerable period of time.
	Violation of vitality		◉				The Dutch economy is seriously affected, in particular the agricultural sector and to a lesser extent tourism. The expectation is that the debt ratio will increase by 1-3% (a maximum of 5% in 4 years). Unemployment will also rise, but by less than 50,000.
Ecological	Violation of nature and the environment	◉					No actual violation of the ecosystem or nature. However, some violations of environmental standards.
Socio-political	Disruption to daily life			◉			The daily lives of people (approximately 10,000) who will be evacuated from the area will be disrupted for one month or longer. The daily lives of between 10,000 and 100,000 people will be disrupted for 3-7 days.
	Violation of constitutional democratic system		◉				Confidence in politicians and administrators will be seriously impacted due to the feeling that this should not have happened and based on the political positions with regard to nuclear power.
	Societal impact			◉			There will be fear and anger, but no major systematic disagreement or conflict between population groups. From a social perspective there will be unrest and stigmatisation of / distrust of the nuclear industry (and government).

◉ average to considerable uncertainty; ◉ minor uncertainty

The impact of the 'Further away in Europe' scenario is shown in table 5.4. The likelihood of an incident (probability of occurrence) is very small for both scenarios with nuclear reactors but the estimated impact of these scenario incidents is very serious to catastrophic for several national security interests.

Table 5.4 Impact of nuclear disaster in Europe scenario.

Likelihood assessment						
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.		◉					An incident of this scope is very unlikely (10-8 per year).
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory			◉			A large portion of the Netherlands is temporarily unusable for the function of agriculture (in connection with agricultural measures). In addition, an area of between 100-1,000 km² can become contaminated by hotspots (due to rain showers). These areas are unusable for agriculture for an extended period.
	International position	◉					Because the accident occurs in a neighbouring country the negative attention will, in the first instance, be focused on the neighbouring country in question. It may also have a limited impact on our own country.
Physical	Fatalities		◉				There will not be any direct victims among the Dutch population. In the long run it is feasible that there may be some victims (10-100) as a consequence of exposure to radiation in hotspot areas or in the form of Dutch citizens who were in the source country at the time of the accident.
	Seriously injured and chronically ill people		◉				Such a large incident close to the Netherlands will produce psychological consequences. In addition, there may be many Dutch citizens on holiday in the source country (summer period).
	A lack of life's basic necessities						Not applicable.

◉ average to considerable uncertainty; ◉ minor uncertainty

Table 5.4 Impact of nuclear disaster in Europe scenario. *(continuation)*

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Economic	Costs				○		Agricultural measures will be taken for the whole of the Netherlands. The airspace is to be closed for a certain period and traffic using other transport routes will experience substantial delays (avoid the area). Even without the contamination of hotspot areas, the financial damage for the Netherlands will be very serious.
	Violation of vitality		○				The violation primarily has to do with the drop in export and unemployment at businesses (in the agricultural sector) which go bankrupt as a result of the measures. Although it has less of a direct effect on the image of Dutch products (because it is an accident occurring in a different country) an effect is feasible because a large part of the Netherlands is located in the affected area.
Ecological	Violation of nature and the environment	○					There is no actual violation of the ecosystem or nature. Although hotspots occur, the consequences for nature and the environment will be minor.
Socio-political	Disruption to daily life			○			The daily lives of people in the hotspot areas will be disrupted for one month or longer. It may be that a large number of people are located at a hotspot in a major city.
	Violation of constitutional democratic system	○					Er is sprake van enige aantasting van vertrouwen in openbaar bestuur en politiek omdat er langere tijd onzekerheid is m.b.t. de veiligheid van hotspot-gebieden. Vaststellen van het daadwerkelijke stralingsgevaar zal enige tijd duren.
	Societal impact			○			There is a certain detrimental effect on confidence in public administration and politicians because of long-term uncertainty with regard to the safety of hotspot areas. It will take some time to determine the actual radiation danger.

○ average to considerable uncertainty; ○ minor uncertainty

5.3 Chemical incidents

5.3.1 Risk

The Netherlands has a substantial chemical industry which is part of a worldwide and European network of companies and transport flows. The sector's turnover in Europe is more than 550 billion euros, of which almost 50 billion is generated in the Netherlands. In a geographical sense the chemical industry in the Netherlands is mainly spread across five regions. Important chemical clusters are located in the following regions: around the Port of Rotterdam, South Limburg (Chemelot), Southwest Brabant / Zeeland, the Northeast of the Netherlands (Delfzijl and Eemshaven), the Eastern Netherlands / Twente and the special municipalities of the BES islands in the Caribbean. The Dutch chemicals sector is ambitious and is growing. For example, the Port of Rotterdam wants to integrate its petrochemical complex in the coming decades with the industries of Antwerp, Moerdijk, Terneuzen and Vlissingen. This will, in effect, create one large petrochemical complex that will be global leader and closely linked to the complexes around the Port of Antwerp and those in Germany, from Gelsenkirchen to Ludwigshafen. Amsterdam is the world's largest cocoa and petrol port and is also the fastest growing port in Northwest Europe. Although there is a focus on security at the Chemistry complexes in the Netherlands, the range of activities that take place there mean that incidents cannot be excluded. Even if extensive precautionary measures are taken and even in the event of an optimal response, incidents that can have an effect at national level are expected to continuously occur.

Historical cases

Worldwide there have, in the past, been several large accidents with chemical companies which resulted in hundreds of fatalities and thousands of wounded. Well-known examples are the leak of methyl isocyanate in Bhopal in India and the recent explosions in the container port where hazardous substances were stored in Tianjin, China. Large accidents and disasters cost millions to tens of millions of euros, with some even costing billions of euros. Incidents involving chemical substances can have major effects locally and regionally on nature and the environment. There can be long-term consequences for the fishing industry and drinking water supply.

Accidents in the chemicals sector (including transportation of chemical substances) occur regularly in the Netherlands but rarely result in large-scale damage or large numbers of victims. Major accidents with chemical substances often involve one or more explosions, fire, and the release of hazardous substances via leakage, or in smoke. Major accidents with chemical substances therefore constitute a risk for public health and can cause substantial (regional) social unrest. In Western Europe victims are mainly staff and members of the emergency services with few fatalities among citizens outside the boundaries of the chemical complex. These types of accidents in the Netherlands generally cost tens of millions of euros (the fireworks disaster in Enschede cost 455 million euros (material damage) and the fire at Chemie-Pack in Moerdijk cost 71 million euros).

Developments

In the chemicals sector an increase is expected in chain integration and complexity. The result will be more complex systems, mutual dependency and a more diverse distribution of responsibilities, particularly at hubs. Complexity will also increase due to a gradual growth and ever-growing computerisation, in combination with increasing outsourcing of certain tasks and elements. As a result it will become more difficult to maintain an overview of processes and dependencies and this will increase the chance of, in particular, large-scale accidents occurring. In the case of larger accidents, operators themselves will have to ensure that they have the knowledge to take appropriate action. However, due to the limited insight of operators in dependencies, it will become more difficult for operators to take appropriate action in conjunction with (the run-up to) accidents. On the other hand the clustering of companies is reducing the possibility of transport-related accidents with hazardous substances because fewer transport movements are necessary.

In the Netherlands more and more mixed industrial estates are being created whereby chemical activities take place on sites where, for example, offices are located as well. This means that it has to be taken into account that more people may be present within certain impact distances when hazardous activities are being performed and that this may increase the impact of any accidents.

The chemicals sector is a truly global sector. Dutch chemical companies are increasingly controlled from locations abroad, operate on a worldwide scale and increasingly have to compete with countries with much lower energy prices and/or raw materials prices. Whenever margins and budgets are under pressure, companies and authorities are generally less inclined to invest in maintenance and in safety systems. In particular the bulk chemical producers are feeling the detrimental effects of globalisation. Fine chemical products are troubled less by an uneven playing field due to the higher added value of more distinctive products. There is a broad expectation that trends in the Netherlands will move towards sustainable and fine

chemicals whereby, incidentally, it cannot be expected that the production of bulk chemicals will disappear from the Netherlands in the coming decades.

The social pressure to make the industry more sustainable is resulting in the use of other substances. Examples are biobased chemicals, LNG, CNG, nitrogen and nanoparticles. This new substances and nanotechnology offer numerous possibilities for the future. New materials are constantly being developed for use in all kinds of products. Our knowledge of the risks of, for example, nanoparticles to public health and the environment is, however, still relatively limited.

5.3.2 Capabilities

General picture and responsibilities

The functional administrative responsibility for crisis management in relation to incidents with hazardous substances is vested in the Minister of Infrastructure and the Environment.
Despite, or perhaps thanks to, the relatively high level of safety in the chemical industry, the Netherlands have a relatively high volume of regulations, and then certainly from an international comparative perspective.
Standards also apply with regard to monitoring in the Netherlands (both government and auditors). Those high standards are partly thanks to efforts by the industry itself, for example coordination between public and company fire brigades and the chain responsibility (meaning that parties in the chain not only focus on their own processes, but also on those of the direct partners in the chain).
Regions which are home to a substantial chemical cluster have specific emergency plans in place for accidents involving chemical companies.

Pro-action, prevention and preparation

A new Environment and Planning Act [Omgevingswet] is being drawn up and will cover environmental safety. The first drafts revealed that there will be additional delegation of responsibilities and authorities to lower levels within the organisations. Within the framework of the Environment and Planning Act, the Major Accidents (Risks) Decree [Besluit Risico's Zware Ongevallen] (BRZO) is particularly relevant to the chemicals sector. The 400 most high-risk chemical companies in the Netherlands are covered by the Major Accidents (Risks) Decree [Besluit Risico's Zware Ongevallen] (BRZO 2015). This is the Dutch implementation of the international Seveso Directive. The most important obligations in the field of security at chemical companies are formalised and recorded in the BRZO. The government reports on the safety situation at these companies every year.
In addition to the formalised agreements relating to safety, the chemicals sector has itself also developed numerous initiatives such as in 2015 the Safety First [Veiligheid Voorop] programme. The programme provides instruments which companies can use to assess their safety performance.

The government is also feeling the social pressure to reduce to a minimum the risks faced by companies that work with hazardous substances. This is leading to different types of inspections, such as system supervision, risk-based supervision, and more unannounced inspections as well as increasing the visibility of inspection results. The Regional Environmental Services [Regionale UitvoeringsDiensten] (RUDs) were centralised in order to increase the quality of the government's implementation tasks in connection with companies that have to have an environmental permit. Increasing quality was also the reason for the centralisation of, in particular, the BRZO tasks for the Safety Regions, which led to the creation of six so-called BRZO-RUDs. These six BRZO-RUDs fulfil a key role for several Safety Regions as regards licensing, supervision and enforcement for the most high-risk companies.

The Ministry of Infrastructure and the Environment also has the 'Safety Deals' policy instrument. The Safety Deal programme is running from 2015-2018 and its goal is to support specific national projects which contribute to the transition to improved environmental safety. The programme relates only to safety aspects which are not regulated in the law.

Response, after-care and evaluation

With regard to dealing with chemical incidents, the focus is often on the rapid exchange of specific information on the products and the expertise relating to necessary measures and possible dangers and consequences for people and the environment. In many cases this is an extra aspect in the context of the standard way to control a fire. With a view to equipping and facilitating the regular emergency services (and in particular the fire brigade which takes the lead in this respect) a number of specific capabilities have been implemented.

- Within the safety regions a number of officials are available who have specific expertise which can be used when dealing with the consequences of a chemical incident. In the case of the fire brigade this is the Hazardous Substances Adviser. In the case of the GHOR that is the Hazardous Substances Medical Adviser. In addition to this the fire brigade has measuring teams who can perform measurements in the area around the chemical incident to determine the concentrations of the chemical substance released into the surrounding area.

- Certainly in the case of more complex chemical incidents, nationally organised public expertise can be called in, for example in the form of the RIVM's Environmental Incidence Service [Milieu Ongevallendienst] (MOD). Wide-ranging expertise is also available via the Environment and Drinking Water CET [CET Milieu en Drinkwater]. This involves cooperation between the RIVM and other knowledge institutes that have specialist knowledge and expertise about hazardous substances and their effects on public health, the environment, agriculture and the food chain. The CBRN (chemical, biological, radiological, nuclear) Defence School can, as a consequence of intensification of the civil military cooperation, contribute to the response to chemical calamities.

In addition to the capabilities from the government, high-risk companies are also obliged to organise their own response capability, often in the form of a company fire brigade. In a number of regions this has led to the creation of very specific public private partnerships.

Partly due to the 'technical' aspects of chemical incidents, communication constitutes an important element of a satisfactory response. This involves the use of regular facilities. BRZO companies are obliged to include a communication paragraph in their company emergency plans which details the communication strategy/measures which need to be implemented in the event that the company suffers an accident with consequences for the surrounding area.

Aftercare and evaluation after a chemical incident takes place within the regular frameworks of crisis management. RIVM has drawn up guidelines for adequate aftercare in the event of chemical incidents which can be used to check whether there is any point investigating, by means of bio-monitoring, whether people have been internally exposed to chemical substances as a consequence of an incident. This monitoring is necessary if, for example, there has been large-scale contamination of people, animals, crops or areas of land. An example is the monitoring of public health of (potentially) exposed people as well as bio-monitoring (blood, urine or breath measurements).

Knowledge

Chemical companies are subcontracting more and more activities. Examples include maintenance, safety and ICT. This leads to fragmentation of (safety) knowledge over several (sub)contractors. In addition, a number of studies suggest that, in the future, there will be a gradual drop in (safety) knowledge within the government (smaller government, trend to move from classical supervision to system-based supervision), the chemical companies (insufficient safeguarding of organisational memory -> brain-drain due to, for example, automation and outsourcing) and the knowledge institutions and universities (less of a research and development focus on process safety). The difference between the level of knowledge of private parties and public parties has increased in favour of the private parties. A reduction in safety knowledge leads both to an increase in the possibility of accidents and an increase in the possible consequences of accidents in the chemical industry. Having the right knowledge available during an incident for crisis decision-making is, and continues to be, a point that requires special attention. Another area that currently requires special attention is to keep up with developments in the sector as regards the use of new substances and, for example, nanoparticles in the field of knowledge relating to safety in the chemicals sector.

5.3.3 Determining factors and impact

The nature and location of a chemical modality (mobile/stationary, in or outside the chemistry cluster) determines, in combination with, among other things, the dangerous properties of the substance, the quantity and the environmental factors which influence the exposure, the type and the degree of impact. Table 5.5 provides the details of all so-called determining factors for chemical incidents. A scenario consists of a combination of the building blocks

Scenario variants and their impact

In order to describe the scope of the possible impact of a chemical accident, the in-depth theme analysis details two scenarios which together cover the space with important characteristics of plausible scenarios which (may) have a national impact (see underlying report). It concerns the scenarios of incidents:

'Chemical accident industry' (ammonia storage) scenario

The 'chemical accident industry' scenario is based on the failure of a cooled ammonia tank on a chemical company's industrial complex. The ammonia cloud spreads within a couple of minutes across the site and a nearby residential area. There are several dozen fatalities and hundreds of seriously ill people (breathing difficulties). The police and ambulances cannot access the area during the first hour due to the high concentrations of ammonia and the work of the fire brigade is hampered due to a shortage of personal protective equipment. The spread of the ammonia also causes temporary damage to nature and surface water in the area downwind. A reception point for drinking water preparation is temporarily closed. The building blocks of the scenario are included in table 5.5.

'Chemical accident shipping' scenario

The 'Chemical accident shipping' accident scenario covers a collision between a container ship and a bulk carrier in the Eurogeul close to the Port of Rotterdam. The building blocks of the scenario are included in table 5.6. While the broken container ship is being tugged it becomes clear that it is increasingly taking on water and starts to heel at a certain point in time. As a result, approximately 700 containers end up in the water. A number of containers containing hazardous substances are broken. Approximately 12 m3 of methyl mercaptan are released from one of the containers during a period of twenty minutes which are carried by the wind to a nearby beach, where tens of thousands of people are enjoying the nice weather. Due to overcrowding people are unable to leave the beach quickly and emergency services are hampered in their rescue efforts. More than a hundred fatalities and approximately one thousand people need emergency medical care and this leads to an overburdening of the care system. An unpleasant smell is detected up to dozens of kilometres downwind and because it is unknown this causes fear and unrest. The capsized ship and the floating containers lead to serious delays for shipping traffic from the sea to the port and vice versa for a number of days which, in turn, leads to substantial economic damage.

The impact of both scenarios is included in tables 5.7 and 5.8.

The occurrence of both scenarios is unlikely. The estimated impact of these scenario incidents is substantial to serious and primarily concern the aspects of 'fatalities' and 'wounded' and the costs as a consequence of the incident.

5.3.4 In perspective

Scenarios relating to chemical incidents are also detailed in the regional risk profiles.
The score patterns for the groups of 'BLEVE, explosion, jet fire' and 'toxic cloud' generally correspond with those of the national scenarios. The impact is also dominated in the regional profiles by the criteria of fatalities, seriously injured people and seriously ill people, costs and socio-psychological impact.

Table 5.5 Determining factors for the 'chemical accident industry' scenario.

Type of danger source	Modality (if mobile)	Type of location	Substance category	Source term	Type of danger	Total substance quantity	Source duration	Time of day	Warning time	Size of affected area (radius)	Nature of danger area	People present (affected area)
Mobile	Road	Chemical cluster	LT3	Instanta-neous	Fire	<10 tons	Instanta-neous	Day	None	<100 m	Inhabited area	0
Stationary	Water	No chemical cluster	GF3	Continuous	Explosion	10 - 50 tons	<5 minutes	Night	<5 minutes	100 - 500 m	Nature reserve	<10
	Railway	Important traffic interchange	GT3		Toxic	50 - 100 tons	<30 minutes		5 - 15 minutes	500 - 1.000 m	Industrial area	10 - 50
	Pipeline	....	GT4			100 - 1,000 tons	>1 hour		15 - 60 minutes	1 - 2 km	Agricultural area	50 - 100
			GT5				...		>1 hour	2 - 5 km	Specifically vulnerable object involved (e.g. stadium event area / means of transport with large numbers of passengers)	100 - 1.000
			...						...	>5 km		1.000 - 10.000
												>10.000

Table 5.6 Determining factors of the 'Chemical accident shipping' scenario.

Type of danger source	Modality (if mobile)	Type of location	Substance category	Source term	Type of danger	Total substance quantity	Source duration	Time of day	Warning time	Size of affected area (radius)	Nature of danger area	People present (affected area)
Mobile	Road	Chemical cluster	LT3	Instanta-neous	Fire	<10 tons	Instanta-neous	Day	None	<100 m	Inhabited area	0
Stationary	Water	No chemical cluster	GF3	Continuous	Explosion	10 - 50 tons	<5 minutes	Night	<5 minutes	100 - 500 m	Nature reserve	<10
	Railway	Important traffic interchange	GT3		Toxic	50 - 100 tons	<30 minutes		5 - 15 minutes	500 - 1.000 m	Industrial area	10 - 50
	Pipeline	....	GT4			100 - 1,000 tons	>1 hour		15 - 60 minutes	1 - 2 km	Agricultural area	50 - 100
			GT5				...		>1 hour	2 - 5 km	Specifically vulnerable object involved (e.g. stadium event area / means of transport with large numbers of passengers)	100 - 1.000
			...						...	>5 km		1.000 - 10.000
												>10.000

Table 5.7 Impact score for the 'chemical accident industry' scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.		○					An incident of this magnitude is very unlikely.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities		○				Several dozen fatalities on the basis of model calculations.
	Seriously injured and chronically ill people			○			On the basis of the exposure described in the scenario it is estimated that there will be more than 400 seriously wounded (serious eye and respiratory irritation).
	A lack of life's basic necessities						Not applicable.
Economic	Costs		○				
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment	○					The environment will be contaminated on a small scale but this is short-lived and maximum 30 km².
Socio-political	Disruption to daily life	○					< 10,000 people cannot function normally in the affected area for a maximum of 1 to 2 days. This means that, for a short time, they cannot go to work or attend education.
	Violation of constitutional democratic system						Not applicable.
	Societal impact		○				Indignation, unrest and negative image / stigmatisation of the chemicals sector.

○ average to considerable uncertainty; ○ minor uncertainty

Table 5.8 Impact score for the 'Chemical accident transport' scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.		O					An incident of this magnitude is very unlikely.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory	O					Due to the long-term pungent smell an area < 100 km² will be unusable for a maximum of several weeks.
	International position	O					Violation of non-political relations cannot be completely ruled out. Reliability and accessibility of the Port of Rotterdam is very important to maintain its reputation.
Physical	Fatalities			O			On the basis of the described exposure to methyl mercaptan 100-150 fatalities can be expected.
	Seriously injured and chronically ill people				O		On the basis of the described exposure to methyl mercaptan, 850-1500 wounded can be expected (including several due to traffic chaos).
	A lack of life's basic necessities						Not applicable.
Economic	Costs			O			In particular, the damage to public health and financial damage are expected to be high.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment	O					The environment will be contaminated on a small and is short-lived (< 1 year), with a maximum 30 km².
Socio-political	Disruption to daily life	O					< 10,000 people cannot function normally in the affected area for a maximum of 1 to 2 days. This means that, for a short time, they cannot go to work or attend education.
	Violation of constitutional democratic system	O					Limited violation public administration and public order and security (due to social sentiments of culpability for events in the incident).
	Societal impact		O				Outrage, indignation and unrest. Negative image / stigmatisation of the chemicals sector.

O average to considerable uncertainty; O minor uncertainty

5.4 Transport accidents

5.4.1 Risk

The transport sector can be divided across four modalities: Shipping, Railways, Road traffic, Aviation. Serious transport-related accidents have a particular impact due to the immediate number of victims and the (possible long-term) disruption of infrastructures such as roads, waterways and railways which can result in the costs of an incident being substantial. Despite the low likelihood, incidents are imaginable for all modalities whereby the impact is so large that it affects national security. This means transport(-related) activities which can cause calamities which may then result in groups of victims. This primarily means safety on the main transport axes/infrastructure. These main transport axes are 'transport flows' (aviation, water, railway, road) intended for the processing of large numbers of people and goods. In the case of road transport the total number of victims on main roads is, incidentally, smaller than on the underlying road network. However, an accident on the main roads is more likely to result in an incident with a national impact.

Historical cases

- Serious transport-related accidents on main transport axes in the Netherlands result in approximately 60 fatalities and approximately 200 seriously wounded people in traffic of passengers and goods each year, with the trend appearing to be consistent. The largest number of victims was caused by accidents involving passenger cars. Table 5.9 presents the maximum number of fatalities and wounded for recent accidents involving Dutch people. With the exception of the Sierre tunnel accident (2012) the accidents with the maximum numbers of fatalities and wounded per modality all took place more than 25 years ago and all of them also occurred abroad (with the exception of Harmelen (railway)).
- The accidents with maximum numbers of wounded per modality also date from a long time ago, but largely occurred on Dutch soil (with the exception of the aircraft accident in Faro, Portugal). Knowledge, technology and safety awareness are progressing, and this is leading to increased transport safety across the board.

Developments

The world of traffic and transport is becoming more and more international. Faster trains and bus connections are making the journeys between Northwest European capital cities increasingly shorter. The simplicity with which workers can move around means that administrators of means of transport (lorry and bus drivers, train drivers, skippers and pilots) are no longer restricted to one country but can perform their work throughout the whole of Europe.

Aviation

There has been an increase in low-cost carriers, which has led to an increase in the number of flight movements. In recent years several new types of larger aircraft have been produced, such as the Boeing 777 and the Airbus A380. The fact that they are relatively economical means these aircraft can fly longer distances with fewer stopovers being necessary, thereby reducing the possibility of incidents (during take-off and landing and activities on the ground).

Shipping

With regard to inland navigation, serious disasters are imaginable, particularly in the context of the commercial transportation of people on, for example, ferries, regular river cruisers and 'public health-related river cruises'. A serious disaster could result in large numbers of victims (dozens/hundreds). The volume and mass of ships is increasing. The result is reduced manoeuvrability and flexibility, with the amount of space to manoeuvre also decreasing. Reduced manoeuvrability and space to manoeuvre increases the possibility of accidents.

Table 5.9 Maximum number of fatalities and wounded in the past 25 years in incidents where Dutch people were involved.

Modality (number of accidents)	Maximum number of fatalities and missing people (average)	Maximum number of wounded (average)
Aviation (37)	583 (Tenerife (Sp.), 1977) (54)	106 (Faro (Portugal), 1992) (10)
Inland navigation (11)	20 (Cologne (Ger), 1975) (8)	30 (Rotterdam, 1961) (6)
Maritime navigation (15)	27 (Skikda, (Tunisia), 1989) (11)	0 (-) (0)
Road (32)	28 (Sierre tunnel (Sw.), 2012) (8)	50 (Schiphol, 1970) (10)
Railway (67)	93 (Harmelen, 1963) (4)	117 (Amsterdam, 2012) (15)

In addition, emergency services response time on water to reach vessels is also increasing (partly as a consequence of the reduction in the number of emergency vessels).
The number of incidents with fatalities in maritime navigation has decreased over the years. Up until 1970 fatal accidents occurred on a regular basis but since 1987 there have only been a couple of fatal incidents. Examples of maritime navigation disasters in 'the Western world' in the past decades are the disaster with the Herald of Free Enterprise ferry (1987), the MS Estonia ferry (1994) and the Costa Concordia cruise ship (2012) (with 193, 852 and 32 fatalities respectively).

Railway transport
Trends within the railway sector concern the introduction of a new train traffic management system, the more and more intensive/pressurised use of railway infrastructure and trains, an increase in transport in conjunction with events and changes relating to the management of parts of the railway infrastructure.
Work is being carried out on the Dutch railway network with a view to introducing the European Rail Traffic Management System (ERMTS). This is a different train safety system by which capacity on the railway can increase, with this having a positive effect on safety because the system continually monitors the train's braking curve.
Rush-hour trains are increasingly congested and disruptions are having more far reaching and lengthier effects on the railway network. The consequence of this for safety is that any accidents involving more congested trains will lead to greater numbers of victims.

Events are being organised more frequently, in which the railway is used as a key transport modality. One concern in this respect is the coordination between events. Although a separate licence is issued for each event, there is no national overview. The railway sector is not in a position to be able to respond to the local licensing policy on the basis of a national overview (autonomy of municipality versus national capacity NS/ProRail).

Road transport
If we also concentrate here on mass transport, a couple of the trends are new fuels (e.g. LNG, hydrogen, CNG and alternative (bio)fuels) and various innovations in the transport system whereby the focus is on the possibilities of ICT, big data and automation. The possibility of cyber incidents (whether deliberate or not) is increasing as a result.

5.4.2 Capabilities

General picture and responsibilities
The functional administrative responsibility for crisis management on transport incidents lies with the Minister of Infrastructure and the Environment.
The responsibilities and authorities with regards to the Dutch main infrastructure are allocated to various parties. In general the following allocation applies:
- National government (Ministry of I&E, Rijkswaterstaat) and local authorities (road management, water management) are responsible for the infrastructure, management, traffic safety measures, communication, supervision and enforcement.
- Transport organisations like ProRail, NS, other public transport companies, transport companies, airline companies, ship owners, inland navigation companies and managers of large transport hubs and mainports (Schiphol, port companies) also have a role to play in: management, traffic safety measures, RTD personnel, communication.
- Safety Regions (fire brigade, GHOR), are responsible for emergency assistance and dealing with incidents in the event of an accident.
- The police and their network are responsible for supervision and enforcement (primarily road traffic). In the case of accidents on the water, Rijkswaterstaat, the Coast Guard and port companies are also responsible.
- As far as traffic safety is concerned citizens have a responsibility as well (recreation and road traffic).

Pro-action, prevention and preparation
In addition to the fact that the Safety Regions have preparation and response capability, the transport sector is characterised by the fact that, in particular, the infrastructure managers and implementing organisations have themselves organised these capabilities. The Ministry of Infrastructure and the Environment (I&E) is responsible for the development, maintenance and management of a significant part of the traffic infrastructure in the Netherlands. Crisis management is also an essential discipline. Within that framework the ministry draws up a crisis management policy plan every four years. Rijkswaterstaat, as the ministry's implementing organisation, has a special role to play in the event of incidents as provider of knowledge with regard to crisis response and as supplier of capacity and intermediary with regard to incident response material/equipment.

ProRail has a department whose task it is to deal with railway incidents (incident control) and its own Rail Incident Management Handbook. In the spring of 2016 government departments and ProRail jointly drew up the rail incident response instructions. Rijkswaterstaat developed the Incident Management particularly for motorways. Incident management concerns a system of agreements and capabilities of Rijkswaterstaat itself, private businesses such as salvagers and insurers and the emergency services.

Our airports are equipped with response capability and the required (company) emergency plans. A few of the Dutch (sea) ports have fire boats and their own emergency plans. The safety regions also have fire boats, albeit not many, to tackle inland navigation incidents. The Incident Response on the Water Handbook was published in 2015 and details the organisation of responsibilities and (incident response) procedures in the event of accidents on the water.

Response, after-care and evaluation

Incident response to transport-related accidents is an everyday occurrence as far as smaller incidents are concerned and serves as a basis for the nature and response to large transport-related accidents. The crisis management relating to major transport accidents often takes place within the regular structures with roles mainly being fulfilled by the safety regions and sections of Rijkswaterstaat.

In special occasions the Ministry of Defence can supply equipment to help restore the original situation following major transport-related accidents such as the train accident in Barendrecht (2009) where two Leopard tanks were used for salvaging purposes in order to pull the destroyed locomotives apart.

No specific aftercare or evaluation capabilities have been arranged for transport incidents, with the regular structures being relied upon instead.

Knowledge

There are no gaps in knowledge in relation to the crisis management of transport-related accidents. However, the training and education of the crew of ships continue to be a key point that requires special attention, partly in the light of continuing internationalisation.

5.4.3 Determining factors and impact

The type of transport modality, the object that the incident relates to, the nature of the transport and the number of people in the means of transport determine, to a considerable degree, the type and the degree of impact of a transport accident. In the theme report it was decided, as regards transport scenarios, to consider a number of examples from historical cases. For each transport modality impact scores have been attributed to the incident with the greatest impact (largest number of fatalities) in Dutch history since 1945. This generates an insight into the impact of transport incidents with Dutch involvement.

For the NRP the plane crash in Tenerife has been included as an example (in the knowledge that modified procedures at airports mean that there will not be any repetition of exactly the same accident). The type of impact and the degree of impact of the chosen plane crash is comparable with that of the accidents from historical cases and therefore provides a sufficient insight into the impact of transport-related accidents.

A comparable but more worst-case incident is certainly conceivable if not just the accident itself but more drastic cascade effects apply due, for example, to the plane crashing on critical infrastructure or at a location where large numbers of people are present.

The case of the Tenerife aircraft accident

Thanks to modified procedures at airports this accident will never occur again in this form but provides a model for this type of aviation accident. The facts of the cases are the collision between a taxiing aircraft and an aircraft taking off which took place on Tenerife in 1977 on the runway at Los Rodeos airport. All 248 passengers of the KLM Boeing and 317 in the PANAM died. 55 people were injured and 9 of these died later.

This accident shows that transport incidence can cause large numbers of victims.
Because, however, the overall impact score of chemical incidents and nuclear disasters are greater than transport-related incidents (due to the other criteria that are important) it was decided not to include a transport accident in the overviews.

5.5 Conclusion and considerations

The risk diagram shows that there is only a minor probability of almost any of the scenarios relating to major accidents occurring. However, the impact extends from limited to very serious and to catastrophic as regards some aspects. In particular, the nuclear disasters stand out within the theme of major accidents. Although the possibility of occurrence is low, the effect is catastrophic in such way that these risk categories remain important for national security and the subsequent capability analysis.

The major accidents analysed fall within the 'small probability, significance effect' range.

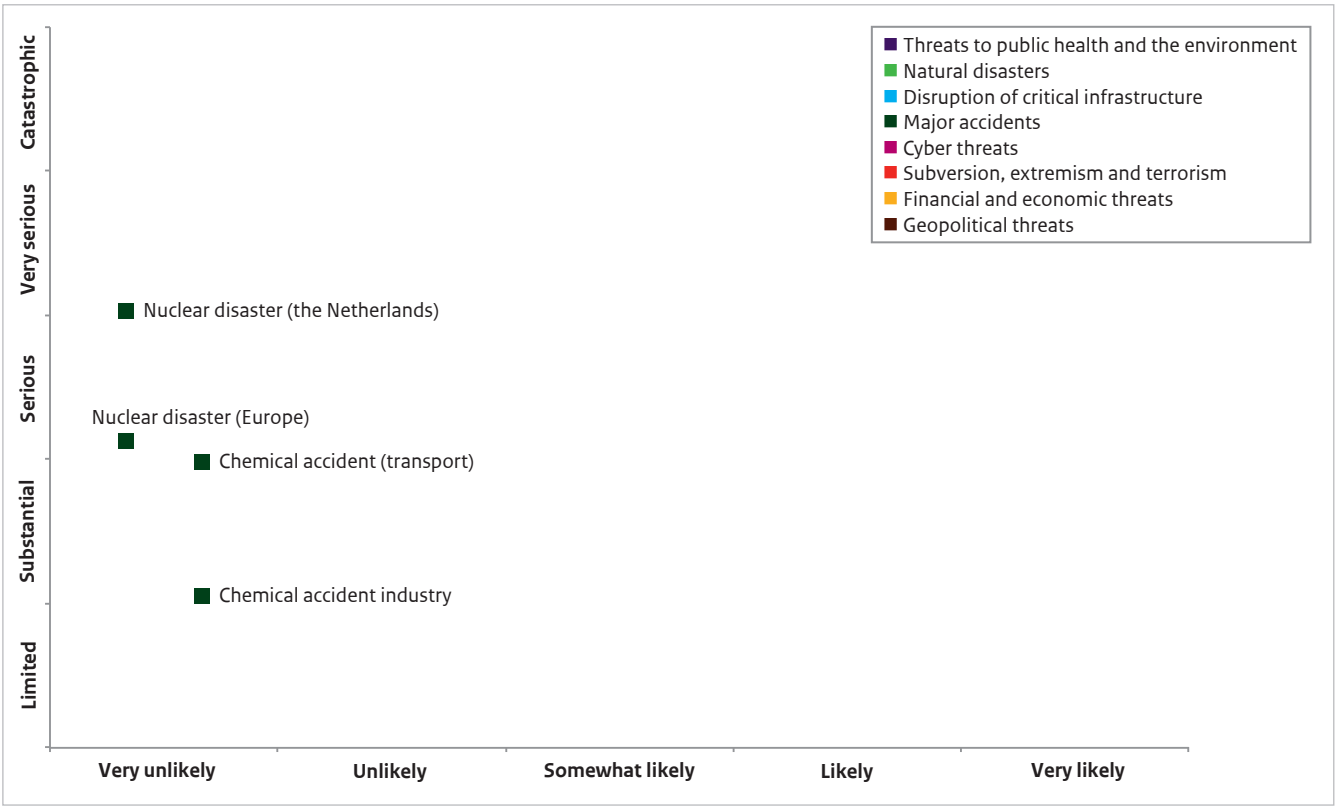
Security in relation to nuclear power is an important issue which is the subject of a lot of attention at national and international levels. There is a tradition of security thought that translates into (legally) formalised capabilities in all links of the crisis management cycle. A new element of the policy context is the creation of a single Authority for Nuclear Safety and Radiation Protection and the transfer of political responsibility for nuclear safety and radiation protection to the Minister of Infrastructure and the Environment.

In the case of the chemical incidents we see that the impact is based particularly on the number of victims and the costs. In the case of those incidents it is also clear that the expectation of society and the government is that the risks are kept to a minimum and that the government is properly prepared for any incidents.

In contrast, an increase is expected in chain integration and fine chemicals in the chemical sector in the Netherlands. This will lead to increasing complexity, mutual dependency and a more diffuse distribution of responsibilities. In addition, the social pressure is causing the industry to become more sustainable with regard to using different and new substances with regard to which there is only fairly limited knowledge about the risks. Having the right knowledge available during an incident for crisis decision-making is, and continues to be, a point that requires special attention by both companies and the government. Consequently, in relation to chemical incidents, the availability of specific knowledge during crisis decision-making is also a key aspect as regards the capability analysis following the NRP.

A relatively small number of serious transport-related accidents have occurred in the Netherlands. The number of victims is generally also limited. Despite the low likelihood, incidents are imaginable for all modalities whereby the impact is so large that it affects national security. Incident response to transport-related accidents is an everyday occurrence as far as smaller incidents are concerned and serves as a basis for the nature and response to large transport-related accidents. The crisis management relating to major transport accidents often takes place within the regular structures with roles mainly being fulfilled by the safety regions and sections of Rijkswaterstaat.

Figure 5.1 Risk diagram major accidents.



6 Disruption of critical infrastructure

6.1 Risk categories

Some processes are so critical for the functioning of our society that disruption leads to serious social destabilisation. These processes jointly constitute the critical infrastructure in the Netherlands. We interpret disruption to critical infrastructure as being the partial or complete failure of a critical process. Within the framework of the Disruption to Critical Infrastructure theme the focus is on the possible vulnerabilities of critical processes and the potential impact of failure. Another key element is the impact of the disruption of the critical processes themselves, irrespective of the circumstances in which the processes fail.

The Disruption to Critical Infrastructure theme deserves a special place within the NRP because the disruption of critical infrastructure can not only constitute a threat for national security in itself, but can also have a reinforcing effect during other threats such as floods or major accidents. Disruption to critical infrastructure is therefore both a possible source of a disruption of national security and a reinforcement of the impact (the effect) of other situations.
Scenarios relating to the disruption to critical infrastructure are also detailed in the regional risk profiles. The national scenarios are partially adapted and dimensioned at regional scale. In addition, specific scenarios are also developed and detailed. Almost all regions have included scenarios relating to the disruption of power supplies (electricity, gas), drinking water and telecommunications.

With regards to the disruption of critical infrastructure for national security we distinguish between three sorts of disruption:

- **The independent disruption of critical processes** with socially destabilising consequences
  Disruption of several critical processes with the same cause: **Common causes**
- Disruption to critical processes as a consequence of failure of other critical processes: **Cascading effects**

Some processes are so critical for the functioning of our society that disruption leads to serious social destabilisation in various areas. In addition, the disruption of one critical process can lead to problems in other critical processes because dependencies exist between systems.

6.1.1 Independent disruption of critical processes

There are only a couple of the critical processes in the Netherlands for which an independent failure or disruption within a short space of time can have destabilising consequences for society. This applies, in any event, to energy (the national and regional distribution of electricity, gas production and national transport and regional distribution of gas, oil supply), ICT and telecommunications (Internet and data services, Internet access and data traffic, speech services and SMS (mobile and landline), Satellite and Time and location positioning (satellite)), Drinking water (drinking water supply), Financial (Retail transactions, Consumer financial transactions, High-value transactions between banks, Securities trading) and Water (water defences and management). In this chapter we focus on the consequences of disruption within the first four hours.

If water defences and management are disrupted this will lead to (a threat of) a flood and this risk is dealt with within the floods risk category (see the Natural disasters theme chapter). For that reason this is not discussed separately in this chapter.

6.1.2 Common causes

A number of situations are imaginable in which several critical processes can be disrupted simultaneously by an external cause. This is, for example, the case in the event of major natural disasters such as floods and storms but can also be the result of smaller incidents. Far-reaching automation means that simultaneous failure due to an internal cause is imaginable if process automation is sabotaged within a number of different processes. Although attention is paid to the impact of a scenario on the critical infrastructure in other themes in the NRP, generally the impact which arises as a consequence of the disruption to these infrastructures is not explicitly mentioned. In this chapter we illustrate, using a scenario from the Natural disasters theme, how part of the impact in the scenario is caused by the disruption of critical infrastructure.

Table 6.1 Overview of building blocks for disruption to critical infrastructure.

Type of disruption	Directly affected critical processes	Scale – source area	Scale – affected area	Duration
Independent disruption, failure or violation	Transport and distribution of electricity	International	International	1 to 4 hours
Common causes	Transport and distribution of gas	National	National	4 to 8 hours
Cascading effects	Oil supply	Regional	Regional	8 to 24 hours
	Internet and data services	Local	Local	24 to 72 hours
	Internet access and data traffic			72 hours - 1 week
	Speech services and SMS (mobile and landline)			1 to 4 weeks
	Satellite			Longer than 1 month
	Time and location positioning (satellite)			
	Communication with and between emergency services via 112 and C2000			
	Drinking water supply			
	Water defences and management			
	Flight and aircraft processing			
	Shipping processing			
	Large-scale production/processing and/or storage of (petro)chemical substances			
	Storage, production and processing of nuclear material			
	Retail transactions			
	Consumer financial transactions			
	High-value transactions between banks			
	Securities trading			
	Deployment of police			
	Digital government			
	Deployment of the military			

6.1.3 Cascading effects

Many critical processes are dependent for their functioning on other critical processes. In many cases these dependencies are not direct and clear. The cascading effect is, for example, limited by emergency supplies for crucial elements of a critical process. A cascading effect is only complete after these emergency supplies have been exhausted. In addition, cascading effects can be influenced by circumstances such as seasonal effects, time of the day, drought or indeed heavy rainfall, etc. Cascading effects occur, in particular, due to the failure of critical processes relating to power, ICT and telecommunications. Based on a scenario related to the disruption of power supply we show how cascading effects of this disruption also influence other critical processes and the impact assessment of the scenario.

6.1.4 Determining factors and impact

In order to structure the Disruption to Critical Infrastructure theme a choice was made for a number of building blocks which can be used to create systematic assessments of scenarios relating to the disruption to critical infrastructure. The emphasis is on the type of disruption and less on the cause of these disruptions because almost all causes dealt with in other NRP themes can also lead to disruption of the critical infrastructure.

For the building blocks we initially make a distinction based on the type of disruption (independent disruption, common causes or cascading effects). The effect then consists of the disruption to one or more critical processes which are immediately affected. For the scale of disruption we make a general distinction between a source and affected area. This is relevant for critical processes because the disruption to a process itself covers a certain area and the effects of the disruption to this process can have a much larger range. The duration relates to the period of time during which the critical infrastructure is unavailable. In the analysis of a scenario attention is paid, supplementary to the building blocks, to the so-called turning points which are determined by substantial changes in the availability of a critical infrastructure, for example due to the exhaustion of emergency supplies or the creation of irreparable damage.

6.2 Independent disruption to critical infrastructure

In this paragraph we assess a number of specific critical processes with regard to which independent disruption has a destabilising impact on society. The processes in question are power supplies, ICT and telecommunications, the drinking water supply, and payment and securities transactions. In order to place the impact of this disruption in the perspective of national security we have chosen to develop two scenarios within this risk category. These are a disruption to national transport and the distribution of power supply and a disruption to satellite services. For drinking water supply and payment and securities transactions we describe, on the basis of analyses from these sectors themselves, where the largest impact of the disruption is expected. In doing so we distinguish between the effects of the disruption to the critical process itself and the consequences of the circumstances which lead to the disruption.

6.2.1 Power supplies

For power a distinction is made between electricity, gas and oil. Particularly in the event of a disruption to the **electricity supply** the societal impact can be huge, due to society's extreme dependency on electricity. Therefore, the disruption to the power supply has both a major direct impact and a major indirect impact due to cascading effects. In addition, the possibility of disruptions to the power supply is increasing due to, for example, the greater use of renewables and decentralised generation, as a result of which controlling the network is more complex. The increase in extreme weather can also lead to increasing and extensive disruptions of the power supply. Finally, experts estimate that the likelihood of the threat of cyber attacks on the sector is increasing, due to both state actors and terrorist groups.

A disruption to the **gas supply** can have a major impact, primarily because many households are dependent on gas for heat. Gas is also important for industry. The fact that, in the long run, the Netherlands are changing from an export to an import country is another important factor. Gas supplies will, eventually, become more dependent on geopolitical developments and that could lead to an increased likelihood of a disruption. The impact of disruption to the gas supply is expected to be smaller in the long term. For the time being it implies minimal changes.
The societal impact of a disruption to the **oil supply** is primarily caused by cascading effects (in particular with regard to transport). The stability of the oil supply is also linked primarily to geopolitical developments.

The impact of the independent disruption of critical processes is primarily determined by the duration of the disruption in combination with the scope and nature of the affected area. Within the framework of power supplies, a disruption of the power supply can be regarded as the worst-case scenario. For that reason we have opted for a scenario with a national disruption to the power supply as an illustration.

A disruption to the power supply can be caused by a multitude of different technical, natural or human causes (both physical and digital). Depending on the duration, a power outage leads to disruptions in other critical processes. After approximately 8 hours the consequences will increase exponentially due, for example, to the failure of (mobile) voice services, a lack of water supply, particularly in the case of high-rise buildings, the spoiling of temperature-sensitive goods, the failure of the heating supply and possible environmental damage in industrial areas due to the disruption to production processes.

Disruption to power supply scenario

In large parts of Europe (including the whole of the Netherlands) there is a power cut due to a significant drop in frequency. Due to complications it takes 24 hours before the network is restored. The consequences for companies, institutions and citizens are extensive because all kinds of processes fail either totally or partially (such as public transport (train, tram, metro), home use medical devices, payment transactions, petrol stations, communication (landline, mobile, internet), shops remain closed, etc.). The assumption is that most elements of the critical infrastructure will continue to function (using emergency power).

Table 6.2 Building blocks for the power supply disruption scenario.

Type of disruption	Directly affected critical processes	Scale – source area	Scale – affected area	Duration
Independent disruption, failure or violation	Transport and distribution of electricity	International	International	1 to 4 hours
Common causes	Transport and distribution of gas	National	National	4 to 8 hours
Cascading effects	Oil supply	Regional	Regional	8 to 24 hours
	Internet and data services	Local	Local	24 to 72 hours
	Internet access and data traffic			72 hours - 1 week
	Speech services and SMS (mobile and landline)			1 to 4 weeks
	Satellite			Longer than 1 month
	Time and location positioning (satellite)			
	Communication with and between emergency services via 112 and C2000			
	Drinking water supply			
	Water defences and management			
	Flight and aircraft processing			
	Shipping processing			
	Large-scale production/processing and/or storage of (petro)chemical substances			
	Storage, production and processing of nuclear material			
	Retail transactions			
	Consumer financial transactions			
	High-value transactions between banks			
	Securities trading			
	Deployment of police			
	Digital government			
	Deployment of the military			

Table 6.3 Assessment of the disruption of power supply scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.					●		
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities		◉				Approximately 20 fatalities as a consequence of the power outage, in particular in nursing homes or involving people who are dependent on medical equipment. There may also be a number of victims of traffic accidents due to the failure traffic management systems.
	Seriously injured and chronically ill people		◉				Between 30-300 wounded due to extra traffic accidents, industrial accidents or accidents in the home.
	A lack of life's basic necessities				◉		All residents of NL are without electricity for a period of 24 hours. Households located higher than the second floor will also have no drinking water.
Economic	Costs			◉			Approximately €2.6 billion.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life				◉		All residents of NL, for 24 hours (5 indicators work, education, social facilities, shops, public transport, virtual networks).
	Violation of constitutional democratic system						Not applicable.
	Societal impact	◉					Limited impact, although there will be some unrest and a limited group of people will (temporarily) lose confidence in government and sector.

● average to considerable uncertainty; ◉ minor uncertainty

6.2.2 ICT and telecommunications

Disruption to Internet and data services and Internet access and data traffic is included under the theme of Cyber threats. Within the Disruption to Critical Infrastructure theme an assessment is made of the disruption of voice services and SMS and satellite services.

Speech services and SMS – both mobile and landline – form a complex critical infrastructure with various mutual dependencies. The complexity consists of, among other things, the multitude of underlying systems and the large number of parties that manage these systems. However, the spread of systems and parties does ensure a certain degree of redundancy, meaning that it is difficult to disrupt voice services completely. An estimate of the impact of disruption to voice services is not provided here, partly because large-scale, complete disruption to voice services is unlikely and because it will primarily lead to nuisance, but not directly to the destabilisation of society.

The availability of **satellite systems** is very important for many critical processes. Satellite disruption primarily has

Table 6.4 Building blocks for the satellite disruption.

Type of disruption	Directly affected critical processes	Scale – source area	Scale – affected area	Duration
Independent disruption, failure or violation	Transport and distribution of electricity	International	International	1 to 4 hours
Common causes	Transport and distribution of gas	National	National	4 to 8 hours
Cascading effects	Oil supply	Regional	Regional	8 to 24 hours
	Internet and data services	Local	Local	24 to 72 hours
	Internet access and data traffic			72 hours - 1 week
	Speech services and SMS (mobile and landline)			1 to 4 weeks
	Satellite			Longer than 1 month
	Time and location positioning (satellite)			
	Communication with and between emergency services via 112 and C2000			
	Drinking water supply			
	Water defences and management			
	Flight and aircraft processing			
	Shipping processing			
	Large-scale production/processing and/or storage of (petro)chemical substances			
	Storage, production and processing of nuclear material			
	Retail transactions			
	Consumer financial transactions			
	High-value transactions between banks			
	Securities trading			
	Deployment of police			
	Digital government			
	Deployment of the military			

an effect on the GPS positioning and time signals used in many systems. Examples include GPS services for controlling traffic. However, systems used to observe the earth for weather information and telecommunications (landline and mobile), Internet and (financial) data traffic are (partially) dependent on satellite systems. Satellite disruption can seriously interfere with these processes. A broad range of natural, physical, technical and deliberate causes (including cyber attacks) can result in the disruption to satellite systems. Here we use the NRB scenario from 2011 in which the failure of satellite systems is caused by a solar storm. Although the likelihood and impact of the failure cannot be regarded separately from the specific cause in that scenario (solar storm) it does give an indication of the consequences of disruption of satellite systems. Table 6.4 shows the building blocks of the satellite systems disruption scenario.

Satellite disruption

After a long, unusual period of relative rest from the sun, a solar storm occurs. The newspapers are full of the many Northern Light displays in the Netherlands, with one being even more beautiful than the other. The disruptions to TV, mobile telephony and wireless computer connections are originally accepted without too much fuss. The consequence of the solar storm is that several satellites cease functioning or end up spinning uncontrollably in space. Only some of the lost communication satellite capacity can be transferred to other communication satellites. GPS positioning and time signals can no longer be delivered reliably above Europe. Cash transportation activities are seriously hampered because the moment-to-moment position of the cash-in-transit vehicles could not be sufficiently verified. At Schiphol airport the vehicle tracking system fails on the platform and around the various runways.

Table 6.5 Assessment of the disruption to satellite systems scenario.

Likelihood assessment						
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.			●			The likelihood assessment is largely determined by the estimate of the likelihood of a solar storm. However the sensitivity of satellite systems is also included. If all satellites fail the impact will be enormous, but the chance of this happening is not that great.

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					It is feasible for there to be limited negative consequences for the international image of NL (NL is relatively poorly prepared).

● average to considerable uncertainty; ○ minor uncertainty

Table 6.5 Assessment of the disruption to satellite systems scenario. *(continuation)*

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Physical	Fatalities		○				Due to e.g. disruption to communication systems for emergency services, failure systems in hospitals or traffic accidents.
	Seriously injured and chronically ill people		○				Due to e.g. disturbances, traffic accidents, and problems for the emergency services.
	A lack of life's basic necessities				○		> 1 million people affected for 2-6 days (in particular a lack of power, as well as supply of food). For < 100,000 people affected even for 1 month or longer.
Economic	Costs				○		< 50 billion (primarily response costs and recovery), but possibly also > 50 billion in the event of a more serious escalation
	Violation of vitality						Not applicable
Ecological	Violation of nature and the environment	○					It cannot be ruled out that, for example, a collision of oil tankers may occur because AIS is not functioning.
Socio-political	Disruption to daily life			○			Obstruction of roads and failure of public transport (people cannot get to work or school) and disruption to doing necessary shopping due to temporary shop closures). For a limited group of people the disruption lasts longer than 1 month.
	Violation of constitutional democratic system						Not applicable.
	Societal impact	○					No structural effects in society, but certainly fear and anger/indignation towards the government and business sectors that this could happen. Neither can hoarding be excluded.

○ average to considerable uncertainty; ○ minor uncertainty

6.2.3 Drinking water supplies

Disruption to the drinking water supply soon leads to social destabilisation, because both people and industrial processes are seriously dependent on drinking water. A lack of drinking water also leads to disruptions in many other (critical) processes. Because disruption of the drinking water supply has major consequences, measures have been taken to prevent disruptions as much as possible and buffers have been put in place to continue supplying in the event of any failure of sources (e.g. due to intake interruptions). Despite all this, drinking water supplies may still fail. This is, for example, the case in the event of major floods whereby sources become contaminated and the infrastructure, such as for example pipes, is (partially) destroyed (by, among other things, subsidence).

During the process of Reviewing the Critical Infrastructure in the Netherlands [Herijking Vitale Infrastructuur] experts from the drinking water sector have, based on the western coast scenario (see the Natural disasters theme), assessed the specific impact of the disruption to drinking water supplies (failure and long time required for recovery). Only certain elements of the impact of the western coast flood can be blamed for the failure of the drinking water supply and it is difficult to isolate the consequences of the drinking water supply failure from the external cause of the disruption (the flood). According to the experts the impact which can be related to the disruption to the drinking water supply particularly concerns:

- A societal impact due to a (long-term) lack of drinking water and a lack of basic sanitary facilities
- Cascade effects due to the failure of drinking water leading to the failure of other (critical) processes
- Physical consequences (disease) due to a lack of clean drinking water and basic sanitary facilities.

6.2.4 Payment and securities transactions

The financial sector identifies four processes as being critical for Dutch society:

- **Retail transactions:** this concerns all cash payments (payments with banknotes and coins) and electronic payments (e.g. debit card, credit card) at the counter. This also includes cash withdrawals (e.g. at cashpoints or in the bank itself).
- **Consumer financial transactions:** this concerns all 'distance payments'. This includes creditor payments (e.g. transfers, giro payment slips and Internet banking, including iDEAL) and periodical payments (e.g. salaries, benefits and pensions). Over-the-counter payments via cash machines, cash withdrawals from cashpoints and cash withdrawals in the bank itself are processed in the systems for mass non-cash payment transactions.
- **High-value transactions between banks:** this concerns the payments between banks and other capital and money market payments (including treasury transactions by large companies). This also includes the processing of currency transactions. In general, this concerns a relatively small number of large amounts.
- **Securities trading:** this concerns securities and derivatives transactions. This includes both the trade in securities and derivatives by private individuals as well as by parties within the wholesale segment.

These processes can be disturbed both by internal disruptions and external causes or as a cascade effect of the failure of other critical processes. During the process of the review of Critical Infrastructures in the Netherlands, the financial sector has estimated the impact of the failure of the four processes. For all processes it applies that disruption creates a drop in confidence in the financial sector leading to possible unrest and a run on the banks.
The failure of retail transactions and consumer financial payment transactions leads primarily to disruption of normal life. The likelihood of complete, long-term failure of retail transactions is low. However, disruption quickly leads to destabilisation and financial-economic damage due to transactions being impossible at, for example, shops, places of entertainment and petrol stations. As far as the disruption to consumer financial transactions is concerned, the moment at which the disruption occurs is important. Social unrest will increase on important payment days each month. Disruption to high-value payment transactions between banks and securities trading constitutes a system risk. A systemic risk means that disruption to part of the system can lead to disruption to the system as a whole. The consequences are detailed in the Financial-economic threats theme.

6.3 Common causes

Various situations are imaginable in which several critical processes fail simultaneously due to an external cause. This is, for example, the case in the event of major natural disasters such as floods and storms but can also be the result of smaller incidents or, for example, deliberate (cyber) attack. Far-reaching automation means that simultaneous failure due to an internal cause is imaginable if process automation is sabotaged within a number of different infrastructures. Incidents whereby several critical processes are affected can constitute a major challenge. For example, a lack of power, telecommunications and transport (accessibility of roads and transport of goods or people) can hamper the response, causing incidents to last longer and have a greater impact.

Although in other themes in the NRP, attention is paid to the impact of a scenario on critical infrastructure, often no explicit mention is made of the impact which arises as a consequence of the disruption to these infrastructures. In this paragraph, we use the wildfire scenario (see the Natural disasters theme) as an example

Table 6.6 Building blocks for the wildfire scenario as a common cause for the disruption to critical infrastructure.

Type of disruption	Directly affected critical processes	Scale – source area	Scale – affected area	Duration
Independent disruption, failure or violation	Transport and distribution of electricity	International	International	1 to 4 hours
Common causes	Transport and distribution of gas	National	National	4 to 8 hours
Cascading effects	Oil supply	Regional	Regional	8 to 24 hours
	Internet and data services	Local	Local	24 to 72 hours
	Internet access and data traffic			72 hours - 1 week
	Speech services and SMS (mobile and landline)			1 to 4 weeks
	Satellite			Longer than 1 month
	Time and location positioning (satellite)			
	Communication with and between emergency services via 112 and C2000			
	Drinking water supply			
	Water defences and management			
	Flight and aircraft processing			
	Shipping processing			
	Large-scale production/processing and/or storage of (petro)chemical substances			
	Storage, production and processing of nuclear material			
	Retail transactions			
	Consumer financial transactions			
	High-value transactions between banks			
	Securities trading			
	Deployment of police			
	Digital government			
	Deployment of the military			

to illustrate the impact of the simultaneous disruption of critical infrastructures. This scenario was chosen because it clearly shows how the failure of various critical processes simultaneously affects the response activities, such as evacuation and communication.
In the scenario the focus is on a large, uncontrollable fire in a nature reserve such as the Hoge Veluwe national park, necessitating the evacuation of the area with several campsites with various critical processes being disrupted. Table 3.1 shows the scenario on the basis of the building blocks for the disruption of critical infrastructure theme. The assessment of the scenario is detailed in the Natural Disasters chapter.

Failure particularly concerns electricity, voice services and SMS (mobile and landline) and drinking water supply. Disruption to power supply concerns both a direct failure (due to fire and thermal effects high-voltage lines become damaged) as a cascading effect (several thousands of households are cut off from electricity for at least 48 hours because they cannot be supplied by any other high-voltage substation). It takes several weeks to repair the entire network and high-voltage substation.

Disruption occurs as a direct effect of the wildfire and as a cascading effect in the case of voice services and SMS as well. The fire causes damage to UMTS and GSM transmitter towers, which results in direct disruption to mobile voice services. In addition, electricity outage creates additional disruption to the mobile voice services as a cascading effect. Although many towers are equipped with emergency facilities, these are generally only sufficient to keep the tower operating for two additional hours. The loss of mobile voice services has an effect on the self-reliance of the population and the capacity to organise the evacuation of the area.
A number of production stations are in the immediate fire zone and are directly affected by the fire. They have to be considered unusable for an extended period of time. In particular, the presence of diesel storage at the production stations and a liquid oxygen tank for forced ventilation leads to the loss of the production stations. Because the fire leads to damage or the closing off of a water pumping station and water pipe, a large portion of the local population has to do without drinking water for many days and have to be supplied with emergency drinking water.
The road network is not considered as critical infrastructure in the Netherlands. Nevertheless, any disruption to the road network plays a significant role in this scenario. Road congestion limits the possibilities for evacuation and hampers the emergency services and repair services for the affected critical infrastructure. The emergency supply of drinking water is also impeded by the hold-ups on the road network.

We cannot make any exact estimate of the proportion of the impact that can be attributed to the disruption of critical processes. It is, however, clear that the electricity outage creates nuisance locally, but only causes limited physical and economic damage. The failure of mobile voice services does contribute directly to the number of fatalities and wounded due to reduced self-reliance. Because the failure of mobile voice services is partially due to electricity outage, power outage does indirectly affect the number of fatalities and wounded. Disruption to drinking water facilities contributes to physical suffering. The presence of an emergency supply will, however, limit the consequences. Congestion on the road network makes it more difficult to combat fire and provide assistance and, in that way, helps to extend the incident and increase the impact.

6.4 Cascading effects

In many cases critical processes are closely interwoven. Therefore, the failure of one process can often lead to the failure of other processes. Table 6.7 provides an overview of the relationships between critical processes and the cascading effects which can cause disruption to other processes. Red areas indicate a direct dependency between processes (if the process were to fail, this would cause almost direct disruption to the other process). Orange areas indicate partial failure, or disruption of other processes. In many cases dependencies are not direct and clear. The cascading effect is, for example, limited by emergency equipment for crucial elements of a critical process. The cascading effect is only complete after these emergency supplies have been exhausted. In addition, cascading effects can be influenced by circumstances such as seasonal effects, time of the day, drought or indeed heavy rainfall, etc.

The table shows that almost all critical processes are 'dependent' on the flood defences. This is because failure of the flood defences creates a (threat of) flood, to which all processes are vulnerable to a certain degree. As already indicated, this effect is included within the Natural disasters theme.
Cascading effects also occur, in particular due to failure of energy supplies, voice services and Internet. For that reason an Electricity and Telecom Capability Recommendation [Capaciteitsadvies Elektriciteit en Telecom] (CAET) has been developed for all critical sectors. These recommendations stipulate which processes are critical within a sector, to what extent these processes are dependent on electricity and telecom, and which measures have been taken to prevent failure.

Table 6.7 Overview of dependencies as referred to by the critical sectors.

	Electricity	Gas	Oil	ICT/Tel	Drinking water	Water	Transport	Chemistry	Nuclear	Financial	Public order and security
Electricity											
Gas											
Oil											
ICT/Tel											
Drinking water											
Water											
Transport											
Chemistry											
Nuclear											
Financial											
Public order and security											

← Failure leads to disruption of...

The sector depends on... →

The above analysis of dependencies is supported by an analysis of historical incidents (from TNO's Critical Infrastructure Incident Database – CIID). The analysis presents a picture of the critical sectors from which cascading effects occur and the critical sectors which are disrupted as a consequence of cascading effects.

The cascading effects are primarily caused by the power and telecom sectors (see figure 6.1). Telecommunications, Internet and the transport sector are the most sensitive to cascading effects. This picture applies both worldwide and within the EU and the Netherlands (see figure 6.2).

As an illustration of the cascading effects of disruption to a critical infrastructure we use a scenario of long-term disruption to power supply (based on the NRB long-term disruption electricity scenario from 2008). It concerns a physical terrorist attack. As indicated earlier a disruption to a critical process and subsequent cascading effects can occur due to a broad range of causes, such as deliberate attacks (physical or cyber) and technical or human failure, or a natural disaster or major accident. The selection of the scenario has to do primarily with the lengthy duration of the disruption in this scenario. The fact that the recovery takes a long time means that emergency supplies become depleted and numerous cascading effects appear. Table 6.8 shows the scenario on the basis of the building blocks for the disruption to critical infrastructure.

Cascading effects of power supply failure scenario

As a consequence of a terrorist attack (as a response to the presence of the Netherlands and other Western countries in a conflict area) on the power network, some of the Netherlands suffers a power cut. Daily life comes abruptly to a standstill. Large numbers of people get stranded in the morning rush-hour. Computers fail, landline and mobile telephony become disrupted, cash machines no longer work, heating systems, radio and TV no longer work, production processes are interrupted, etc. In the affected area (approx. 1.5 million people) it takes several days to a couple of weeks to restore the power supply. Although emergency provisions and makeshift solutions partially help to restore the power supply, it takes several months before the network is fully functioning again. A disruption to the power supply has a major impact on the functioning of other critical processes in the affected region. Although emergency

power systems are available for many critical processes, these become exhausted quite quickly or break down due to technical failings or a shortage of fuel (experience-based figures show that approximately 10% of the emergency power systems fail to work at crucial moments). In this scenario the entire impact is due to the failure of critical processes. Table 6.9 shows an overview of the assessment of the likelihood and the impact of the scenario.

The long duration of the power outage means that almost all critical processes are eventually affected.

Other energy supplies are disrupted, telecommunications fail after several hours, the management of surface water, waste water and drinking water become disrupted, as does transport, with public administration also being seriously hampered. Drinking water companies are legally obliged to be self-sufficient for 10 days. After those ten days, they are dependent on, in any event, the supply of diesel oil for the emergency generators. These disruptions occur in phases, as it were, because the emergency supplies for more and more critical infrastructures are exhausted or indeed because makeshift measures may start functioning after a certain period of time.

Table 6.8 Building blocks for the wildfire scenario as a common cause for the disruption to critical infrastructure.

Type of disruption	Directly affected critical processes	Scale – source area	Scale – affected area	Duration
Independent disruption, failure or violation	Transport and distribution of electricity	International	International	1 to 4 hours
Common causes	Transport and distribution of gas	National	National	4 to 8 hours
Cascading effects	Oil supply	Regional	Regional	8 to 24 hours
	Internet and data services	Local	Local	24 to 72 hours
	Internet access and data traffic			72 hours - 1 week
	Speech services and SMS (mobile and landline)			1 to 4 weeks
	Satellite			Longer than 1 month
	Time and location positioning (satellite)			
	Communication with and between emergency services via 112 and C2000			
	Drinking water supply			
	Water defences and management			
	Flight and aircraft processing			
	Shipping processing			
	Large-scale production/processing and/or storage of (petro)chemical substances			
	Storage, production and processing of nuclear material			
	Retail transactions			
	Consumer financial transactions			
	High-value transactions between banks			
	Securities trading			
	Deployment of police			
	Digital government			
	Deployment of the military			

Table 6.9 Assessment of cascading effects of power supply failure scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.			○				
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position			○			E.g. activities and demonstrations against NL and Western presence in the Middle East and seriously declining tourism.
Physical	Fatalities		○				Several dozen fatalities involving people who are dependent on medical equipment, and due to a lack of heat. There may also be fatalities as a result of looting and riots or chaos during evacuation.
	Seriously injured and chronically ill people		○				Fewer than 100 wounded, both during riots and in traffic during evacuations.
	A lack of life's basic necessities					◎	Approx. 1.5 million will have no electricity for at least one month. Households located higher than the second floor will also have no drinking water and heating.
Economic	Costs				○		The financial damage is particularly high, costing approx. €12,5 billion, with material damage costing approx. €100 mln., damage to health approx. €17-€41 mln. and relief and recovery approx. €150 mln.
	Violation of vitality	○					
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life					◎	> 1 million people for at least one month (and partially longer) 5 indicators.
	Violation of constitutional democratic system		○				Violation of functioning of e.g. public order and security, and to a lesser extent also public administration and political representation.
	Societal impact			○			Fear, anger, protest, hoarding, avoidance behaviour, stigmatization Muslims, protest towards government, looting, riots.

○ average to considerable uncertainty; ◎ minor uncertainty

Direct disruptions

Road traffic is almost immediately disrupted by the failure of signalling and lighting. Rail transport comes to a standstill. The inland navigation traffic comes to a standstill almost immediately due to the failure of bridges and sluices. In many cases the landline telephone network fails because users do not have any emergency equipment. The capacity of the mobile telecommunications network declines due to the loss of towers without emergency backup equipment. Pressure pumps for drinking water in buildings of more than two storeys fail, meaning that drinking water is no longer available on higher storeys.
Having emergency measures can help resolve a number of disruptions. For example, communication with trains may be possible for an additional eight hours if emergency measures are in place. Diesel locomotives can be used to tow away stranded trains. In addition, mobile emergency generators can, for example, be used to pump water to the upper storeys of large buildings. In contrast, the road network will become congested after time due to people trying to flee the affected area. Mobility will also be restricted by the failure of petrol stations which generally do not have any emergency backup systems in place.

Exhaustion of emergency supplies

After a certain period of time a new series of disruptions will occur due to depletion of emergency measures. Air traffic will initially be able to function for some time using emergency power. After several hours airport operations will also be disrupted, not because of the lack of electricity but because of the failure of running water and the discharge of waste water. The capacity of mobile telecommunications networks will continue to decrease because transmitter tower batteries will run out of power. In addition, sluices, measuring and control systems and other provisions with emergency power systems become unusable. After a certain period of time the process industry will fail because of the increasing risks of production without electricity.

Long-term effects

In time the processes will also be disrupted which could originally rely on a buffer. For example, the waste water system will become overburdened if the sewer system cannot be pumped out. Shops will run out of stock and organisations will experience problems because of a lack of staff. In the long run the emergency supplies at critical locations such as hospitals, waste water purification plants and town halls will also run out. If almost all critical processes are affected, it is likely that a debate will start about the distribution of diesel for emergency generators.

Effecten op termijn

Op termijn worden ook de processen verstoord die aanvankelijk gebruik konden maken van een buffer. Zo raakt het afvalwatersysteem overbelast wanneer het rioolstelsel niet kan worden gepompt. Voorraden in winkels raken op. En organisaties komen in problemen doordat personeel niet kan worden afgelost. Daarnaast raken op termijn ook de noodvoorzieningen van vitale locaties zoals ziekenhuizen, afvalwaterzuiveringen en gemeentehuizen op. Wanneer bijna alle vitale processen zijn getroffen is het Likely dat de distributie van diesel voor noodaggregaten ter discussie komt te staan.

6.5 Developments

Due to an increasing focus on sustainability, more economical equipment and smarter technology will be introduced to many critical processes so that systems can become more efficient and can be controlled more effectively. However, the introduction of SMART technology also means increased dependency on, for example, electricity and data traffic systems. Dependency on the Internet is also increasing because more and more process control systems are connected to the Internet via an IP network. These developments are closely linked to the emergence of the Internet of Things (IoT) which consists of devices connected via Internet which, on the basis of data, are able to function independently. The introduction of technological innovations also means that classic (analogue) alternatives (such as landline voice services) disappear increasingly and that ICT disruptions are having an ever greater impact on various system components.

In the case of some critical processes, such as transport and distribution of gas and electricity, as well as ICT and telecommunications, (European) networks are becoming ever more interconnected, meaning that disruptions in one part of the network can also have an effect on other parts of the network. In general it applies that networks of mutually connected systems (also intersectoral) are becoming more and more complex.

Critical processes are regularly the target of (cyber) attacks perpetrated by malicious actors. This, in combination with the fact that knowledge and technology are becoming more and more accessible, means that the cyber skills of malicious actors are expected to continue increasing, as a result of which the likelihood of a cyber attack on critical processes also appears to be increasing. In this context, geopolitical developments and the emergence of hybrid warfare also play a role.

The increase in extreme weather conditions such as extreme rain showers and heat/drought can lead to problems in critical processes. The lack of cooling water in the event of drought can hamper industrial production processes. During recent hot summers, the capacity of industrial production had to be reduced on a number of occasions because the temperature of the available water turned out to be excessively high and the river discharge to low. On the other hand, heat and drought can jeopardise the continuity of the drinking water supply because the quality of the surface water is compromised as a result of the suspension of water supplies in connection with the rising water temperature and/or silting up of groundwater and surface water. Extreme gusts of wind, rainfall and snow or black ice can have a disruptive effect on telecommunications and transport networks.

6.6 Capabilities of resilient critical infrastructure

The actors involved in the continuity and resilience of the critical infrastructure together form the critical infrastructure playing field. These are the critical partners (organisation which is critical for the continuity and resilience of a critical process), the European Commission (DG HOME), the Ministry of Security and Justice, line ministries, and safety regions. The critical partners bear main responsibility for the continuity and resilience of critical processes. This includes obtaining insight into threats and vulnerabilities, risks and the development and maintenance of capabilities to safeguard the continuity and resilience of critical processes. The responsible ministry determines general frameworks for the critical processes (in policy or in legislation and regulations). The multiplicity and diversity of actors in the critical infrastructure playing field means that coordination and control are desirable. The Ministry of Security and Justice controls the resilience of critical infrastructure and provides the link and correlation with the line ministries, critical partners and the safety regions.

Pro-action and Prevention

Legislation and regulations
The various critical processes are subject to specific legislation and regulations relating to the protection and security of supply. Examples are the Electricity Act [Elektriciteitswet] 1998, the Gas Act [Gaswet], the Petroleum Products Stockpiling Act [Wet voorraad-vorming aardolieproducten], the Telecommunications Act [Telecommunicatiewet], and the Drinking Water Act [Drinkwaterwet].

Critical Infrastructure Protection and Review of Critical Infrastructres in the Netherlands
In recent years a great deal of research has been done to improve the knowledge about the sectors with a critical social function. The Critical Infrastructure Protection' project, that was completed in 2010 has created an important basis for this. A review recently took place. On the basis of a number of criteria it was stipulated, in the Review of Critical Infrastructure, which infrastructure is critical for the functioning of Dutch society. For this review the degree of criticality was assessed on the basis of uniform criteria and limiting values for social destabilisation which apply to all public and (semi) private partners.

The physical security of critical objects (essential components of a critical infrastructure) is an important issue. Following investigations, action was taken within the sectors to improve security. Examples of specific measures are the screening of personnel, intensive monitoring of the most critical locations, ICT security, etc. In practice this continues to be a point that requires special attention.

The majority of the critical sectors are connected to the Counterterrorism Alert System [Alerteringssysteem Terrorismebestrijding] (ATb) that has been operational since 2005. In the event of an increased terrorist threat for a certain sector or part of a sector, the business sectors, government bodies and operational services are kept informed via the ATb. This enables rapid action in the event of threats.

Cyber security is also a high priority of critical partners. For many critical processes an ISAC (Information Sharing & Analysis Centre) has been set up in which organisations from the sector can exchange information and cooperate in the field of cyber security policy. In addition, there is close coordination with the NCSC (National Cyber Security Centrum), the AIVD and the National Police.

For specific threats, such as climate change and floods, attention is paid, in the National Adaptation Strategy [Nationale adaptatiestrategie] (NAS) and the Delta Programme, to the vulnerability and resilience of critical sectors.

Preparation and Response

Risk communication
In large-scale publicity campaigns aimed at preparing the population for various crises, attention is also paid to the failure of critical processes such as electricity and gas. Nevertheless, the population is generally not well-prepared because people are accustomed to critical processes being extremely reliable.

Emergency supplies
Specific critical processes are subject to (legal) agreements relating to the delivery of emergency supplies. In the case of electricity, for example, the sector itself does not have to provide emergency power systems. Companies and institutions are themselves responsible for arranging emergency generators and their maintenance. Certain sectors (for example healthcare or BRZO companies) are subject to rules relating to the taking of measures on behalf of emergency power systems. The drinking water sector has, in turn, a legal obligation to deliver and, in the event of failure, it has to be possible to continue the supply of drinking water for a period of ten days. However, there are no clear agreements about the allocation of emergency supplies in the event of a large-scale disruption of critical processes.

Vulnerabilities due to dependency
An Electricity and Telecom Capability Recommendation (CAET) has been drawn up for all critical sectors. These recommendations stipulate which processes are critical within a sector, to what extent these processes are dependent on electricity and telecom, and which measures have been taken to prevent failure.

Recovery and Aftercare

Generally speaking the national and regional infrastructure managers are responsible for restoring critical processes after a disruption. Often this not only means the (technical) recovery of the systems, but also dealing with claims for damage and compensation.

Evaluation of incidents
Research and evaluation of incidents involving the failure of critical processes, such as the recent power outage in the province of North Holland, or the rupture of the water pipe at the VU University Medical Center, provide an insight into specific vulnerabilities and often lead to the taking of specific measures. Incidents are often investigated by both the sector itself and the regulator or an independent party.

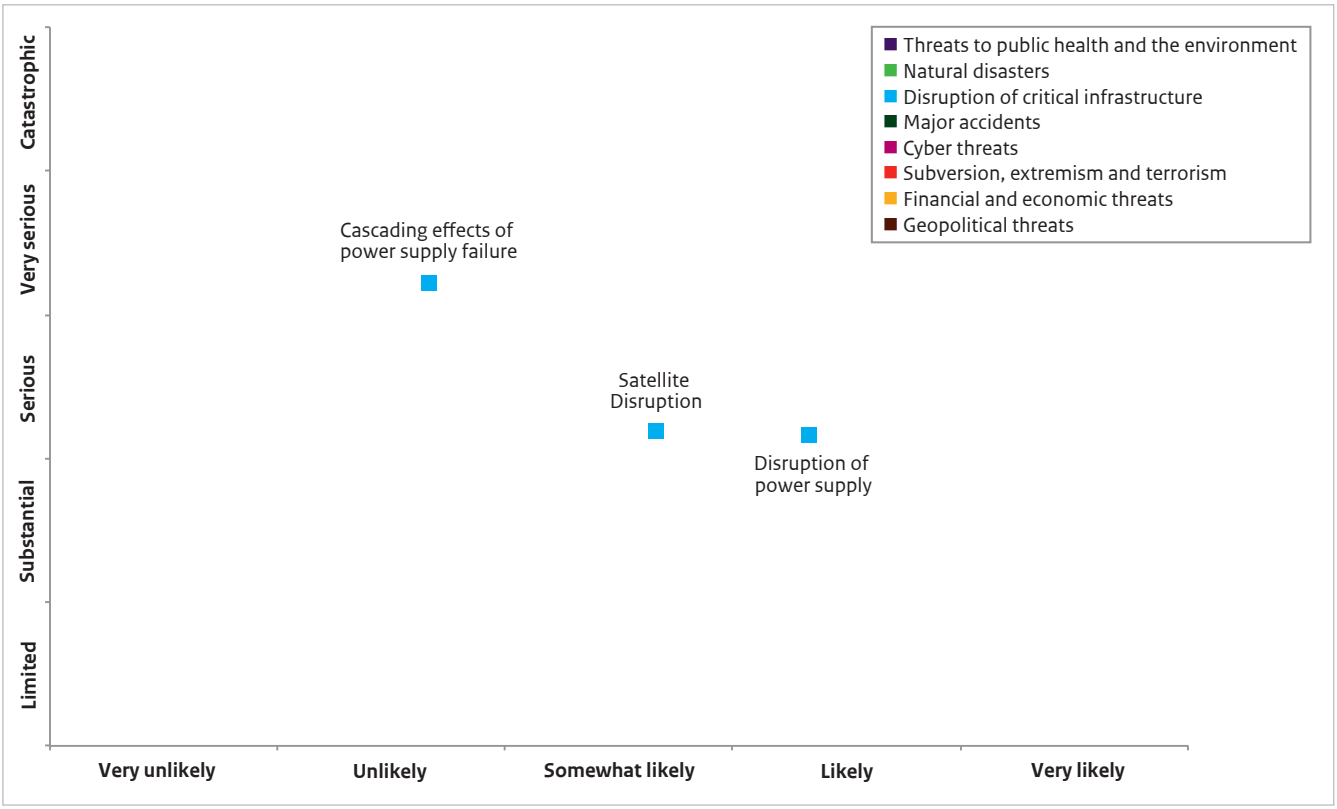
6.7 Conclusion and considerations

The risk diagram shows that disruption to critical infrastructure can cause very serious destabilisation. In the other themes within the NRP these effects are often not explicitly detailed, despite the impact of the disruptions having an escalating effect on the overall impact of a scenario.
Society is becoming increasingly dependent on critical processes and the dependency between various critical processes is also increasing, and with that the possibility of cascading effects.

The growing complexity in society and the interconnectedness of critical processes can result in an increase in the effects of disruptions in the critical infrastructure.

The analysis has revealed that the circumstances which cause disruption to critical infrastructure largely determine the degree of impact. In the case of a disaster whereby several critical processes simultaneously fail due to cascading effects, recovery is often more difficult and that may lead to the disruption lasting longer and to additional disruption of other processes.

Figure 6.1 Disruption of critical infrastructure risk diagram.



7 Cyber threats

7.1 Risk categories

The digital domain is growing both in an absolute sense and in the relative share in the Dutch economy. Due to the growth of the digital domain and the ever increasing societal dependency of digital systems, cyber threats can have major consequences. Due to the significant complexity of the digital domain, the nature, scope and likelihood of cyber scenarios with large-scale implications are uncertain. Cyber incidents can cause both direct damage and destabilisation (for example due to a substantial data leak or the corruption of important systems) and indirect damage due to the disruption of physical systems. In a number of cases the impact of cyber incidents is determined not so much by the incident itself, but by the failure of critical infrastructure. In addition, while the impact of (a series of) cyber incidents can, in itself, be limited, the undermining of confidence in digital systems eventually has a greater impact.

Due to the significant complexity of the digital domain, the nature, scope and likelihood of cyber scenarios with large-scale implications are uncertain.

7.1.1 Interconnectedness and impact

The digital domain is strongly interconnected in the society, among other things due to office IT, process automation, data storage (including cloud solutions) and network dependency. This interconnectedness ensures that cyber attacks can be carried out at many locations and that the impact of a cyber attack can quickly spread through society. With that in mind, warnings are emerging about the monoculture of digital systems, as a result of which vulnerabilities in one system can cause problems in numerous locations.
The threat of large-scale cyber attacks is concentrated partially on the possible disruption to the functioning of critical infrastructure. The interconnectedness of critical infrastructure with the digital domain is also increasing. Critical infrastructure consists in several cases of a single, central system and, in many cases, of various parallel or redundant systems. The larger the compartmentalisation of a critical infrastructure in several parallel and/or redundant systems, the more difficult it is for a cyber attack to eliminate the entire infrastructure, or damage it in some other way.
The networked nature of much critical infrastructure means that cyber attacks can cause nuisance (with sometimes unpredictable cascading effects) without reaching the level of a threat to national security. In many cases a large-scale impact is difficult to achieve and therefore only possible for actors with extensive cyber capabilities. The unique nature of such a large-scale attack can, however, increase the impact when it occurs. This is also because alternative (analogue) systems are disappearing more and more frequently.

The response to cyber incidents is generally characterised by a large number of parties being involved (both public and private). The cause of cyber incidents differs greatly and it usually takes some time to discover the exact nature of an incident. If a system is disrupted, it is often difficult for the system owner to determine why the system is malfunctioning. The impact of cyber incidents depends on the sort of effect that an incident has on a system. Cyber incidents can disrupt the availability or reliability of an information system, compromise the integrity of a system and/or the information in a system, or violate the confidentiality of information (for example due to unauthorised access to systems or data theft). In many cases cyber incidents are characterised by a combination of the above effect classifications.
Although the digital domain has been developing for some time now, there is only a short history of cyber incidents with major social consequences. Given the lack of examples there is some debate about the plausibility and possible impact of various cyber scenarios. Despite these uncertainties experts agree that digital vulnerabilities and threats need to be addressed as a matter of urgency. Within this theme we make a distinction between the following four risk categories:

- Digital sabotage
- Disruption Internet
- Cyber espionage
- Cyber crime

In addition to this, an increase in geopolitical conflicts are occurring in the digital domain. However, we do not treat cyber conflicts and digital warfare as a separate risk category here. The above-mentioned risk categories (with the exception of cyber crime) may also have a geopolitical background. The specific geopolitical developments and aspects are addressed within the theme of Geopolitical threats.

In a number of cases the impact of cyber incidents is determined not so much by the incident itself, but by the failure of critical infrastructure. In addition, while the impact of (a series of) cyber incidents can, in itself, be limited, the undermining of confidence in digital systems eventually has a greater impact.

7.1.2 Digital sabotage

The focus of this risk category is on the availability and reliability of digital systems such as for example Process Control Systems (ICS/SCADA) which are used to monitor and control physical processes. Process Control Systems (PCS) are used in many sectors to monitor and control a variety of processes such as energy systems, drinking water distribution, the operation of pumps, bridges and sluices, security systems or chemical industry processes. Disrupting these systems can cause major problems. A well-known example of deliberate manipulation of PCS is the Stuxnet virus (2010), whereby a virus in the control systems of the nuclear centrifuges in Iran rendered them unusable. Other types of (non-industrial) digital systems (as used for payment transactions or telecommunications) can be disrupted by means of digital sabotage. Although a great deal of attention is paid to the security of this type of system, the risk of deliberate disruption of critical processes, in particular, continues to be a major threat.

7.1.3 Disruption Internet

Our society is becoming increasingly dependent on the Internet and other data traffic systems. More and more devices and systems are connected via IP networks. Smart technology, often connected via the Internet, makes processes and systems more efficient and easier to control. At the same time there is an increasing dependency on reliable data traffic and a stable Internet capacity. In this risk category the focus is on vulnerabilities relating to the Internet capacity. This not only means the data traffic or the reliability of networks, but also risks which relate to the foundations of the Internet such as certificates and protocols. Any error that occurs in such a foundation can potentially have far-reaching consequences for Internet capacity.

7.1.4 Cyber espionage

Intelligence and security services are increasingly detecting incidences of digital espionage (also referred to as cyber espionage) as a supplementary tool to classical types of covert intelligence gathering. Cyber espionage can be carried out for various reasons. For example state actors use it to enhance their information position, while it can also be used for economic gain through the stealing of intellectual property and information which could have implications for the stock market. Advanced digital espionage started with targeted attacks *(spear phishing)* whereby specific e-mails are sent to people with attachments that are infected with malware or links to malware websites. Well-known examples of cyber espionage are Operation GhostNet (2009) and the Belgacom hack (2013).

7.1.5 Cyber crime

Old-fashioned crime is increasingly moving into the digital domain. An important development is the increasing presence of organised groups of professional criminals. Types of cyber crime which have recently manifested themselves include extortion using *cryptoware (ransomware)*, whereby criminals penetrate systems and encrypt information or take the systems hostage until the ransom has been paid. Just as many other types of cyber attacks, the types of attacks are gradually becoming more sophisticated, with the cyber attack often being offered as a service to generate income for the criminals. Consequently it can potentially be used by all (non-cyber) criminals. A recent example of this is Ransom32 (2016), a JavaScript based Ransomware-As-A-Service.
Targeted attacks on companies in various forms of *phishing* is still a key type of cyber crime. However, other forms of cyber crime are developing at lightning speed, and it is often impossible to take protective measures after problems have already occurred. According to experts, large-scale cyber crime is already targeting the business community, but this is often not made public because companies did not want their image to be tarnished.

Because cyber criminals have an economic motive (monetary gain), companies and private individuals are the main targets. Within the context of national security,

it is relevant to assess the risk of large-scale cyber crime in the business community. The financial sector is a potentially attractive target for cyber criminals and the impact on society can be huge if banks are on the brink of collapse if social confidence in the financial system is compromised. Together with cyber security experts from the sector, four main categories of processes within the financial (mainly banking) sector were explored to determine what a plausible scenario could be. This involved retail transactions, consumer financial transactions, high-value transactions between banks and securities trading (see also under the Disruption to Critical Infrastructure theme).

The analysis revealed that, above all, a scenario of cyber crime targeted at high-value transactions between banks can result in a serious societal impact, primarily due to the large amounts involved and the effect of a loss of societal confidence in the financial sector. This is detailed in the Financial-Economic threats theme. For that reason this issue is not discussed in any greater detail in this chapter.

7.2 Developments

The development of the Internet of Things (IoT), together with the significantly increasing quantity of networked systems, is creating an increasing connectedness between networks, physical processes (via machines) and people. This connectedness facilitates data collection and coordination between processes (devices are becoming 'smarter') but also means that disruptions and vulnerabilities are having a broader impact. At the same time, the design of IoT systems still takes too little account of the security aspects. Due to digitisation and the broad application of IoT, for example, the opportunities for sabotage and espionage are increasing, which could lead to new threat scenarios. In addition, processes are also becoming more and more dependent on reliable ICT systems because the analogue alternatives are disappearing ever faster, meaning that it is no longer possible to fall back on old systems (for example paper back-ups of dossiers – such as the electronic patients' dossier – or analogue communication methods). Disruption to ICT systems can therefore lead to ever greater problems in more and more areas of society.

In addition, the quantity of data collected and used is increasing, partly as a consequence of the development of the IoT. This is providing a broad range of possibilities to optimise processes or analyse the behaviour of companies or individuals but, at the same time, it is causing an increase in the importance of confidence between parties and the collected data itself. The integrity of managers of large quantities of data (so-called *data-herders* such as data centres, network providers, and Internet exchanges) is becoming more and more important for confidence in the cyber domain. Identity theft is seen as an important form of future cyber crime and a threat to (social) confidence in data collection. Techniques for anonymising data and encryption are important resources when it comes to protecting data and confidence in that data. Developments relating to the governance of the Internet will be important in the future. Fragmentation can occur as a consequence of differences in insight into the way in which the Internet has to be managed (for example net neutrality, the authorities for Internet regulation in the event of emergencies or shielding parts of the Internet). Political viewpoints differ greatly, particularly with regard to agreements relating to data encryption, access to systems by authorities and government influence on online services.

Another important development is that the digital domain is increasingly becoming a new setting for warfare. Digital attacks can be carried out relatively anonymously, whereby the risk of damage is lower and there may be a greater willingness to use this resource. In addition, digital attacks are a relatively cheap and accessible means of creating an impact both in terms of damage and scope. Various recent cyber incidents (for example the attack on the Ukrainian electricity network in 2015, DDoS attacks on government websites in Estonia, 2007) took place in a geopolitical context. Cyber attacks on critical infrastructure appeared to be part of larger, armed conflicts with (social) media being used to influence public opinion or reach people who potentially share the same ideology. There is a good reason why NATO recently designated cyberspace as an operational domain.

The digital domain is still characterised by a large diversity of threats. Professional criminals have found success using *Ransomware* and targeted attacks on companies by means of *Phishing*. Terrorist cyber capabilities appear to be increasing but have not yet led to effective attacks. In addition to this, state actors increasingly represent a significant threat to the international stability of and in the digital domain because more and more governments are developing offensive cyber capabilities. At the same time the fact that it is difficult to link cyber attacks to specific actors (attribution) is one of the main challenges. This makes it difficult for organisations to determine adequate measures. Attribution is also a stumbling block for investigation services and cyber defence organisations when it comes to responding quickly and assuredly to malicious actors.

With regard to vulnerabilities, most striking are those in the public core of the Internet (the deeper technological layers of the Internet, consisting of protocols and standards which ensure that data traffic can take place), meaning that investments are also necessary to ensure the security of open source systems.

The digital domain is largely in the hands of private parties, meaning that state influence is limited. The increasing use of private ICT services to supply government services (such as cloud services) is also reducing the government's control of public services. Parties may also be finding it attractive, from the point of view of cost considerations, to use systems developed abroad or systems in which privacy is exchanged for economic gain. This can reduce the influence of citizens and the influence of the Dutch government on freedom (privacy) and security.

Far-reaching digitisation implies a risk of creating a digital underclass, in other words, a social group which, due to a lack of skills or as a matter of principle, refuses to cooperate with digitisation. The emergence of such a digital underclass can lead to social exclusion. Digitisation and robotisation can also play a role in dealing with the consequences of ageing and care for socially vulnerable groups.

7.3 Capabilities

The so-called *Cyber Kill Chain* is often used to analyse cyber threats and to organise countermeasures rather than the crisis management cycle. In order to embed the capabilities for cyber in the NRP we are opting here to structure the capabilities on the basis of the crisis management cycle. Because cyber capacities are strongly oriented around *intelligence* and information exchange, we are focusing extra attention on these aspects.

Cyber capacities can be divided into organisational measures (both within public administration and in private sectors) which can be used to direct, control and monitor the digital domain and more practical (often technical) measures to counteract specific threats. The majority of the digital domain is in the hands of private parties such as Internet Service Providers, Internet exchanges and data centres. Consequently, most of the responsibility for security and continuity of digital services is borne by these private parties that protect themselves against cyber threats. Wherever the government has a partial responsibility, forms of public-private partnerships are mostly used.

The National Cyber Security Centre (NCSC) of the Ministry of Security and Justice (the coordinating ministry) is the first point of contact for the government in the event of cyber incidents. On top of this, various other ministries are important for the digital domain, in particular the Ministry of Economic Affairs as the line ministry for the ICT and telecommunications sector, the Ministry of Infrastructure and the Environment as the line ministry for various critical sectors, the Ministry of Finance as the line ministry for the financial sector and DNB as the supervising authority. Furthermore, there are the Ministry of Internal Affairs and Kingdom Relations, which is the line ministry for digital government services, and the General Intelligence and Security Service, the Ministry of Defence with, as specific cyber capability, the military Cyber Commando and the Military Intelligence and Security Service and the Ministry of Foreign Affairs for cyber threats with an international/geo-political dimension. Key supervisory bodies in the digital domain include the Netherlands Radiocommunications Agency [Agentschap Telecom], the Dutch Authority for the Financial Markets [Autoriteit Financiële Markten] and the Dutch Data Protection Authority [Autoriteit Persoonsgegevens].

Cooperation and information exchange

The digital domain is complex and dynamic and punctual signalling and identification of developments, threats and effective countermeasures is therefore crucial. Various partnerships have been developed for this signalling and identification task. These include the Cyber Security Council [Cyber Security Raad] in which the government, business community and knowledge institutions are represented and whose task is to advise the government. An I*nformation Sharing and Analysis Centre* (ISAC) was also set up to serve many critical sectors through the exchange of information about threats and measures within specific sectors.
More specific capabilities have also been developed for information exchange, such as the *Abuse Information Exchange* in which *Internet Service Providers* (ISP) exchange information and the National Detection Network (NDN) in which the government and critical sectors cooperate in order to detect digital dangers more effectively and quicker and to coordinate measures accordingly. This is done by, among other things, sharing information about cyber threats and attacks. There is also the Cyber Security Council, which has been set up at strategic level and in which the government, business community and knowledge institutions are represented and whose task is to advise the government.

Legislation and regulations

Various laws apply within the digital domain in order to guarantee the security of systems and information. The Personal Data Protection Act [Wet bescherming persoonsgegevens] is also important, just as laws which oblige companies to take adequate measures against threats from outside, such as the Drinking Water Act [Drinkwaterwet]. The Telecom Act [Telecomwet] is intended to protect the rights of users of digital communication. This act prescribes, among other things, that, in the interest of protecting personal data, the providers have to take technical and organisational measures on behalf of the security and protection of the networks and services they offer. The data breach notification obligation came into effect on 1 January 2016. This duty to report means that companies and authorities have to report major data breaches directly to the Dutch Data Protection Authority. In January 2016, the government has submitted the 'Data processing and Cyber security Notification Obligation' bill to the Dutch House of Representatives. The Computer Crime III bill (to help detect and prosecute computer crime) and the new Intelligence and Security Services Act [Wet op de Inlichtingen- en Veiligheidsdiensten] (WIV, concerning changes to the authorities of the AIVD and MIVD) are also important instruments in the fight against increasing cyber threats.
In addition to laws and regulations, more and more private parties have their own *coordinated vulnerability disclosure* policy which they can use to encourage researchers and hackers to report vulnerabilities in a responsible manner. The first European cyber security directive on Network and Information Security (the NIS directive) came into effect in August 2016. This directive is intended to create a communal level of network and information security within Europe. The cooperation between the Cyber Security Incident Response Teams in the various member states (such as the NCSC) is an important element of this.

Pro-action and Prevention

Various capabilities have been developed, on the one hand to prevent or eliminate, and on the other hand to reduce, exposure to cyber threats. In many cases preventing cyber incidents is the responsibility of (a chain of) individuals and private parties. Organisations are, in principle, themselves responsible for their information security. Specialised companies offer support for information security and advanced cyber security advice. Private parties share information among themselves and coordinate measures to prevent cyber incidents. The National Cyber Security Centrum issues security advice to support or resolve vulnerabilities. Warnings and information on threats are distributed by private security parties, the NCSC, the AIVD, the MIVD and foreign institutions. The AIVD and MIVD mainly become involved in the event of advanced cyber threats relating to national security concerns. In order to facilitate international information exchange, fifteen developed countries, including the Netherlands, are represented in the *International Watch and Warning Network* (IWWN). In addition, the NCSC is part of the European Government CERTs (EGC) group and other international networks of cyber experts (such as FIRST).
In addition to cooperation and information exchange, investments are also being made in research into, the development of and the implementation of technical protection measures such as improved authentication and cryptography. In addition, various awareness campaigns have been conducted in the digital domain (such as Alert Online and the safe banking campaign of the Dutch Payments Association [Betaalvereniging]) and various platforms have been set up to make end users more aware and to offer frameworks for action (such as the website veiliginternetten.nl and the Platform for the information society, ECP).

Preparation and Response

The government response in the case of major cyber incidents is laid down in the National ICT Incidents Crisis Plan. During cyber incidents the response is, in principle, based on the national crisis decision-making structure as described in the national crisis decision-making handbook. In addition, a number of specific forums play a role. The ICT Response Board (IRB) was set up to advise during major cyber incidents. The IRB is a public-private advisory body facilitated by the NCSC. The IRB advises existing crisis decision-making forums such as the Interdepartmental Crisis Management Committee [Interdepartementale Commissie Crisisbeheersing] (ICCb). Other important parties that play a role in the response are the NCSC, which includes the national CERT, Team High-Tech Crime of the National Police, the military Cyber Commando, the Operational Incident Response Team Consultation Group and the AIVD and MIVD. One dilemma that almost always has to be dealt with during the response to cyber incidents is the dilemma of disconnecting a system to reduce problems, knowing that it will cause damage, versus allowing a system to function so that the damage is initially limited but may increase in the long term.
Drills are regularly organised in order to prepare for major cyber incidents. Recent examples of this are ISIDOOR and CyberDawn.

Recovery and Aftercare

It can take quite a long time to recover from cyber incidents. This is because it generally takes time to determine how an incident occurred, develop an adequate solution and implement it in the apparently

vulnerable systems. The fact that attribution of cyber attacks in a borderless digital domain is problematic impedes the detection and prosecution of perpetrators. Developments in the field of digital forensic techniques may improve things in the future. The existing capabilities for research *(digital forensics)* are partially available from the government (NCSC, AIVD, MIVD, National Police, KMAR and NFI) and partially from private cyber security companies which offer digital forensic services. In addition to this the Dutch Safety Board [Onderzoeksraad voor Veiligheid] and the public prosecutor's office [Openbaar Ministerie] are developing capabilities to perform (judicial) research in the digital domain.

7.4 Determining factors and impact

The impact of cyber incidents depends on the sort of effect that an incident has on a system. Cyber incidents can disrupt the availability or reliability of an information system, compromise the integrity of a system and/or the information in a system, or violate the confidentiality of information (for example due to unauthorised access to systems or data theft). In many cases, cyber incidents are characterised by a combination of the above types of effect. The impact is not only determined by the nature of the violation, but also by the affected users. Although it perhaps appears to be more logical, from a technical perspective, to make a distinction between specific systems which are compromised, the focus when determining the impact is on the consequences of the violation for the users. With regards to deliberate attacks, the actors and their motives are also important although, in practice, this often remains unclear for a long time. Finally the impact is determined by the scope of the violation. It is also quite difficult to express this in an absolute sense. The 'scope' of the digital domain cannot be determined and, furthermore, a very small error can have an extremely large effect. This makes any statement about scope rather pointless. For that reason we have decided to translate the scope, on the one hand, into the degree of penetration of the violation (the relative part of the affected users) and, on the other hand, into the duration of the violation (time to recovery). Table 7.1 details these building blocks for the cyber threats theme.

Table 7.1 Building blocks for the scenarios in the cyber threats theme.

Cause	Actor*	Motive*	Target / people affected	Nature of the violation	Degree of penetration	Duration
Technical failure	Professional criminals	Economic gain	Public administration and politicians	Violation of availability	Small number of the institutions / critical sector(s) / companies / citizens affected (< 10%)	Up to 1 day
Human error	States	Ideological objective	Critical sector(s)	Violation of integrity	Large number of the institutions / critical sector(s) / companies / citizens affected (10-50%)	2 to 6 days
Deliberate	Terrorists	Political objective	Business community (other)	Violation of confidentiality	Majority of the institutions / critical sector(s) / companies / citizens affected (> 50%)	1 to 4 weeks
	Cyber vandals and script kiddies	Ego, profiling or revenge	Citizens			1 to 6 months
	Hacktivists					Six months or longer
	Internal actors					Irreparable
	Cyber researchers					
	Private organisations					

*The 'Actor' and 'Motive' building blocks are only relevant for events with a deliberate cause.

7.5 Complexity and uncertainty

The considerable complexity and interconnectedness of the digital domain make it problematic to determine the plausibility of cyber scenarios and this means the views of experts on this issue also differ greatly. There are a number of reasons for the uncertainty with regard to cyber scenarios, including: 1) Uncertainty about the possibilities of violating systems from within the digital domain, 2) Uncertainty about the impact of the violation, 3) Uncertainty about a clear attribution of malicious actors in the context of a cyber attack, 4) A lack of clarity about the intention of the malicious actor and 5) Uncertainty about the perception of society, which is fed by the unfamiliarity with, and inability to understand, the complexity and implications of a cyber attack.
Cyber attacks consist, in many cases, of a number of different steps, in which one or more components of a digital system are compromised and can, in some cases, lead to a disruption of physical systems. In order to determine the likelihood and impact of a large-scale cyber attack, it is necessary to find out the likelihood of the steps in the attack chain and their impact on the affected systems (taking account of measures already taken). Because many of these steps and the effectiveness of taken measures are uncertain, there is considerable uncertainty about the likelihood of large-scale attacks (therefore comprising several different steps) and their impact. In addition, people need to be aware of which actors could carry out a cyber attack (and on the basis of which motive) and which capabilities they possess to enable them to actually take the various steps required for a cyber attack.

In view of the considerable uncertainty relating to the likelihood and impact of cyber attacks it is difficult to determine a normative or worst-case situation for cyber scenarios. In the case of a disruption of critical infrastructure the consequences are more or less known and it is possible to state that, in many cases, large-scale failure is many times more difficult to achieve with a (cyber) attack than partial or regional failure. However, given a clear motive and a capable actor, a targeted cyber attack has the potential to cause just as much impact as a physical attack on a critical part of the process.

There is less clarity about the consequences of cyber attacks in which the integrity or confidentiality of systems is compromised. The possibilities of cyber attacks themselves are becoming increasingly known. What is often lacking is knowledge about the social consequences of cyber attacks.

7.6 Digital sabotage

The focus of this risk category is on the availability and reliability of digital systems such as Process Control Systems (for example ICS/SCADA) which are used to direct physical processes. Process Control Systems (PCS) are used in many sectors to control and monitor a variety of processes such as energy systems, drinking water distribution, the operation of pumps, bridges and sluices, security systems or chemical industry processes. Other types of (non-industrial) digital systems (as used for payment transactions or telecommunications can be disrupted by means of digital sabotage. Disrupting these systems can lead to major problems at many locations in society simultaneously and this may result, for example, in insufficient available capacity on the part of the emergency services. PCS are widely used to control critical infrastructures and the impact is therefore closely related to the types of disruptions which have been discussed within the Disruption of Critical Infrastructure theme. Although a lot of attention is paid to protecting PCS, it continues to be a relevant threat, particularly in critical sectors and within government or large companies. Table 7.2 shows a scenario relating to the disruption of a PCS of a critical sector (electricity).

Cyber attack - disruption critical infrastructure (PCS)

A group of activists with political motives wishes to disrupt the Dutch energy sector. One of the activists is employed by a third party that has access to the process control systems. He remotely shuts down substations operated by network managers leading to a large-scale power failure. Energy company websites are also compromised. Euronext has to shut down and almost no payment transactions can take place. People are no longer able to use the telephone and heating systems are unusable for a considerable period of time. Traffic is hindered: train and tram traffic stops, traffic management systems fail and gas stations close down because payments cannot be processed.

Because PCS are playing an ever more important role in the critical infrastructure, there is a clear link with the scenarios in the Disruption to Critical Infrastructure theme. With the increasing vulnerabilities in the digital domain, it can be asked whether these scenarios can also occur as a consequence of a 'cyber' cause. Within this framework we discussed the 'deliberate, long-term power outage' scenario from the 2009 NRB with experts in the field of electricity networks, ICS/SCADA and digital sabotage and asked to what extent it is feasible that this scenario occurs as a consequence of a 'cyber' cause. There are various possible forms of digital sabotage. In the first place digital sabotage can be caused by getting

remote access to a control centre. Experts believe it is feasible for a malicious party to gain remote access to a control centre. Due to security measures and restrictions on the possibilities of controlling processes remotely, digital sabotage is more difficult to achieve.
A second form of digital sabotage can take place after physical infiltration of a control centre. This does not so much have a 'cyber' cause, but is considered to be relevant because the disruption it causes is greater due to increasing automation and digitisation of the distribution network controls. An intruder can cause greater disruption.
In the third place digital sabotage can take place through contamination of a control centre via existing interfaces or networks. For now, the Stuxnet virus is the only example. If, for example, complex malware is used to disrupt processes, it is both more difficult to determine that a cyber attack is taking place and more difficult to detect the malware. The impact of malware that causes parts of the distribution network to shut down is, of course, greater than if only irregularities occur. Experts estimate the likelihood of digital sabotage by means of malware to be low because currently only actors with substantial resources would be able to develop such malware. Such actors generally do not intend to disrupt the distribution network.
The final form of digital sabotage is through the contamination of equipment in the transport and distribution network (possibly via a supplier). In the case of contamination experts expect that it will generally take a couple of hours to replace the equipment or to rid it of the malware. Experts estimate the probability of this form of digital sabotage to be low because the equipment's software is generally inaccessible due to the systems not being updated very often, meaning that the possibilities of installing malware via updates is limited, and also because the equipment is geographically distributed across various locations, meaning that contamination would require a considerable effort.
In the future the possibilities of causing a major impact via digital sabotage will increase due to, for example, data concentration (which will create more attractive targets for sabotage). In addition, if data is corrupted, the possible consequences would appear to be increasing. On the other hand, data concentration makes it easier to protect data.

Table 7.2 Building blocks for the Cyber attack - disruption critical infrastructure (PCS) scenario.

Cause	Actor*	Motive*	Target / people affected	Nature of the violation	Degree of penetration	Duration
Technical failure	Professional criminals	Economic gain	Public administration and politicians	Violation of availability	Small number of the institutions / critical sector(s) / companies / citizens affected (< 10%)	Up to 1 day
Human error	States	Ideological objective	Critical sector(s)	Violation of integrity	Large number of the institutions / critical sector(s) / companies / citizens affected (10-50%)	2 to 6 days
Deliberate	Terrorists	Political objective	Business community (other)	Violation of confidentiality	Majority of the institutions / critical sector(s) / companies / citizens affected (> 50%)	1 to 4 weeks
	Cyber vandals and script kiddies	Ego, profiling or revenge	Citizens			1 to 6 months
	Hacktivists					Six months or longer
	Internal actors					Irreparable
	Cyber researchers					
	Private organisations					

*The 'Actor' and 'Motive' building blocks are only relevant for events with a deliberate cause.

Table 7.3 Assessment of the Cyber attack – disruption critical infrastructure (PCS) scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				○			
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities		○				10-100 fatalities as a consequence of the power outage, particularly in care homes or involving people who are dependent on medical equipment. There may also be a number of victims of traffic accidents due to the failure traffic management systems.
	Seriously injured and chronically ill people			○			Injuries can primarily arise due to an increase in (traffic) accidents.
	A lack of life's basic necessities			●			Short failure of heating systems, drinking water (higher than two floors) for < 1 mln. people.
Economic	Costs			●			Primarily financial damage.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life				●		4-5 indicators applicable, 1-2 days, > 1 million people.
	Violation of constitutional democratic system	●					Limited violation of the functioning of public order and security.
	Societal impact	●					No structural effects in society, but certainly fear and indignation and a certain degree of blaming the sector/government.

○ average to considerable uncertainty; ● minor uncertainty

7.7 Disruption Internet

Our society is becoming increasingly dependent on the Internet and other data traffic systems. More and more devices and systems are connected via IP networks. Smart technology, often connected via the Internet, makes processes and systems more efficient and easier to control. At the same time there is an increasing dependency on reliable data traffic and a stable Internet. There are various ways in which a network can be disrupted via a cyber attack, but only a few of these appear to be able to cause a truly large-scale disruption. This not only means the data traffic or the reliability of networks, but also risks which relate to the foundations of the Internet such as certificates and protocols. Any error that occurs in such a foundation can potentially have far-reaching consequences for Internet capacity. In this risk category vulnerabilities relating to the disruption of Internet are key, With regard to the *Availability* the *Confidentiality* and the *Integrity* of the Internet.

In order to disturb the availability of the Internet, one of the possibilities is to perform large-scale DDoS attacks (similar to the incident in Estonia, 2007). However, in the Netherlands, measures have been taken, following a number of serious DDoS attacks on financial institutions (2013), to ensure that the impact of such attacks will always be limited.
Two other scenarios have already been detailed within the NRB framework, namely a scenario relating to the disruption of the IP network and a scenario involving the failure of the Amsterdam Internet Exchange. The scenario relating to the disruption of the IP network is shown in table 7.4 using the building blocks for cyber threats.

Disruption Internet scenario

The development of IP means that separate analogue and digital networks are combined to form a single digital network. Large telecom providers have, on a large scale, switched to IP networks in order to provide their services. The fact that service providers purchase the basic network services from large providers, and therefore use the same network infrastructure, means there is an increasing dependency on the IP infrastructure and the equipment and software used in that infrastructure. Although some providers still have their own network, it is still connected to, and

Table 7.4 Building blocks for the disruption of the Internet capacity of the IP network (Internet basis) scenario.

Cause	Actor*	Motive*	Target / people affected	Nature of the violation	Degree of penetration	Duration
Technical failure	Professional criminals	Economic gain	Public administration and politicians	Violation of availability	Small number of the institutions / critical sector(s) / companies / citizens affected (< 10%)	Up to 1 day
Human error	States	Ideological objective	Critical sector(s)	Violation of integrity	Large number of the institutions / critical sector(s) / companies / citizens affected (10-50%)	2 to 6 days
Deliberate	Terrorists	Political objective	Business community (other)	Violation of confidentiality	Majority of the institutions / critical sector(s) / companies / citizens affected (> 50%)	1 to 4 weeks
	Cyber vandals and script kiddies	Ego, profiling or revenge	Citizens			1 to 6 months
	Hacktivists					Six months or longer
	Internal actors					Irreparable
	Cyber researchers					
	Private organisations					

*The 'Actor' and 'Motive' building blocks are only relevant for events with a deliberate cause.

Table 7.5 Assessment of the Disruption Internet scenario.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				O			
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities		O				Fatalities cannot be ruled out due to, for example, emergency services not arriving on time.
	Seriously injured and chronically ill people		O				Injuries cannot be ruled out as a consequence of disruptions.
	A lack of life's basic necessities			O			> 100,000 people for a maximum of 1 week.
Economic	Costs				O		Depending on the duration (2 days to a week) the economic damage will be around 50 billion. In particular, there will be considerable financial damage.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life				O		>1 mln. people, for a maximum of 1 week.
	Violation of constitutional democratic system		O				3-4 indicators limited.
	Societal impact		O				Looting cannot be ruled out. In addition anger, fear and indignation and poss. increased polarisation (related to the views of the perpetrators).

O average to considerable uncertainty; O minor uncertainty

dependent on, the IP network. A group of activists decide to disrupt IP networks. The group's members have built up a great deal of knowledge about this network. The group announces that it is going to take action. They are known to have the capability of shutting down parts of the network. A few days later the Netherlands, together with the surrounding countries, are affected by a manipulation of the IP networks. Network equipment has been remotely shut down and the Dutch part of the IP network has been directly deactivated. Companies and citizens have no Internet and telephone services. This leads to considerable social unrest, partly because of the cascading effects of the Internet failure for critical processes. Payment transactions and stock exchange trading are no longer possible, resulting in substantial economic damage. Telecommunications systems which are now IP-based no longer work. Energy supplies may become partially disrupted. Especially the transport sector becomes disrupted due to disruption to rail traffic, flight connections and ports (customs and import and export come to a standstill).

We have chosen to include the above scenario in the NRP because it is a good illustration of how broad the impact of a disruption of the Internet can be. According to the experts, this scenario is, however, not the worst scenario imaginable.

Disruption of the foundations of the Internet – an assessment

Another type of scenario relates to the failure or disruption of (a part of) the Internet as a consequence of vulnerabilities in the foundations of the Internet infrastructure. This is a type of scenario which the experts indicate may have extremely substantial consequences, depending on the type of violation, the network topology and the place within the network where the violation occurs.
Violation of the Internet due to a disruption via the Internet routing protocol is a good, but less well-known, example of this. A few known examples of such incidents are the YouTube Pakistan incident (2008) in which Pakistan wrongly routed the global YouTube traffic and the AS 7007 incident (1997) in which, as a consequence of the leaking of a large portion of the routing table of a server, Internet traffic was rerouted in such a way that it resulted in a global Internet disruption. Although research is currently being carried out into the possible consequences of such an incident, it is difficult to say at the moment how great the impact of such a scenario on society may be. In order to draw extra attention to these routing protocols, which form part of the backbone of the Internet, a brief, exploratory, analysis of the use of the so-called Border Gateway Protocol (BGP) has been conducted.
BGP is regarded as the most important Internet routing protocol. It is used to route traffic between various providers via the exchange of routing information between Autonomous Systems (AS) on the Internet. An AS can be regarded as a 'network island' that is managed by an ISP.
A lot of disruptions relating to the BGP are a consequence of human error. This does not detract from the possibility of malicious actors also being able to use these options/ vulnerabilities to disturb or compromise parts of the Internet temporarily. Up to now relatively little attention has been paid to this issue, despite BGP certainly being one of the few protocols at the heart of the Internet. However, it is also a protocol that is based on mutual trust between parties, meaning that misuse certainly is possible. The number of examples of this misuse are increasing all the time. For example, malicious parties can use BGP to reroute traffic deliberately, as a result of which a Man-in-the-Middle attack may take place. If this is insufficiently monitored, such a violation of integrity can take place for quite a long time without being noticed. Another aspect that occurs in connection with BGP problems is that critical services and processes are sometimes hosted outside the Netherlands. As a result a route change can cause critical services or processes to be temporarily cut off abroad from the Dutch network, leading to a violation of availability.
This short analysis shows that there are many possible scenarios in which a violation of BGP can have consequences for the Netherlands, even if it occurs far away. It is, however, not known how significant these consequences can be. Given the large number of measures taken, in many cases the impact will not be that high. However, the situation could be completely different in the event of insidious incidents and problems with the integrity of the data traffic. It is clear, however, that this is not just a national problem and the risk applies to any country that is dependent on a broad Internet network. It is advisable to explore this issue in more detail.

7.8 Cyber espionage

Digital espionage has increased in recent years and the emphasis is currently on digital economic espionage (in particular key sectors). This is putting pressure on the international competitive position of the Netherlands. In addition, political espionage undermines Dutch politics and administration and therefore constitutes a threat to our democracy. The AIVD has also observed an increase in digital espionage attacks from state actors in a variety of countries. These attacks represent a threat to political and economic interests and the attacks are aimed at both government institutions and companies

in, for example, the key sectors. Cyber espionage is taking place on a very large scale worldwide and is therefore regarded by the security services as one of the most specific and current risks to national security. Cyber espionage can be carried out for various reasons. For example, state actors use it to enhance their information position (with the aim being to collect information which may be useful or to obtain specific information which can be used in a conflict), while it can also be used for economic gain through the stealing of intellectual property and information which could have implications for the stock market. In this context a distinction has to be made between digital industrial espionage (companies spying on each other in order to increase their competitiveness) and digital economic espionage (by state actors).
Advanced digital espionage is often carried out with targeted attacks (spear phishing) with e-mails being sent to people with attachments that are infected with malware or links to malware websites. Well-known examples of cyber espionage are Operation GhostNet (2009) and the Belgacom hack (2013).
Not only industrial espionage is increasingly taking place in digital form, investigations by the AIVD and MIVD have shown that Dutch government institutions are frequently the target of advanced cyber espionage as well. For that reason it has been decided, together with experts, to develop a scenario in which large-scale, structural cyber espionage takes place at a ministry. Espionage primarily affects the confidentiality of information (the confidentiality of leaked information is irrevocably compromised). Irrespective of whether the information is used by the perpetrators for other purposes, (reputational) damage occurs purely due to the fact that confidential or secret information has been leaked. It generally implies that espionage has to take place on a huge scale before it actually destabilises society. In addition, the effects of cyber espionage are generally difficult to determine with real precision and only become visible in the longer term. The terms 'societal destabilisation' and 'espionage' do not really belong together. Although the damage can be significant, the tangible societal impact in terms of unrest or other impact criteria is generally relatively small because it is more of a latent process and incidents of espionage are not always made public. Despite the fact that the societal impact is not always directly tangible, according to experts the consequences for the

Table 7.6 Building blocks for the Cyber espionage government scenario.

Cause	Actor*	Motive*	Target / people affected	Nature of the violation	Degree of penetration	Duration
Technical failure	Professional criminals	Economic gain	Public administration and politicians	Violation of availability	Small number of the institutions / critical sector(s) / companies / citizens affected (< 10%)	Up to 1 day
Human error	States	Ideological objective	Critical sector(s)	Violation of integrity	Large number of the institutions / critical sector(s) / companies / citizens affected (10-50%)	2 to 6 days
Deliberate	Terrorists	Political objective	Business community (other)	Violation of confidentiality	Majority of the institutions / critical sector(s) / companies / citizens affected (> 50%)	1 to 4 weeks
	Cyber vandals and script kiddies	Ego, profiling or revenge	Citizens			1 to 6 months
	Hacktivists					Six months or longer
	Internal actors					Irreparable
	Cyber researchers					
	Private organisations					

*The 'Actor' and 'Motive' building blocks are only relevant for events with a deliberate cause.

Table 7.7 Assessment of the cyber espionage government scenario.

Likelihood assessment						
	Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				⊙		Investigations by the intelligence services and known international examples reveal that this type of espionage has already occurred on several occasions. The estimate of the likelihood depends on the exact impact which can occur and that is difficult to estimate.

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable in the sense of the physical territory. However, a substantial violation did occur of the Netherlands' digital functional scope.
	International position		⊙				Although the public image of the Netherlands will suffer some damage due to the events, the actual response will depend heavily on which information has been leaked and whether it has been made public.
Physical	Fatalities	⊙					It is quite feasible that there will be a number of fatalities due to revenge attacks or suicide. For that reason the criterion is applicable.
	Seriously injured and chronically ill people	⊙					It is quite feasible that a number of people will be injured. For that reason the criterion is applicable.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			⊙			The damage depends very much on the specific information and on the consequences of the loss of confidentiality. If trade agreements are affected, the damage can be between 500 mln. and 5 billion.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.

⊙ average to considerable uncertainty; ⊙ minor uncertainty

Table 7.7 Assessment of the cyber espionage government scenario. *(continuation)*

Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Socio-political	Disruption to daily life	○					< 10,000 people may not be able to go to work for a short period of time (employees of the affected ministry) due to the digital systems having to be completely changed.
	Violation of constitutional democratic system			◉			The functioning of political representation, public administration and public order and security is compromised, but the degree also depends significantly on the type of information that has been leaked.
	Societal impact	○					Although there is some indignation and loss of confidence, this is limited because it is not an unknown or unexpected phenomenon.

◉ average to considerable uncertainty; ○ minor uncertainty

Netherlands in the longer term can be considerable. It was decided to include a degree of uncertainty in the scenario with regard to the possible goals of the perpetrators. This means that the assessment of the impact covers, on some points, a relatively large bandwidth because the effects can be greater or smaller, depending on the type of information and whether it has been made public. Table 7.6 shows the scenario shown on the basis of the building blocks for cyber threats.

Cyber espionage government scenario

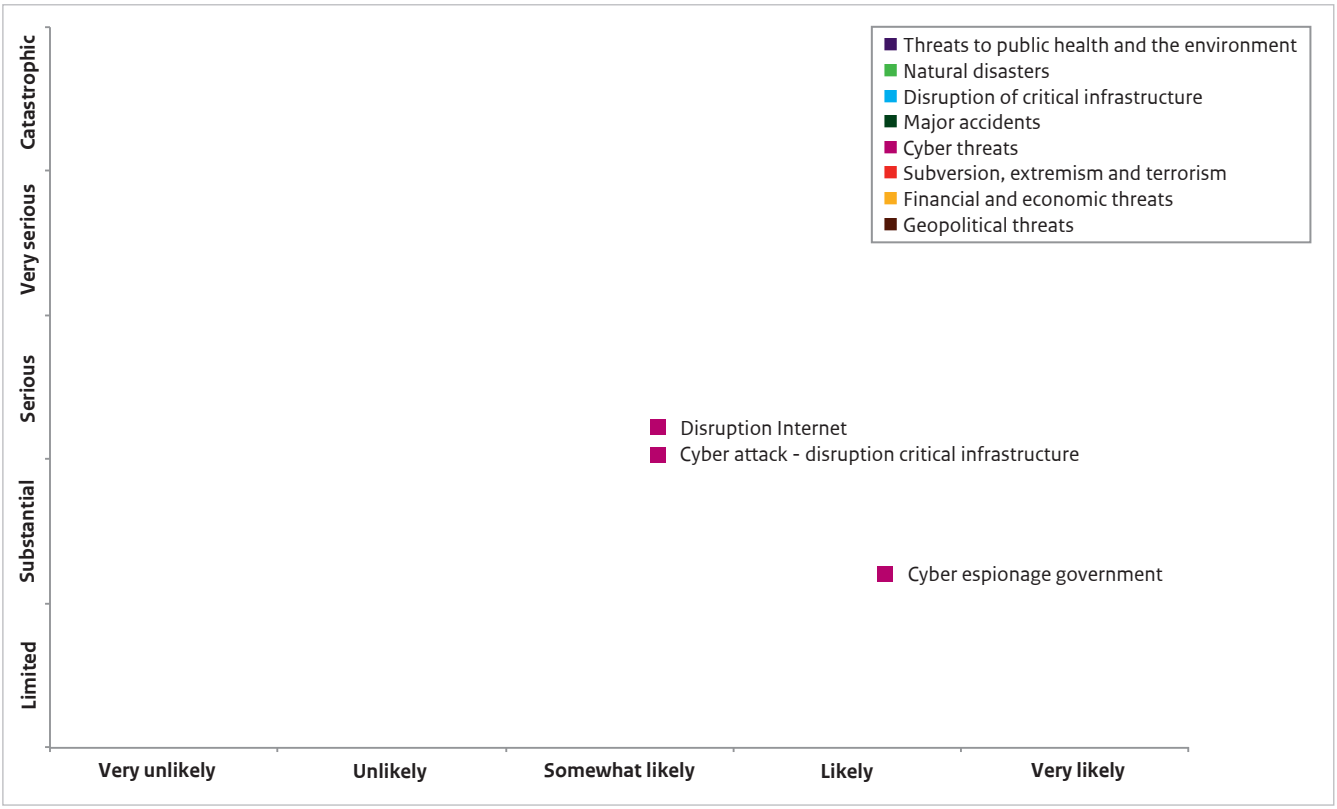
At a certain point in time it transpires that an unauthorised party has had access, during the past three years, to the content of data traffic within a Dutch Ministry. This unauthorised party was able to read all the email traffic, including classified information. Following the discovery, a major investigation is initiated and systems are shut down and replaced. It takes 1 to 6 months before the ministry's systems are purged. Soon after the discovery, the incident is also reported in the media although, to date, none of the stolen information has been shared publicly. It is unclear what the perpetrators intend to do with the information and precisely which information is involved. However, the incident has compromised the confidentiality of all information and this concerns, among other things, information about (negotiations on) trade contracts and diplomatic and security missions. This may also cause cascading effects to occur at other organisations and parties which are affected by the leak at this ministry.

7.9 Conclusion and considerations

The cyber threats theme is characterised by the rapid development of the digital domain, the interconnectedness of digital systems in all facets of society, the complexity of cyber threats, a high degree of uncertainty relating to the consequences and the fact that there is relatively little history. The past does not offer much a basis for estimating the possibility of cyber incidents and their impact on society. An exploration of various imaginable cyber incidents reveals that the possibility of physical damage is considered limited, but that social unrest and economic damage can be considerable, certainly in the long run. See the results in the following figure.

Cyber espionage can cause huge damage to the position of the Netherlands in the long run, but this is difficult to quantify in advance. Although cybercrime causes a great deal of inconvenience for citizens and companies, to date there have not been any destabilising consequences for society. Attacks on industrial control systems represent a doom scenario but occur very infrequently in practice, or their impact is limited. The same applies to the loss of Internet capacity which has occurred, but without major consequences. The last two risks could be more significant in the event of an intensification of geopolitical tensions.

Figure 7.1 Cyber threats risk diagram.



The digital domain is developing rapidly and society is reaping the benefits every day. Confidence in digital systems is essential in order to use the potential of the digital domain. Systems therefore have to be sufficiently reliable and confidential, and regarded as such by users. The impact of incidents on the confidence in digital systems and the (economic) damage which can occur as a result is potentially substantial but difficult to assess.

A great deal of work has been done on improving the resilience of the digital domain. The organisation of resilience – often in the form of public-private partnerships – has been structured at a strategic and operational level and capabilities are available to counteract, limit or resolve cyber incidents. The rapid developments in the digital domain represent a challenge for the effectiveness of the developed capabilities and continual development and the adaptation of changing circumstances would appear to be essential. One example of this is the continual scarcity of cyber security expertise and the need for cyber security professionals to maintain knowledge of existing, sometimes old systems, and stay up-to-date on the latest threats.

8 Subversion, extremism and terrorism

8.1 Risk categories

The Subversion, extremism and terrorism theme focuses on large-scale disorder with a national impact, subversion practices and (possible) consequences of extremism and terrorism. This also includes insidious processes, certainly in the context of types of subversion. When classifying the theme into various risk categories the focus was particularly on the consequences of potential threats which have to be taken into account. Categories addressed within this theme include:

- Large-scale public order disturbances
- Subversion of the democratic system and open society
- Extremism and terrorism

The potential events or developments which can constitute a risk described within this theme are partly determined by the important developments in the background, such as polarisation, increasing instability on European borders and the high levels of migration. These developments are determining context factors and are therefore not assessed as a separate risk category in this National Risk Profile.

8.1.1 Large-scale public order disturbances

The analysis of this risk category is based on large-scale public order disturbances as a consequence of social unrest and/or polarisation. In order for collective protest to occur there has to be moral turmoil, accompanied by a strong 'us against them' feeling (shared social identity) and the idea that action is possible (expected efficacy). Mass protests can escalate into collective violence. The scope of this is determined, in particular, by the degree of solidarity with and support for the protest among segments of the population, due to negative expectations beforehand, incidents which confirm these expectations and responses to mass protest situations which have an escalating effect.

Many incidents within this risk category do not directly affect national security, but have a local or regional impact. One example of national security being compromised concerns riots that last several days in a number of different cities, in which a large group of people create major public order disturbances at various locations around the country. We regard this as a 'worst-case scenario'.

In addition to a number of injured people (in the event of escalation there may even be a number of fatalities) and unrest among the population, considerable financial damage to objects will occur. Public order disturbances can also escalate, leading to greater polarisation and distrust and enmity between groups. The overall impact on national security will ultimately be limited. Therefore, this category is not developed in more detail in a separate paragraph. The theme report does contain a (more) extensive analysis. In addition, the elements from the worst-case scenario in this risk category (partially) recur in the extremism scenario that is detailed in the Extremism and terrorism risk category. Furthermore, a great deal of attention is paid in the regional risk profiles to disruption to the public order within the Social environment theme.

Developments

Despite the fact that large-scale public order disturbances are not developed in any greater detail in this document, a number of developments within this domain are worth mentioning. For example, increasing polarisation can create a breeding ground for radicalisation. The number of issues in which damaging effects of polarisation can occur has increased in recent years, such as integration of minorities, the jihadist threat and the quality of European cooperation. At the end of 2015, much of the dissatisfaction that had existed for some time on various issues, acquired a new focus due to the large influx of refugees. For many people this was evidence that politicians and European cooperation are failing and it confirmed their concerns about jihadist terrorism or

integration problems. For other people concerns about the increase in anti-Islam sentiments or actual xenophobia were confirmed.

Another worrying development is the increasing distance between social groups in the Netherlands, in particular groups in which anti-Moslim sentiments are vivid and groups of Muslims who do not feel part of Dutch society. This is not only a concern within the framework of possible public order disturbances, but can also lead to a decrease of confidence in official bodies or government. Such uncertainty and loss of confidence can, in some cases, have a detrimental effect on resilience to extremism.

8.1.2 Subversion of the democratic system and open society

The analysis of this risk category assesses the systematic, deliberate and in many cases covert activities of state or non-state actors that, due to the targets pursued, the resources used or related effects may compromise, impair, destabilise, undermine or sabotage the political and social system of the Netherlands. Serious damage caused to social cohesion is also included by taking account of the mutual confidence and solidarity between citizens.
The impact on a national scale of these scenarios is primarily determined by the national security interest of 'social and political stability', although it is also feasible for other interests to be affected, such as the integrity of the Netherlands' international position. Incidents within this risk category score particularly high on the criterion of 'violation of the democratic system', for example because the functioning of politicians or public administration is compromised. In many cases subversion does not lead to direct, acute destabilisation but the detrimental effect can lead, in the longer term, to serious disruption and dysfunctioning of the political and social system of the Netherlands (the democratic legal order and open society).

Developments

A few autonomous developments could, in the long run, influence the democratic legal order and open society, such as polarisation of social groups, the uncertainty among citizens regarding the confidence in the government and the increased migration flow. In addition to a legitimate, serious debate in relation to themes such as the refugee crisis, activities are also taking place outside the democratic frameworks. For example, some groups are choosing to disseminate hatred, spread fear and enemy images and an atmosphere of intimidation. This may hamper the functioning of administrators and politicians, democratic institutions may be disrupted and citizens' basic rights may be violated. If this were to take place structurally and on a large scale, it would affect national security.

There is also increasing concern about the emergence of parallel societies in neighbourhoods and municipalities in the Netherlands (enclaves) in which, for example, radical Muslim groups are strongly represented. In these places intolerant, antidemocratic messages can be actively broadcast and people can be urged to reject democracy and open society. In the long run this can lead to a violation of the government's authority. Parallel societies can also be imposed by actors other than extremist groups. Criminal groups may also play a role, for example by attempting to create their own 'no go area'. Administrators and politicians who try to restrict their space and influence can end up facing intimidation and threats.

In the 'Subversion of democratic legal order and open society' risk category, the discussion focuses not only on the possible consequences of the activities of non-state actors, such as extremist and criminal actors, but also on undesirable interference of foreign state actors in the Netherlands. Foreign powers with diaspora communities in the Netherlands can use covert influencing activities, intimidation and blackmail to try and take control of those communities. Such a covert 'controlling network' not only violates the sovereignty of the Netherlands, but can also have a detrimental effect on the basic rights of Dutch citizens from communities in question. In addition to foreign powers with diaspora communities in the Netherlands, powers with which the Netherlands is in conflict or with which there is a tense relationship may also engage in undesirable interference by covertly trying to gaining influence as regards students, the media, politicians and public opinion often without the parties involved being aware that this is going on. Covert financing is another tactic that is sometimes used, as are disinformation, the spreading of false rumours and conspiracy theories via shady news sites and social media. All these covert interference and influencing activities can be described using the term 'active measures'. Based on estimates by the experts involved in the development of the NRP, these constitute very real risks for the interests of national security.

8.1.3 Extremism and terrorism

Within the Extremism and terrorism risk category an analysis was made of political, ethnic or religiously motivated extremism and terrorism, with the focus being on acute and unexpected acts of violence. The threat assessment is complex with various actors in various compositions that could take actions outside the democratic frameworks and even perpetrate small-scale or large-scale attacks.

The impact on a national scale of these scenarios within the framework of Extremism and terrorism is determined by the national security interests of 'physical safety' (fatalities and injured) and 'social and political stability' (in particular disruption to daily life and socio-psychological consequences). In particular a terrorist attack can, in the short term, have a (temporary and very) destabilising effect. It can also have a lasting effect in the long term (for example if social groups become more alienated from each other and become enemies).

Developments

Just as in other risk categories, the migration flow is a development which influences the threat posed by extremists and terrorists. The increase in threats, intimidating activities and incidents of violence in relation to refugee centres is a cause for concern. Such acts of violence and threats increase feelings of insecurity among various social groups. There is a lack of clarity with regard to developments relating to the number of asylum applications. This is partly due to measures which are being taken to limit the high influx of refugees, such as the agreements between the EU and Turkey.

In regard to the jihadist threat, which is the largest terrorist threat at the moment, the decision by the Netherlands to join the coalition which is carrying out bombings of ISIS in Syria plays a role. This is also pointed out in the terrorism threat assessment[12]: all countries that participate in the anti-ISIS coalition are regarded as targets by jihadists. Countries such as France, Germany, the United Kingdom and the United States are receiving more attention in jihadist propaganda, but the military actions of the Netherlands in Syria/Iraq, that are intended to eliminate the ISIS threat in the long term, may increase the profile of the Netherlands.

The possibility of an attack on Dutch territory other than jihadist is currently small but cannot be ruled out. This means that people have to stay alert. The increasing tensions between Kurds and Turks, for example, is also evident in European countries, including the Netherlands.

This risk category, as well as the 'Subversion democratic system and society' risk category are analysed in more detail below.

8.2 Subversion of the democratic system and open society

8.2.1 Risk

The Netherlands have an open society based on democratic principles in which certain values are promoted but are not, by definition, shared by everyone. Consequently, there are both state and non-state actors that have an interest to subvert. In addition, they can engage in activities to disrupt the relationship between citizens and the government (vertical dimension of the democratic legal order) and relationships between citizens themselves (open society). The Netherlands are actively involved in international politics, for example within the EU, in NATO and globally. There may also be parties within this framework that wish to destabilise our country.

Undermining practices have been used since time immemorial. There are still indications that actors are trying to influence the functioning of the Dutch system. Extremist and criminal groups, for example, are using resources to seriously disrupt, destabilise and damage the Dutch system. For example, by influencing administrators through the use of undemocratic resources (threats, intimidation). Another phenomenon is 'withdrawal' from society. Over time 'parallel' societies may arise in which democracy and open society are (actively) rejected and thereby defy the government's authority.

State actors also engage in subversive activities. Foreign governments try to exert their power via their diaspora community in the Netherlands. They try to 'win over' influential people or use international social problems to achieve political or economic goals. Covert financing is another tactic that is sometimes used, as are disinformation, the spreading of false rumours and conspiracy theories via shady news sites and social media. All these activities are referred to as 'active measures'. Such practices could (in the longer term) lead to serious destabilisation of the democratic system and open society.

Hate campaigns, large-scale intimidation, the creation of enclaves, interference and influencing activities by both state and non-state actors can have a seriously subversive effect.

[12] NCTV, National Terrorism Threat Assessment 42,July 2016

8.2.2 Capabilities

This paragraph describes capabilities in general. A more detailed assessment can be found in the theme report.

Spread of responsibilities

Various ministries and institutes are responsible for (elements) of the capabilities which can increase the resilience to subversion. For examples, knowledge of, and contact with, diaspora communities, ethnic and religious minorities, research into interference and influencing activities by non-state and state actors and policy which is aimed at combating this.

Pro-action, prevention, preparation

- (Policy) measures to combat extremism and prevent social destabilisation
- The monitoring of, and research into, extremist groups and movements which are involved in activities that intend to disrupt democracy (and which directly use violent means such as dissemination of hatred, intimidation, etc.).
- The monitoring of and research into the creation of parallel social structures by extremist groups or criminals.
- The monitoring of and research into interference and influencing activities by foreign authorities in the Netherlands.
- Increasing the resilience of minorities (diaspora communities) and other vulnerable groups in the face of interference by foreign authorities.

Repression and aftercare

- Limit the consequences of the destabilising effect of subversion.
- Keep control of subversion activities.
- Prosecute people who have broken the law.
- Possible measures against diplomats and representatives of foreign authorities or organisations that are involved in interference and influencing activities.

8.2.3 Determining factors and impact

The variables and factors shown in table 8.1 influence the impact of subversion practices on the Dutch democratic system and society.

Scenario variants and their impact

An actual subversion incident consists of a combination of the building blocks as described above. To describe the scope of the possible impact of potential threats relating to subversion of the democratic legal order and open society, two scenarios for both state and non-state actors are developed and assessed in the theme report (giving a total of four). The summaries of two of the scenarios are included in this document, namely the 'Subversive enclaves' scenario, as the worst-case scenario for subversion by non-state actors, and the 'Subversion foreign actors' scenario, as the worst-case scenario for subversion by state actors.

Worst-case non-state actors scenario – 'Subversive enclaves'

The 'Subversive enclaves' scenario describes how, in various cities in the Netherlands as well as in the rest of Europe, parallel societies have originated in which a large proportion of the population who live there have little respect for local and national government. Indeed, these are even rejected, circumvented wherever possible and opposed in all kinds of ways. In practice, people want to exercise and enforce their own authority, their own legislation and regulations on the basis of the individual values and standards of the group to which they belong.

The scenario specifically describes the situation in a large city in the Netherlands. In the past ten years two deprived neighbourhoods have developed into parallel societies. Both neighbourhoods have a mixed ethnic population. However, in one of the neighbourhoods there is a majority of low-skilled, white families while in the other neighbourhood, (in a different part of the city) the majority are migrant families with a Muslim background. In both cases, the local government has major problems exercising and enforcing its authority (in some cases because it has been taken out of their hands). The residents of the neighbourhoods are encouraged by their leaders to resist and oppose the government. In one of the neighbourhoods, the population has been urged to have as little contact as possible with the authorities. Also, they are told not to cooperate on initiatives aimed at integration and creating a good relationship between ethnic and religious groups. Democracy as a political system is incompatible with the political and religious views that people hold. People are being urged to comply with their own (religious) legislation and regulations and not those of the Dutch government. For instance, to set up their own courts on the basis of the (religious) legal system. Among the minorities in these neighbourhoods there is a feeling of insecurity and fear that they might become victims of bullying, intimidation and threats from the dominant groups.

An overview of the combination of building blocks for this normative scenario are shaded in grey in table 8.2.

Table 8.1 Building blocks for the normative scenario.

Category	Subcategories	Aims	Resources	Targets
State	Politically inspired extremist groups	Gain and exercise control over own ethnic or religious community	Disseminate hatred; spread fear and create enemies	Own ethnic or religious community
Non-state	Religiously inspired extremist groups	Create parallel society/ enclave of their own with as little government control as possible	Create antagonism between social groups / deliberately cause polarisation	Diaspora communities
	Ethnically inspired extremist groups	Gain and exercise control over diaspora community abroad (control network by foreign government)	Question and undermine the government's legitimaticy	Authorities (national or local)
	Criminal groups	Damage confidence in the government and undermine the legitimacy of the government	Blackmail	Minorities
	Foreign authorities with a substantial diaspora community in the Netherlands	Create a political system which is different to the democratic system	Intimidation	Media
	Authorities from countries with which Europe / the Netherlands has a tense relationship or a conflict	Restrict (basic) rights of other political, religious or ethnic groups/minorities	(Covert) influencing	Science
	Authorities from countries of origin or transit countries of the migration flow	Create a form of society which is different to the open society	Propaganda via classical and social media	Western world/EU
		Win over public opinion	Disinformation via classical and social media	Dutch citizens / public opinion
		Acquire political influence	Recruit people	
		Obtain political or social favours/benefits	Become involved in politics / acquire membership, with a hidden agenda, of political parties, municipal councils, government consultation bodies, etc.	
		Financial gain	Cultivate/task people with influence in the business community	
		Damage the image of the Netherlands and the West	Acquire influence in the media in order to disseminate a certain view	
		Create divisions within the EU	Acquire influence in the world of science	

Table 8.2 Building blocks for the worst-case non-state actors scenario – 'Subversive enclaves'.

Category	Subcategories	Aims	Resources	Targets
State	Politically inspired extremist groups	Gain and exercise control over own ethnic or religious community	Disseminate hatred; spread fear and create enemies	Own ethnic or religious community
Non-state	Religiously inspired extremist groups	Create parallel society/ enclave of their own with as little government control as possible	Create antagonism between social groups / deliberately cause polarisation	Diaspora communities
	Ethnically inspired extremist groups	Gain and exercise control over diaspora community abroad (control network by foreign government)	Question and undermine the government's legitimaticy	Authorities (national or local)
	Criminal groups	Damage confidence in the government and undermine the legitimacy of the government	Blackmail	Minorities
	Foreign authorities with a substantial diaspora community in the Netherlands	Create a political system which is different to the democratic system	Intimidation	Media
	Authorities from countries with which Europe / the Netherlands has a tense relationship or a conflict	Restrict (basic) rights of other political, religious or ethnic groups/minorities	(Covert) influencing	Science
	Authorities from countries of origin or transit countries of the migration flow	Create a form of society which is different to the open society	Propaganda via classical and social media	Western world/EU
		Win over public opinion	Disinformation via classical and social media	Dutch citizens / public opinion
		Acquire political influence	Recruit people	
		Obtain political or social favours/benefits	Become involved in politics / acquire membership, with a hidden agenda, of political parties, municipal councils, government consultation bodies, etc.	
		Financial gain	Cultivate/task people with influence in the business community	
		Damage the image of the Netherlands and the West	Acquire influence in the media in order to disseminate a certain view	
		Create divisions within the EU	Acquire influence in the world of science	

Table 8.3 Worst-case non-state actors scenario – 'Subversive enclaves'.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					○		This corresponds with the description from the guidelines: 'The scenario is very conceivable and there are indications that the scenario can occur'.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position						Not applicable.
Physical	Fatalities						Not applicable.
	Seriously injured and chronically ill people						Not applicable.
	A lack of life's basic necessities						Not applicable.
Economic	Costs	○					Limited.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life		○				Some people in enclaves are (on average) no longer able to use social facilities (community work, youth care etc. scarcely exists).
	Violation of constitutional democratic system				○		National and local government are seriously losing grip on minorities; basic rights are extremely restricted in the 'enclaves'.
	Societal impact			○			Segregation, polarisation.

○ average to considerable uncertainty; ○ minor uncertainty

Physical safety interest can also play a role if any disorder turns violent, for example, in the form of riots between groups. Details on the impact can be found in the theme report and, in particular, the Large-scale public order disturbances risk category.

Worst-case state actors scenario – 'Subversion foreign actors'
Dutch young people, the media and the elite (business, political, academic) are influenced by a range of (covert) activities by a non-Western country that wants to subvert the EU and wants sanctions imposed on them to be lifted. For example, rumours are spread about large-scale fraud and corruption scandals within the EU (see e.g. 'resources' in the building blocks diagram for other activities carried out). A number of Dutch administrators and politicians feel obligated to resign (despite a lack of any clear evidence). Conspiracy theories about Dutch and European migration policy are disseminated. The suggestion is also made that migrants have been harassing women and that the government has not taken any action. After a certain period of time, the Dutch population starts to lose confidence in the government and doubts emerge about the EU and other forms of cooperation. A far right party with an anti-EU and anti-migration agenda, of which the activities are covertly sponsored by the country in question (something that is also happening in other EU countries), quickly starts acquiring more and more members. The gap between advocates and opponents of the EU and the refugee policy is increasing all the time. The Dutch anti-EU and anti-migration parties regularly organise demonstrations which end in serious public disorder. Via social media Dutch politicians and administrators are continuously confronted with a torrent of manifestations of hate, intimidation and threats related to EU and migration themes, which seriously hampers their ability to work.

An overview of the combination of building blocks for this worst-case scenario are shaded in grey in table 8.4.

Likelihood of occurrence of scenarios
For all four scenarios developed in the thematic report under the theme of Subversion of the democratic system and open society, it is highly conceivable that they may occur, as are some specific indications. In some cases, certain aspects have even started (or have occurred). There is a tendency, for example, for enclaves to be created in a number of cities and municipalities along with rejection, opposition, disruption and subversion of local government. In the Netherlands, however, this is not occurring to the same degree as in other European countries. In addition, there are also specific examples of (covert) interference and influencing activities by foreign authorities, as detailed in the worst-case scenario.

8.2.4 In perspective
At the moment, there are no non-state actors which are able to overthrow democracy and frustrate open society. However, non-state actors may, in the short and long term, subvert processes, for example by hampering the functioning of government and public administration. Extremist or criminal groups have the capability to disrupt or influence democratic institutions and processes. State actors can constitute a threat to Dutch national security due to covert information or influencing activities. They can have a detrimental effect on the rights and freedoms of Dutch citizens within minorities or can use covalent resources to try and win over influential groups among the Dutch population and undermine the legitimacy of the Dutch government and democratic values. The global developments in migration flows, the instability of European borders, or the tensions between Europe and other powers can all play an important role in this respect, particularly with regard to the role or position adopted by the Netherlands.

Incidentally, it is striking that subversion scenarios do not explicitly feature in the regional risk profiles.

8.3 Extremism and terrorism

8.3.1 Risk
As a result of migration flow and the asylum and immigration policy, it has to be taken into account that a 'jealousy debate' may arise; ‘why are so many social facilities free of charge for asylumseekers and not for other citizens?’. Extreme right-wing groups are trying to exploit feelings of fear and anger in relation to the influx of migrants. Their unpredictability and a lack of organisation makes it difficult to gain an insight into who is likely to engage in criminal activities. Furthermore, distinguishing 'concerned citizen' from far right supporter or extremists can be challenging, primarily due to the level of resistance against refugee centres. In response to the increasing support for, and manifestation of, right-wing populism and extremism, left-wing extremists may adopt more aggressive stances. This means it is realistic to expect renewed, violent confrontations between both camps.

The greatest risk within this risk category is, however, the threat represented by jihadism. Never before have there been so many jihadist-terrorist attacks in western countries as in 2015. For example, nine attacks were carried out in Western Europe (with France being the main target). In addition, various attacks have taken

Table 8.4 Building blocks for the worst-case state actors scenario – 'Subversion foreign actors'.

Category	Subcategories	Aims	Resources	Targets
State	Politically inspired extremist groups	Gain and exercise control over own ethnic or religious community	Disseminate hatred; spread fear and create enemies	Own ethnic or religious community
Non-state	Religiously inspired extremist groups	Create parallel society/ enclave of their own with as little government control as possible	Create antagonism between social groups / deliberately cause polarisation	Diaspora communities
	Ethnically inspired extremist groups	Gain and exercise control over diaspora community abroad (control network by foreign government)	Question and undermine the government's legitimaticy	Authorities (national or local)
	Criminal groups	Damage confidence in the government and undermine the legitimacy of the government	Blackmail	Minorities
	Foreign authorities with a substantial diaspora community in the Netherlands	Create a political system which is different to the democratic system	Intimidation	Media
	Authorities from countries with which Europe / the Netherlands has a tense relationship or a conflict	Restrict (basic) rights of other political, religious or ethnic groups/minorities	(Covert) influencing	Science
	Authorities from countries of origin or transit countries of the migration flow	Create a form of society which is different to the open society	Propaganda via classical and social media	Western world/EU
		Win over public opinion	Disinformation via classical and social media	Dutch citizens / public opinion
		Acquire political influence	Recruit people	
		Obtain political or social favours/benefits	Become involved in politics / acquire membership, with a hidden agenda, of political parties, municipal councils, government consultation bodies, etc.	
		Financial gain	Cultivate/task people with influence in the business community	
		Damage the image of the Netherlands and the West	Acquire influence in the media in order to disseminate a certain view	
		Create divisions within the EU	Acquire influence in the world of science	

Table 8.5 Worst-case state actors scenario – 'Subversion foreign actors'.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					○		This corresponds with the description from the guidelines: 'The scenario is very conceivable and there are indications that the scenario can occur'.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position			○			cyber is used as a means; serious violation of the Netherlands' international position.
Physical	Fatalities						Not applicable.
	Seriously injured and chronically ill people						Not applicable.
	A lack of life's basic necessities						Not applicable.
Economic	Costs		○				< 500 million euros.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life						Not applicable.
	Violation of constitutional democratic system				○		Political representation and public administration are seriously compromised for longer than half a year; subversion of support for the democratic system and basic rights.
	Societal impact			○			Corruption scandals, etc. feed social distrust, with the polarisation between social groups being seriously exacerbated.

○ average to considerable uncertainty; ○ minor uncertainty

place in 2016, with the attacks in Brussels making the greatest impression as far as Dutch national security is concerned; not only were they 'close to home', it also transpired that one of the attackers had travelled via the Netherlands (following deportation from Turkey).

The most recent attacks in Western countries match threat assessments, but the relative complexity and scope (in terms of number of victims, targets and perpetrators) has still surprised the experts. The resulting investigations revealed a variety of vulnerabilities in resistance to attacks. For example, it transpired that terrorists can travel to and within Europe relatively simply and unnoticed. For instance, under the cover of the migration flow to Europe.

At the moment, the jihadist threat is the greatest terrorist threat. According current expectations, it will remain so in the coming years as well.

8.3.2 Capabilities

This paragraph describes general capabilities. A more detailed assessment can be found in the theme report.

Spread of responsibilities

Although many ministries and institutes are responsible for (parts of) the capabilities which can increase resilience to extremism and terrorism, the Ministry of Security and Justice (prevention policy and coordination in times of crises), the Ministry of Social Affairs and Employment (increase resilience, prevention of radicalisation, contacts with key figures, provide knowledge), the Ministry of Foreign Affairs (international cooperation), the AIVD (monitor groups and movements), municipalities (anti-radicalisation programmes), the police (monitoring, detection, response) and the Public Prosecutor's Office (detection, prosecution), are regarded as key players.

Pro-action, prevention, preparation

- International cooperation to prevent terrorism
- (Policy) measures against extremism, terrorism and the prevention of social destabilisation
- National Counterterrorism Strategy 2016-2020
- Monitor groups and movements
- Establish and maintain contacts and cooperate with key figures in groups
- Take security measures (to protect people, objects and services which belong to the national domain)
- Increase resilience to and prevention of radicalisation

Repression and aftercare

- Limit the consequences of a crisis (management)
- Control acts of violence
- Deradicalisation
- Prosecute people who have broken the law
- Repair damage to objects
- Help for victims

Knowledge

There is a lot of attention for Islamic threats, both in politics and science, but less for (right-wing and) left-wing extremism. This can create a 'knowledge gap'. It is also important to point out that there are differences in academic and practical knowledge. People within the last group, for example, have operational knowledge and information which is not publicly available. It is not always easy (nor desirable) to share this information. In addition, experts have expressed the need to collect more knowledge on an extremist/ terrorist network's perimetre, to make it gain insight into which actors do or do not belong to this network. Such knowledge can help when taking more specific (preventive) measures.

8.3.3 Determining factors and impact

The building blocks which determine the type of impact and the scope of the impact of extremist or terrorist incidents are shown in table 8.6.

Scenario variants and their impact

The NRB 'Violent loner' scenario (2012) is chosen as normative scenario, because an incident as a consequence of the actions of a violent loner is something that can always occur. A new scenario was developed for a conceivable worst-case incident is, partly with the help of historical cases: 'Multiple terrorist attack'. Apart from the ecological security, which is not jeopardised, both scenarios have an impact on all national security interests. The following contains the summaries of the scenarios with a short clarification. The full description can be found in the theme report.

Normative scenario – 'Violent loner' (NRB 2012)

The NRB 2012 details a 'violent loner' scenario in which a series of murders (attacks) are committed. For a long time, it remains unclear which person or group is responsible. Pressure on investigation services and unrest increases, in particular among politicians. Based on a 'hit list' that has been found, one of them is expected to be the next target. The scenario scores with regard to the social and political security national security interest and, in particular, with regard to violation of the democratic system. A scenario like this also has a socio-psychological impact.

Table 8.6 Extremism and terrorism building blocks.

Actor – Category	Movements	Composition	Aim	Resources	Targets
Right-wing extremism	Neo-Nazism	Lone actor	Recapture the country from Islam	Violent demonstrations	Government and the judicial authorities
Left-wing extremism	Anti-Jewish orientation	Group	More political and cultural rights for a certain group	Arson	Suppliers and service providers
Animal-rights extremism	Anti-Islam orientation		Bring an end to Western influence	Destruction of objects	Other organisations
Jihadist terrorism	Identity-based		Set up an own state	Intimidation	The homes of refugees
Other terrorism	Animal-rights extremism		Drastically change social order	Home visits	Reception centres for asylumseekers
	Resistance to asylum and immigration policy		Retaliation	Involvement in armed combat in conflict area	Houses of prayer
	Anti-fascism		Prevent overwhelming of EU	Violence (assault)	Specific groups/ people
	Anarcho-extremism		Greater awareness of nature & environment	Hostage-taking / kidnappings	Non-specific targets
	Jihadist extremism			Murder	Public events
				Attacks – explosives	Hospital/biolab
				Attacks – weapons	Chemical sector
				Attacks – CBRN	Nuclear sector
				Attacks – cyber	Public transport
					Critical objects
					Other objects

Table 8.7 Violent loner.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.					◉		The likelihood is somewhere between 'somewhat likely' and 'likely' and is therefore regarded as 'Likely-low'.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position		◉				The scenario includes negative publicity aimed at the Netherlands and is reinforced by the activities of the loner.
Physical	Fatalities	◉					There are less than 10 fatalities, more is unlikely.
	Seriously injured and chronically ill people	◉					There are no injuries. However, it is possible that several people will become traumatised.
	A lack of life's basic necessities						Not applicable.
Economic	Costs	◉					Death insurance benefits response costs due to increased security and other services. Together less than 50 million.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life	◉					The activities of a group of threatened people, namely members of parliament, are hampered for a short period of time.
	Violation of constitutional democratic system		◉				There is a limited detrimental impact on the political representation function because members of parliament are being threatened.
	Societal impact		◉				The expectation is that the impact will be limited, but that it will lead to indignation.

◉ average to considerable uncertainty; ◉ minor uncertainty

Table 8.7 Building blocks for the 'Multiple terrorist attack' worst-case scenario'.

Actor – Category	Movements	Composition	Aim	Resources	Targets
Right-wing extremism	Neo-Nazism	Lone actor	Recapture the country from Islam	Violent demonstrations	Government and the judicial authorities
Left-wing extremism	Anti-Jewish orientation	Group	More political and cultural rights for a certain group	Arson	Suppliers and service providers
Animal-rights extremism	Anti-Islam orientation		Bring an end to Western influence	Destruction of objects	Other organisations
Jihadist terrorism	Identity-based		Set up an own state	Intimidation	The homes of refugees
Other terrorism	Animal-rights extremism		Drastically change social order	Home visits	Reception centres for asylumseekers
	Resistance to asylum and immigration policy		Retaliation	Involvement in armed combat in conflict area	Houses of prayer
	Anti-fascism		Prevent overwhelming of EU	Violence (assault)	Specific groups/ people
	Anarcho-extremism		Greater awareness of nature & environment	Hostage-taking / kidnappings	Non-specific targets
	Jihadist extremism			Murder	Public events
				Attacks – explosives	Hospital/biolab
				Attacks – weapons	Chemical sector
				Attacks – CBRN	Nuclear sector
				Attacks – cyber	Public transport
					Critical objects
					Other objects

Table 8.8 Worst-case – Multiple terrorist attack.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.				◉			Due to comparable attacks in surrounding countries, the scenario is regarded as being (somewhat) likely and conceivable. However, a dirty bomb had never previously been used during an attack.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory	○					This criterion may be applicable (for example in the case of serious radiological contamination or after actions against Dutch embassies – dependent on response).
	International position		◉				Decline in tourism; if terrorists are not captured for a long time possibly also pressure on political relations.
Physical	Fatalities			○			On the basis of historical cases, dozens to more than 100 fatalities are expected.
	Seriously injured and chronically ill people			○			On the basis of historical cases, 100 to several hundred fatalities are expected.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			◉			Up to max. 5 billion euros in costs as a consequence of damage to people and objects, and deployment of emergency and security services.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life			◉			Among other things, closing of key traffic hubs makes it difficult for people to go to work/ school/etc.
	Violation of constitutional democratic system		◉				The declaration of a state of emergency can temporarily restrict rights and freedoms. This may be higher depending on the response.
	Societal impact				◉		Based primarily on fear and uncertainty (e.g. with regard to radiological material).

◉ average to considerable uncertainty; ○ minor uncertainty

Worst-case scenario – 'Multiple terrorist attack'
The 'Response to exogenous jihadist threat' scenario, in the NRB 2011, was written, at the time, as a worst-case scenario. However, in recent years, developments have occurred as a result of which some of the consequences described have already materialised (such as a growing anti-Islam movement and increasing polarisation). Therefore, a new worst-case scenario has been developed for the NRP, entitled 'Multiple terrorist attack', based on simultaneous terrorist attacks on a major airport and train station in the centre of the country, both of which are important traffic hubs. Automatic weapons are used as well as explosives and radiological material. Additionally, some of the perpetrators managed to escape.

Likelihood of occurrence of scenarios

On the basis of historical cases (attacks in neighbouring countries) and developments, the threats as described in both the normative and the worst-case scenario are conceivable. However, an attack in which a dirty bomb is exploded has never taken place in the past. There are examples of Chechen rebels who, in 1995 and 1998, placed bombs containing Cesium-137 in respectively a park in Moscow, Russia and near a railway line in Grozny in Chechnya. A threat of a dirty bomb is therefore not purely theoretical. For that reason the worst-case scenario is still regarded as 'somewhat likely'.

8.3.4 In perspective

Although 2015 was an exceptional year with regard to terrorist violence in Europe, by far the majority of terrorist attacks take place outside Western countries. If the attack of 11 September 2001 is included (exceptional high number of fatalities), the percentage of fatalities due to terrorism in Western countries is 2.6% since 2000, and 0.5% without this attack.

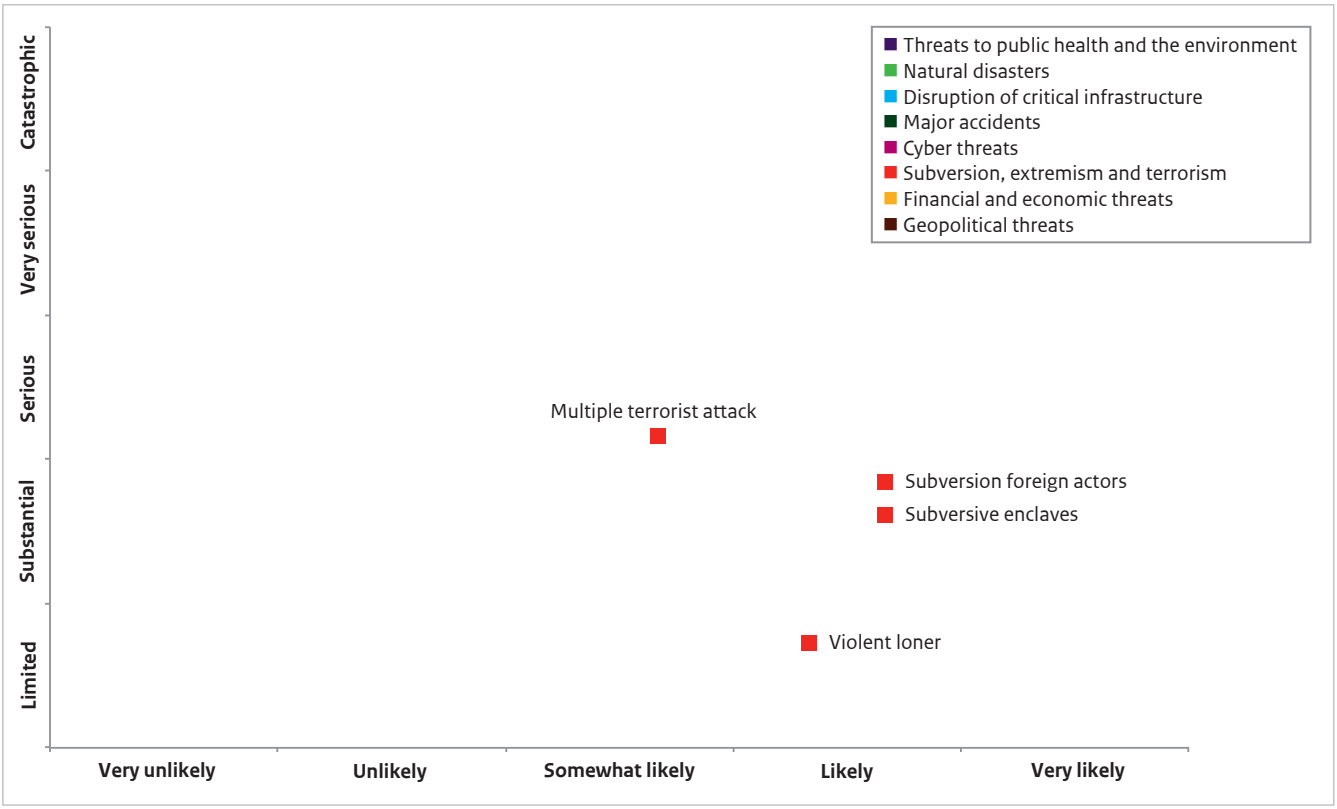
8.4 Conclusion and considerations

The three risk categories within the Extremism and terrorism theme are closely connected. Most actors and driving forces feature, for example, in each category. The Subversion the democratic system and open society risk category describes examples of breeding grounds which, in combination with a 'trigger event', can lead to the escalation of violence as described in the Large-scale public order disturbances and Extremist and terrorism risk categories.

The number of issues in which harmful effects of polarisation can occur has increased. In particular, the influx of refugees (and integration problems) are the subject of fierce debate. In this context, the increased threats, intimidating activities and violent incidents are a cause of concern. On the other hand, there are plenty of initiatives to help refugees. It also appears that far right and right-wing extremist groups, which are trying to stir up feelings, are not really getting a proper foothold. For the time being, Dutch society as a whole therefore appears to be fairly flexible and resilient (including to extremism).

The circumstances that can provide a breeding ground for the incidents described are present in society. For that reason, it continues to be important to keep a close eye on developments. The issues included in the theme are developing and changing and this can, for example, lead to the (ever-stronger) manifestation of disorder. This appears to be the case in neighbouring countries.

Figure 8.1 Subversion, extremism and terrorism risk diagram.



9 Geopolitical threats

9.1 Risk categories

Geopolitics concerns the influence of geographical factors on (international) political issues, and more specifically, the battle to control land, sea and air space in order to define borders and spheres of influence. Geopolitical threats are generally large-scale developments which rarely affect just one country, but usually several (groups of) countries, and which sometimes even have global consequences. In that sense geopolitical developments primarily constitute an overall threat for the entire European Union, with an undeniable knock-on effect on the Netherlands.

In this theme we consider three different risk categories:
- Power shifts within the international state structure;
- Increasing tensions between great powers;
- Resource scarcity.

In this theme chapter we focus on the possible, more or less direct effects of geopolitical developments on the Netherlands. A more general assessment of these developments in a global perspective can be found in Chapter 11. This includes the correlation with other (autonomous) developments, such as economic, social and demographic developments.

Geopolitical threats are overall threats for the entire European Union, with an undeniable knock-on effect on the Netherlands.

9.1.1 Shifting power relations

Shifting power relations in the international-political playing field have traditionally constituted a major geopolitical threat – at least for the parties that lose international power as a result. Such shifts in power relations are often part of a slow process which is influenced by, for example, economic changes and internal social and political developments in various countries. However, certain changes in power relations can also be caused by, for example, armed conflicts, with a well-known example being the Second World War after which the international power relations were extremely different to before.

Developments

A gradual, but clear shift in the international power relations is taking place, and it is not favourable for the Netherlands. The dominance of the West (North America and Europe) in global politics is gradually decreasing in the face of various emerging powers, with China leading the way. In recent years Russia has also assertively started to claim a great power position once again.

The emerging powers sometimes openly question multilateral cooperation structures and international standards and values which have long been regarded as unassailable in the West (including the Netherlands). One of the many examples we could mention is the establishment of the Asian Infrastructure Investment Bank by China, which is intended to act as an alternative to the World Bank and the International Monetary Fund. In addition, internal problems within the EU (for example the Brexit discussion or the migration crisis) have not had a positive effect on Europe's position of power.

As far as the Netherlands are concerned, shifts in international power relations can be a threat, particularly if they have a detrimental effect on the current relative position of power compared to other countries. Such a shift in power relations can take many different forms.

First and foremost the Netherlands is a relatively small player on the international and political stage. However, since the end of the Nineteen Forties it has managed to increase its importance through cooperation with powerful allies in political and economic fields (the European Union and its forerunners) and in a military sense (the North Atlantic Treaty Organisation – NATO). In addition, the multilateral system of international rules and standards, of which the United Nations (UN) is a key

example, is hugely important for the Dutch position in the world. While such generally accepted forms of cooperation and accompanying rules in international politics are, to a certain extent, having a levelling effect on international power relations – being based not on the survival of the fittest but more or less equal relations with each other via regulated conduct – a relatively small country can make more gains than a great power that can also impose its will without multilateral forms of cooperation. Consequently, the violation of such alliances and multilateral links would also threaten the global position of the Netherlands.

9.1.2 Tensions between the great powers

Tensions are increasing between the great powers, in particular between China and the United States, and between the West (EU/US) and Russia. Such tensions are leading to a certain degree of instability in the international system and, in addition, there is always a risk of escalation. Escalating tensions can lead to conflict, both armed (war or proxy-wars in each other's sphere of influence) and unarmed (for example in the form of a trade boycott or other types of sanctions). There is also a chance that tense relations between great powers will cause them to be less inclined to adopt a cooperative attitude in multilateral institutions and negotiations, thereby causing them to lose importance.

Developments

It is partly the influence of the emerging powers and the tension between great powers that is making it increasingly difficult for the global system of multilateral cooperation to function. The rules, values and principles on which this system is based are increasingly being questioned, not only because emerging powers are openly criticising what are regarded as 'Western' core values of the current multilateral system, but also because agreement between the great powers is becoming more and more difficult as their relationship becomes more and more tense.

9.1.3 Resource scarcity

Increasing prosperity and a growing world population are leading to greater global pressure on the extraction and use of raw materials. In itself, resource scarcity is not a geopolitical threat. However, in the event of a conflict about acquiring access to raw materials, or in the event that the scarcity of raw materials is used as an instrument by states to exert power, this is tantamount to a geopolitical threat with all the possible consequences this entails.

9.1.4 Selection of developed risk categories

Because the consequences of a shifting balance of power for the Netherlands (and its allies) are closely related to those of increasing tensions between great powers, these are included in the latter risk category. The resource scarcity risk category is developed separately.

9.2 Increasing tensions between the great powers

9.2.1 Risk

Tension between the great powers, in particular between the US/EU and Russia and China/US, is clearly increasing, partly because of the global shift in power in the direction of emerging powers. A few current examples of where this tension is surfacing are the Chinese-American disagreement about territorial claims in the South China Sea and about cyber espionage, as well as the tensions between the EU and the US (including in a NATO context) on the one hand, and Russia on the other, with regard to Russian military interference in Ukraine and Syria. As a result, the risk of direct or indirect armed confrontations between great powers is also increasing. Although, for the time being, all the countries involved appear to be doing their best to prevent large-scale escalation of the tensions, such an atmosphere always provides a fertile breeding ground for unintended escalation in which the effects of actions, miscommunication or mistakes, which have not been factored in, can have major consequences in times of tension.

The Netherlands face a variety of threats due to tensions between great powers. If a tense situation were to escalate, the Netherlands would also experience immediately harmful consequences, certainly in relation to the economy, because the Dutch economy is extremely dependent on international free trade. However, it could also be affected in other areas. If Dutch allies were to become involved in an armed conflict, the Netherlands would find it difficult not to get involved as well.

9.2.2 Determining factors and impact

Key factors which determine the impact and scope of increasing tensions between the great powers (see table 9.1) are, for example, the actors involved and the geographical proximity of the escalating incident or conflict. Conflicts on the borders of the EU have a more direct effect than conflicts elsewhere in the world. This has to do particularly with the direct involvement of NATO in this case (an attack on one is an attack on all). If the US were to be attacked, the Netherlands would

Table 9.1 General building blocks for impact of tensions between great powers.

Great powers involved	Geographical proximity of conflict	Type of conflict	Use of instruments	Degree of escalation
EU	EU borders	Armed	Military	High
Russia	Elsewhere in the world	Unarmed	Cyber	Medium
China		Hybrid	Economic	Low
US			Influence through interference (in companies, political and ideological groups, administration)	

also be obliged, as an ally, to provide support. The degree of escalation is also an important factor. If an incident were to escalate very quickly and to a high level, this would have major consequences for the Netherlands.

The use of instruments determines the type of conflict, with all possible resources being used in the event of hybrid warfare: conventional military resources, but also wide range of non-military resources, such as political influencing of the enemy, economic blackmail, cyber attacks, propaganda, etc. See also Chapter 11.

The phenomenon of hybrid threat is an increasing concern. The insidious way of dealing with conflicts and the deception, ambiguity and denial which accompanies the actions hamper the attribution and response.

Normative scenario

A combination of building blocks can lead to a realistic and feasible (so-called 'normative') scenario (see table 9.2). A scenario has been chosen in which tensions exist between Russia and a NATO ally (Latvia), leading to the Netherlands becoming involved in a conflict. This conflict came about after the escalation of a minor border incident. The following is a short summary. The complete scenario is described in the corresponding theme report.

Scenario summary

During an exercise in Latvia a number of soldiers find themselves, by mistake, on Russian territory. Russian border troops make a mistake when assessing the situation and accidentally kill them. This leads to furious responses in Latvia. The Russian Embassy is set on fire and ethnic Russians are attacked. The Russians who had been attacked organise themselves into a kind of rebel movement. The response of the Russian government is initially reticent but public indignation at home causes it to provide a certain degree of support to the rebels. The conflict gradually escalates to the level at which rebels supported by Russia take up arms to seize power in Latvia on the premise of protecting the threatened Russian minority.

Table 9.2 Building blocks for the normative scenario.

Great powers involved	Geographical proximity of conflict	Type of conflict	Use of instruments	Degree of escalation
EU	EU borders	Armed	Military	High
Russia	Elsewhere in the world	Unarmed	Cyber	Medium
China		Hybrid	Economic	Low
US			Influence through interference (in companies, political and ideological groups, administration)	

Table 9.3 Normative scenario – international conflict.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.				◉			
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory		◉				Allied territory is compromised, as is Dutch cyber integrity.
	International position				◉		A part of the international community regards the Netherlands (as a NATO member) as an aggressor because NATO behaves in a way which escalates the conflict;the Russian disinformation campaign damages its position within NATO.
Physical	Fatalities		○				Several dozen Dutch soldiers are killed.
	Seriously injured and chronically ill people		◉				A few Dutch soldiers are injured and several suffer from PTSS.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			◉			Trade with Russia ceases and several countries set up a trade boycott.
	Violation of vitality						Not applicable.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life						Not applicable.
	Violation of constitutional democratic system		○				Russian cyber provocations increase mistrust of government.
	Societal impact		◉				Fear of further escalation of violence; regional tensions relating to the natural gas debate.

◉ average to considerable uncertainty; ○ minor uncertainty

NATO takes action on the basis of a '*coalition of the willing*' and the Netherlands also send soldiers to the region. However, the hybrid conflict quickly spreads to Estonia and Lithuania and Russia does not hesitate to use a variety of instruments, such as provocative cyber operations.

In addition, trade between Russia and NATO countries ceases, a number of other countries set up a trade boycott of NATO member states as a protest against a lack of a de-escalating policy and Russian gas supplies to Europe are largely terminated, leading to an increase in the international gas price. An appeal for an increase in Dutch gas extraction leads to protests in Groningen, where the population is afraid of new earthquake damage.

Several dozen Dutch soldiers are killed during armed confrontations. Dutch society responds very emotionally to the conflict and the Dutch victims, without things getting out of hand. A certain degree of social commotion arises with regard to some (new) political parties that are said to receive financial support from Russia, as well as Russian attempts to influence journalists and users of social media.

Likelihood of occurrence of scenario

The probability of an incident escalating, against the backdrop of tense relations between the great powers, is still relatively limited, but it is certainly feasible. With regard to impact the consequences are relatively limited.

9.2.3 In perspective

The probability of an incident escalating into an armed conflict increases with rising tension between great powers. Although history has shown that the possibility exists of such tensions escalating into a global conflict, it has been decided not to develop this escalation in any great detail in a scenario because the probability of it occurring is regarded as extremely small (see also the observations on the geopolitical developments at global level in Chapter 11). If a scenario like this nevertheless occurs, our national security will be evidently threatened and the impact will be extremely large for several criteria, and possibly even 'beyond worst-case'.

We also have to bear in mind that the emerging powers, including the more assertive powers like Russia and China, are economically (and therefore also socially and politically) dependent on the global market for goods, raw materials, power and capital. In that sense they also stand to gain something from increasing international tensions so that they turn into an actual conflict, in addition to smaller-scale squabbles in which the conflicts between (semi-) great powers is conducted indirectly in other countries (also referred to as proxy wars).

9.3 Resource scarcity

9.3.1 Risk

A typical geopolitical threat such as the battle for raw materials can also have negative consequences for the Netherlands. If scarce, and important raw materials becoming even more scarce, and therefore more expensive, this can have a major economic impact. With regard to the majority of raw materials the damage will be limited to the economic domain. However, there are also raw materials which can have direct and broader consequences for national security. One example is an oil crisis, like the one that took place in the '70s, or the shortage in minerals that threatened to arise due to a Chinese embargo in 2010.

A scarcity of raw materials can, in some cases, lead to military conflicts, for example if various parties try to get control of these raw materials, or if a party that owns these raw materials tries to use this position as a way of gaining power in relation to other political or economic issues. In addition, the raw materials policy of other countries, for example via interference of state-owned companies, '*country-grabbing*' and the creation of trade restrictions and stocks, can have direct and indirect consequences for national security.

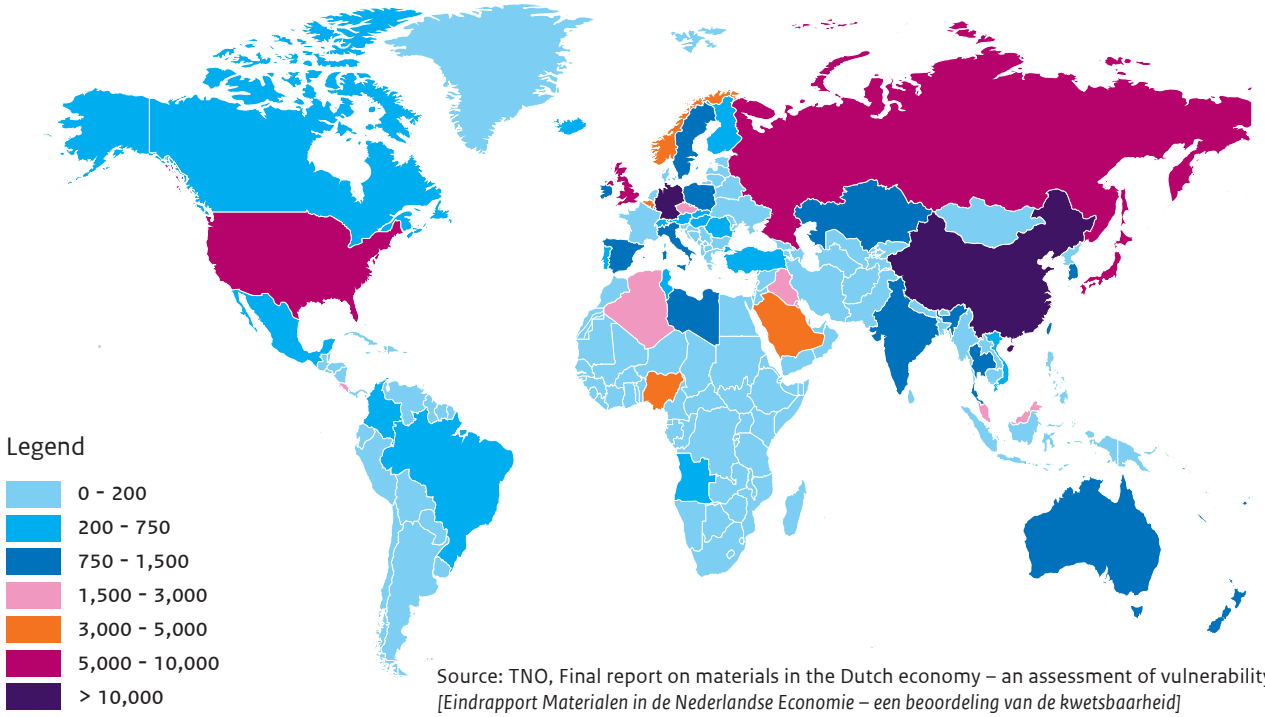
With regard to scarcity of raw materials this means, in particular, fossil fuels, phosphate, minerals and metals such as iron ore, copper and rare earth metals. One cause for concern is that some of these raw materials are concentrated in (not always stable) non-Western countries and regions. China is, for example, the largest producer of rare earth metals (essential for many high-tech processes) and minerals. The Netherlands are largely dependent on Morocco for the supply of phosphate, which is important for food production. In 2014 TNO carried out a vulnerability analysis into Dutch imports of a group of 22 strategic raw materials for the Dutch economy.[13] This study revealed that phosphate and metals from the so-called platinum group are extremely important for the Dutch economy and that the main risk applies to the security of supply of rare earth metals, antimony, tungsten and indium.[14]

Figure 9.1 shows the relative interest of the trade partners in the supply of the 22 strategic raw materials.

[13] These are: Antimony, beryllium, chrome, coking coal, fluorite, phosphate, graphite, indium, cobalt, light rare earth metals, lithium, molybdenum, niobium, platinum group metals, silicon, tin, titanium dioxide, vanadium, tungsten, silver, zinc and heavy rare earth metals. Fossil fuels are not included in this study.

[14] Ton Bastein, Elmer Rietveld en Stephan van Zyl, *Final report on materials in the Dutch economy – an assessment of vulnerability [Eindrapport Materialen in de Nederlandse economie – een beoordeling van de kwetsbaarheid]*, Delft: TNO, May 2014, p.4

Figure 9.1 Input value of 22 strategic raw materials in millions of euros.



Source: TNO, Final report on materials in the Dutch economy – an assessment of vulnerability *[Eindrapport Materialen in de Nederlandse Economie – een beoordeling van de kwetsbaarheid]*

9.3.2 Scenario variant and impact

Scenarios were worked out in more detail previously in the NRB which are still relevant for this risk category. In 2007 the *Oil geopolitics* scenario was described, in which the supply of oil on the global market decreases seriously due to the loss of part of the production from the Middle East, as a consequence of an internal conflict. The loss of a substantial part of the global production immediately led to very significant price increases in oil and oil products. At the time this scenario had a relatively high likelihood and had, in particular, very serious consequences for the Dutch economy, despite the use of the IEA oil crisis mechanism. Although this scenario assumed an extremely high oil price, which is now actually very low, this scenario is still an example of the possible consequences of scarce raw materials. Such processes can, in fact, also occur in connection with other types of raw materials and fuels. For example, the expectation is that the demand for copper will increase explosively in the near future (although it is difficult to assess when exactly this will be). In addition to oil, natural gas is also an important fuel with a fluctuating supply and demand mechanism.

The 2010 NRB detailed the *Minerals scarcity* scenario. This includes an exponentially increased growth in minerals due to a global economic demand which, among other things, is related to the transition to sustainable sources of energy. This scenario also includes a disruption to the supply because an extremely important producer imposes trade restrictions for a number of key minerals, causing prices to increase enormously. The consequences of this scenario particularly affected the competitive position of Dutch and European industry. Such a scenario is now considered to be less likely because, a number of years ago, China imposed an export quota for rare earth metals, after which other (Western) mining companies again started to extract rare earth metals themselves. This had a particular effect on China itself.

The *Oil geopolitics* scenario was selected as representative of the resource scarcity risk category.

Summary of Oil geopolitics scenario

The supply of oil on the global market decreases due to the loss of part of the production from the Middle East, as a consequence of an internal conflict between Islamic groups in one of the Middle East countries. The loss of a considerable part of the global production will immediately lead to very significant price increases in oil and oil products. The insufficient spare production capacity available worldwide means the decision has been taken to use up emergency stocks via the IEA oil crisis mechanism.

Despite the use of that crisis mechanism an oil crisis has certain consequences for the global economy and therefore also for the Dutch economy. A number of sectors are affected, transport costs increase (and therefore also the costs of other products, primarily basic foodstuffs) and inflation also rises. Confidence in the economy decreases, causing people to start hoarding, for example. Consequences can also be expected for the social and political stability in the Netherlands, in particular because the crisis originated in a conflict between Islamic groups.

Table 9.4 Resource scarcity – Oil geopolitics scenario.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				○			
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					Declining tourism and recalled embassy staff.
Physical	Fatalities	◎					Possible in the event of fights.
	Seriously injured and chronically ill people	◎					Ditto. Also a possibility of several people suffering long-term psychological damage.
	A lack of life's basic necessities						Not applicable (however, products do become more expensive).
Economic	Costs				◎		Number of sectors are hit hard. Long-term effects.
	Violation of vitality	○					The structural violation of the economy is limited, e.g. due to substitution possibilities.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life			○			Restriction of freedom of movement for a long period. This affects a large group of people.
	Violation of constitutional democratic system	◎					Limited violation of public order and security. Declining confidence in government.
	Societal impact		◎				Uncertainty about duration of the crisis; hoarding; tensions between groups.

○ average to considerable uncertainty; ◎ minor uncertainty

Likelihood of occurrence of scenario

On the basis of economic model calculations, the likelihood of a disruption occurring at least once in a period of 5 years, of 10 mln. barrels or more a day and lasting at least one month, is assessed at 6.25%. The probability of a disruption lasting longer than 1 month is assessed at 50%. The probability that the cause of that disruption being related to a war in the Middle East is estimated at 60%. Consequently, the cumulative probability of this scenario is 1.9% over 5 years and that corresponds to the classification of 'somewhat likely'.

9.3.3 In perspective

The international battle for scare resources appears to have decreased in relative terms in recent years. Whereas a number of years ago the huge demand from China, in particular, caused excessive increases in raw materials prices, which in turn intensified the battle for those raw materials, the demand as well as the price and the fight have all declined during the past few years. In the case of key raw materials such as oil and gas it is currently more accurate to speak of overproduction than scarcity and prices are therefore extremely low. Although precious metals continue to be scarce, the geopolitical fight for these raw materials, which is expressed by, among other things, the Chinese investments in African countries, no longer appears to be as fierce as a few years ago.

In addition, corrective (economic) mechanisms come into play in the event of scarcity. In the event of a shortage of raw materials or higher prices, attempts are made to find the raw materials in new locations. In addition, scarcity will encourage the market to look for alternatives (substitution) which are only profitable in conjunction with higher prices. Finally, it will become more attractive to recycle, although the feasibility of this depends on the raw material.

Nevertheless raw materials continue to be an important geopolitical instrument, primarily in the short term, as a result of which countries and regions where such raw materials are located will always be attractive spheres of influence and therefore a possible source of conflict.

9.3.4 Capabilities

Pro-action, prevention and preparation

Geopolitical threats are an excellent example of developments with global consequences. The question is, therefore, whether the Netherlands alone can contribute to risk management in order to prevent or reduce such threats. Risk management – as regards pro-action, prevention and preparation – can, from this perspective, only really be tackled at international level, whether via international organisations such as the UN or the EU, via military alliances such as NATO, or via bilateral cooperation on certain issues between the Netherlands and any other country. A serious Dutch commitment to international cooperation, both diplomatically and militarily, as well as with regard to, for example, economic partnerships will help to reduce geopolitical threats to a certain extent.

The current capabilities of the Netherlands with regard to pro-action, prevention and preparation within the framework of geopolitical threats are therefore primarily related to international cooperation. Traditionally, the Netherlands have been an active player in multilateral diplomacy, through the promotion of international peace and security as a powerful point of departure. From the military and economic points of view the focus of the Netherlands is also on broad international cooperation. In that context the Netherlands are continually working proactively and preventively on keeping geopolitical threats to a minimum.

Because there are so many different dimensions to geopolitical developments, information and analysis capabilities also represent a capacity which helps to be prepared for possible future developments. That capacity is available in the Netherlands from the intelligence services, the various ministries and knowledge institutions. In addition, the capacity relating to making information and analyses available to all the parties involved (information sharing) is an important factor when it comes to pro-action, prevention and preparation.

Response and Aftercare

If geopolitical threats result in a crisis which (among other things) directly affects the Netherlands, national crisis management will be required in the sense of response and aftercare.

This response will also largely have to be tackled at international level, partly because it is almost unthinkable that only the Netherlands will be affected by such a crisis. It also applies that Dutch capacity is linked primarily to foreign and defence policy with the focus, once again, on close cooperation with foreign allies. Nevertheless it may, to a certain extent, be possible to manage the national consequences of such crises via national policy, for example by keeping socio-economic damage and social unrest to a minimum. Proper risk management primarily involves the proactive use of macro-economic policy by central government, although regional and local policy layers may also play an influential role in this respect. The precise use of this instrument depends on the specific events, for example the capacity to support certain economic sectors which run into problems due to geopolitical developments by,

among other things, helping to change companies so that they are no longer dependent on certain customers, suppliers, or raw materials. Sound government communication, for example to prevent panic and negativism, can also be referred to as response capability.

Because geopolitical threats can include so many different facets, it is difficult to be prepared in detail beforehand for all the conceivable consequences. However, the Netherlands have a government organisation which is equipped to change course rapidly, dares to think 'out of the box' and can adapt flexibly to sudden events.

9.4 Conclusion and considerations

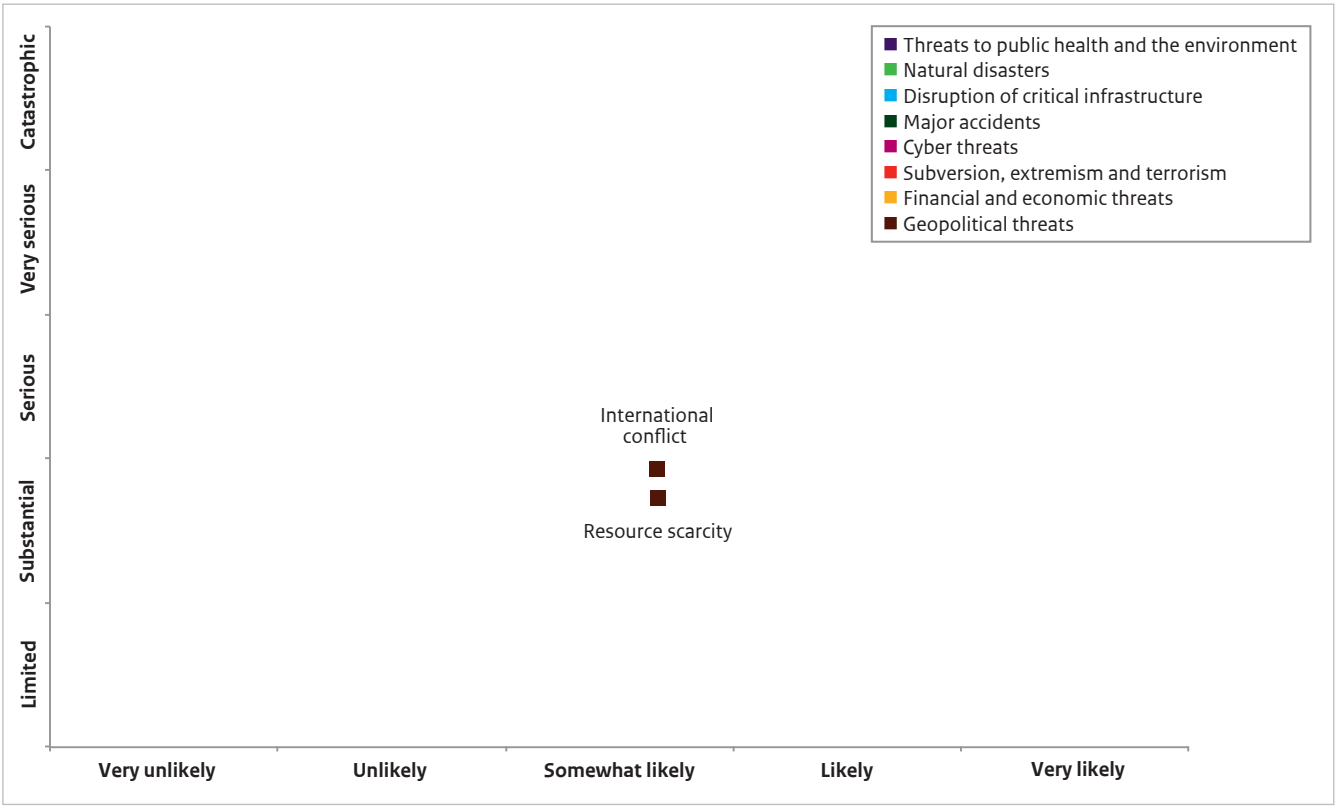
Geopolitical threats for the Netherlands particularly mean shifts in the international power relations, tensions between great powers and resource scarcity. The threat represented by these developments can be expected more in the long term than the short term.

Because geopolitical threats primarily mean developments with global consequences, the question is whether the Dutch government can, on its own, make much of a contribution to risk management with a view to preventing or reducing such threats. Risk management will primarily have to be tackled in an international context.

If geopolitical threats result in an actual crisis which has harmful consequences for Dutch national security as, to a certain extent, in the two scenarios described here, the response will still partially have to be organised in an international context. Nevertheless, the national consequences of such crises can partially be governed by national policy. This could take the form of keeping socio-economic damage and social unrest to a minimum.

The current capabilities of the Netherlands within the framework of geopolitical crisis management are linked particularly to international cooperation. From the diplomatic, military and economic points of view the focus of the Netherlands is on broad international cooperation. In addition, information and analysis capabilities, which are available from the intelligence services, various ministries and knowledge institutions, represent a capacity which contributes to being prepared for possible geopolitical threat situations.

Figure 9.2 Geopolitical threats risk diagram.




Index

10 Financial and economic threats

10.1 Risk categories

With regard to the Financial-economic threats theme, the focus is on potential incidents or crises which can occur within the financial-economic system and which have such an impact that they can also affect national security. This means events which can, in any event, be differentiated from the normal pattern of fluctuations in the economy. A distinction is made according to the following risk categories:

- **Destabilisation of the financial system**
  There are various elements of the current financial and economic system which can, potentially, lead to destabilisation. Issues such as current low interest rate, the high debt burden of authorities and the loan portfolios with (primarily southern European) banks and the low inflationrate imply certain risks. When developing the NRP an assessment was made of any consequences and impact of a new financial crisis on national security.

- **Cyber crime in the financial sector**
  This means, in particular, types of cyber crime which may lead to a large-scale impact. The classification into critical processes also applied within the NRP. This also means crime aimed at retail transactions, consumer financial transactions, high-value transactions between banks and securities trading.

- **Other economic crime**
  Within this part the accent is on other deliberate actions by criminal organisations (other than via the cyber domain). Issues such as large-scale crime and criminal interference in critical organisations are also dealt with. The detailing is linked to scenarios which have already been developed in the National Risk Assessment (NRB).

The relevant developments for this theme are described in Chapter 11.

10.2 Destabilisation of the financial system

10.2.1 Risk

The financial system has been regularly destabilised in the past. Examples of the major crisis during the '30s and '80s when there were high levels of unemployment, national debt, inflation and interest rates and a stagnant housing market. The most recent financial crisis (2008) was characterised by the collapse of major banks with the policy response consisting of fiscal incentives and broader funding. This limited the consequences. However, there is still no real recovery in Europe, partly due to the continuing policy uncertainty as a consequence of the problems relating to Greece and Brexit, which is formally going to be initiated in 2017. Despite various key measures taken in recent years, such as the higher buffers for banks, destabilisation of the financial system is still possible and can once again lead to a financial crisis if the underlying problems continue. There are various elements of the current financial and economic system which can, potentially, lead to destabilisation. Issues such as current low interest rate, the high debt burden of authorities and the loan portfolios with (primarily southern European) banks and the low inflation imply certain risks.

There are various elements of the current financial and economic system which can, potentially, lead to destabilisation.

The financial crisis of 2008 is a good example of an initially limited crisis which unexpectedly spread to other financial markets and to the actual economy sometime later. The total costs of the 2008 crisis are difficult to determine and estimates vary greatly. Significant economic costs in this context are the loss of production of the Dutch economy, the rise in unemployment and the increase in public debt.

The question of whether such a crisis can occur again in the current climate is an appropriate one. An assessment of the monetary policy that is effective at lowering interest rates and also covers the widespread buying up of financial securities by the central banks reveals risky side-effects. For example the long-term low interest rate is leading to increased tension in the financial system. The fact that large debts are becoming normal and investors' increasing willingness to take risks will, if interest levels rise, lead to increasing turbulence within the financial system. In effect, a major underlying problem of the previous financial crisis has not been improved, namely the highly levels of debt on the part of governments and households.

In addition, the low interest rate is bringing pressure to bear on the funding ratios of the pension funds and, as a consequence, retired people's pensions are being cut. Life insurance companies are also suffering major damage from the low interest rate, and this too is pressurising their business models. As a result, investors are looking for higher yields at higher risks, in what is known as the 'search for yield'. The Dutch Central Bank [De Nederlandsche Bank] believes that the combination of the current broad monetary relationships and the greater willingness to take risks has increased the possibility of a financial bubble being formed. On the one hand normalisation of the interest rates may then result in significant decreases in the values of securities and therefore to increasing turbulence on the financial markets. On the other hand a continuation of low interest rates is also quite likely.

Another key question relates to contamination risk: Can an incident that starts on a small scale be limited to a single sector, or can it spread later to other sectors (as was the case with the 2008 crisis)? A contamination risk is conceivable due to the connectedness and the interconnectedness within a sector and between the sectors. For example, there are still links (despite new regulations) between the regulated banks and the shadow banks, meaning that problems at the shadow banks can spread to the regulated banks. In addition, the financial markets are, by definition, connected to each other by the many hybrid products.

Besides the contamination risk, public confidence in the system is another important factor for any consequences of an incident or crisis. Should a financial crisis occur, questions will arise about the possibilities taking action and gaining control, given the apparent lack of additional instruments needed in a crisis, meaning that there appears to be limited space to absorb new shocks. That could mean that a crisis may potentially have greater consequences than the 2008 crisis. From the national security perspective, a financial crisis will primarily impact economic and social and political stability.

10.2.2 Capabilities

Since the onset of the financial crisis a significant number of measures were being taken to make financial institutions more resilient and subservient. For example, the capital requirements applicable to banks have been substantially increased. Depending on the scope and the risk profile of the banks, the minimum capital requirements that banks have to serve are three to five times higher than before the crisis. In addition, the quality requirements which this capital has to fulfil have also become stricter. In addition, greater demands have been imposed with regard to the unweighted capital requirements *(leverage ratio)*, with which the four most important system banks in the Netherlands now more or less comply.

At the time of the financial crisis many banks had to be supported using taxpayer money. Meanwhile, agreements have been made at EU level. If a bank gets into trouble again, the ones who initially suffer the losses are those who took on the risk. A bank tax has also been introduced and banks have to contribute to the deposit guarantee funds. Finally, measures have also been taken to improve the working procedures and culture and both the supervision of the financial institutions and the internal supervision have been strengthened.

The government is also trying to create a more diverse financing landscape by encouraging competition and creating space for new players in the financial sector. In addition to these stringent requirements, the government has also tried to take measures aimed at making the banks more service oriented, with a focus on the customer. For example, the general duty of care was introduced for financial service providers in 2014, a ban has been imposed on commissions and the competency requirements for financial service providers have also been made more stringent. On top of this, strict rules on remuneration were introduced in 2015 which are intended to reduce irresponsible risk-taking.
In addition, Dutch public finances offer a certain amount of space to counteract the negative consequences for the real economy of any new financial crisis.

The government debt ratio was 65.4% in 2016 and is therefore significantly higher than the 42.4% in 2007. This means that the room for the government to intervene directly in the financial sector through acquisitions (which have an immediate impact on national debt) has become smaller.

Table 10.1 Impact assessment of destabilisation of the financial system.

Likelihood assessment							
		Very unlikely	**Unlikely**	**Somewhat likely**	**Likely**	**Very likely**	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				◉			
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					The crisis will be international in nature. The reputation of Western capitalism will also be negatively affected.
Physical	Fatalities						Not applicable.
	Seriously injured and chronically ill people						Not applicable.
	A lack of life's basic necessities						Not applicable.
Economic	Costs				◉		There is considerable loss of production (40 billion), a significant rise in unemployment and a serious decline in public finances.
	Violation of vitality				◉		The debt ratio increases substantially. Unemployment will increase: in any event by as much as 100,000 and perhaps even 200,000.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life						Not applicable.
	Violation of constitutional democratic system	○					The functioning of public administration, public order and the independent judiciary will only be slightly compromised by a new financial crisis.
	Societal impact		◉				A new financial crisis with rising unemployment and declining economic growth will have a detrimental effect on citizens' confidence in the state. An increase in social unrest and polarisation is expected. The mutual solidarity in Dutch society will decrease.

◉ average to considerable uncertainty; ○ minor uncertainty

10.2.3 Destabilisation of the financial system scenario variant

The financial markets in 2016 are jittery. Many things can cause considerable turbulence on the financial markets. These include geopolitical tensions, the transformation of the Chinese economy, Brexit and its consequences, the consistently low oil price, the vulnerable economic growth in Europe, the American elections, etc. Any negative developments with regard to any of these issues can trigger a response on the financial markets which will then spread to other parts of the financial system, such as banks and shadow banks.

10.3 Cyber crime in the financial sector

10.3.1 Risk

The analysis of the cyber threats (see NRP Chapter 7, and the underlying report) referred to, among other things, the possible risks of large-scale targeted cyber crime in the financial sector. Cyber attacks aimed at payment and securities transactions can cause the shut-down of critical parts of the financial system, as a result of which, in a worst-case scenario, the financial stability may be jeopardised.
The term 'large-scale cyber crime' means that a form of cyber crime (form of crime aimed at an ICT system or the information which is processed by such a system) leads to a large-scale impact.

Cyber attacks aimed at payment and securities transactions can shut down critical parts of the financial system.

The fact that perpetrators are difficult to trace in the cyber domain means there is a relatively low chance of catching people involved in cyber crime. In addition, it is easier for cyber criminals to operate internationally and that makes detection particularly difficult because of the dependency on foreign agencies. In addition to this, cyber crime can quickly be profitable for perpetrators because of the considerable benefits of scale which can be achieved. For example, many people can fall victim to a phishing attack within a short period of time.
According to the Cyber Security Assessment Netherlands 2015 [Cyber Security Beeld Nederland 2015] cyber criminals can be interpreted as: 'Actors who commit cyber crime professionally, the main aim of which is financial gain'. The CSBN differentiates between the following groups of cyber criminals:

- in a strict sense, those who carry out attacks themselves (or threaten to do so) for monetary gain;
- criminal cyber service providers, those who offer services and tools through which or
- with which others can carry out cyber attacks;
- dealers or service providers for stolen information;
- criminals who use cyber attacks for traditional crime.

10.3.2 Capabilities

Adequate prevention, detection and response to cyber attacks in the financial sector is of considerable social importance.

Preventive

The financial sector is taking various measures which are intended to safeguard the integrity and confidentiality of the provision of information. Supervision is provided by DNB and AFM. Increasing the cyber resilience of financial institutions is high on the DNB agenda. For example DNB is developing a framework at national level to test the ICT systems of Dutch financial institutions. Work is also going on at international level on standards which are intended to increase cyber resilience. This is important because the payment transactions are set up internationally and can no longer be regarded as typical Dutch or national payment transactions.
The financial sector has itself taken measures, for example to detect suspect transactions. This information is not only used within one financial organisation for further analysis and response, since there are also interbank forms of cooperation in which the relevant cyber security information is shared for further analysis and understanding in the fight against cyber crime.

Response

There are various crisis measures and procedures which are intended to resolve disruptions caused by a cyber attack. The financial institutions each have their own crisis management structures which are regularly tested. In addition to this, a crisis management consultation body exists at sector level. These structures are linked to national and international structures, for example, to the crisis plans of the Ministry of Finance and to the European System of Central Banks.

10.3.3 Impact and scenario variant

Cyber attacks on payment transactions primarily lead to direct financial damage but can also indirectly influence financial stability whenever confidence might be damaged on a large scale and for the long term. This is detailed in the cyber attack of the financial system scenario.

Table 10.2 Factoren scenariovariant.

Cause	Actor	Motive	Target / people affected	Nature of the violation	Degree of penetration	Duration
Technical failure	Professional criminals	Idealistic	Public administration and politicians	Violation of availability	Small number of the institutions/ organisations/ companies/citizens affected	Up to 1 day
Human error	States	Economic gain	Public organisations	Violation of integrity	Large number of the institutions/ organisations/ companies/citizens affected	2 to 6 days
Deliberate	Terrorists	Reinforcement of information position	Private organisations	Violation of confidentiality	Majority of the institutions/ organisations/ companies/citizens affected	1 to 4 weeks
	Cyber vandals and script kiddies	Destabilisation of society	Citizens			1 to 6 months
	Hacktivists	Protest				Six months or longer
	Internal actors					Irreparable
	Cyber researchers					
	Private organisations					

Cyber attack on the financial system scenario variant
Interbank settlement is affected by malware, in which large amounts (billions of euros) are diverted by cyber criminals. This causes a liquidity problem at the affected banks, as a result of which they risk collapsing. This option is conceivable when based on a cyber crime motive but, with regard to impact, depends on which banks are affected. Government support is available for the major banks because they are regarded as system banks. However, the same does not apply to smaller banks, and it is also conceivable that the malware affects several small banks in a similar way. The BC VIF platform describes this as a systemic risk: 'Although, in the event of failure of high-end payment transactions between banks and securities transactions, social unrest is less likely, that substantial financial-economic damage can occur due to the very high total amount that is involved.' The expectation is that, if several (small) banks collapse, social unrest will occur.
The determining factors and the chosen scenario variant are shown below (highlighted).

Scenario line

The European interbank settlement system (TARGET2)[15] is affected by malware, in which large amounts (billions of euros) are diverted by cyber criminals. This causes a liquidity problem at the affected banks, as a result of which they risk collapsing. Because a number of the affected banks are not designated as system banks, no government support is made available. Huge numbers of affected customers try, for a number of weeks, to transfer their money to other (unaffected) banks, thereby increasing the liquidity problem of the affected banks. During this period the policy is not to provide government support to the smaller banks that have been affected.

[15] TARGET2 is an interbank payment system for the real-time processing of cross-border payments within the European Union. More information can be found at: *https://www.ecb.europa.eu/paym/t2/html/index.and.html*

Table 10.3 Impact assessment of cyber attack on the financial system.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	**Explanation**
Likelihood of the scenario occurring between now and 5 years.				◉			No specific indications, but the scenario is considered to be somewhat conceivable.
Impact assessment							
Security interest	**Criterion**	Limited	Substantial	Serious	Very serious	Catastrophic	**Explanation**
Territorial	Territory						Not applicable.*
	International position	○					Damage to the reputation of the affected banks and infringement of the international confidence in the Dutch financial sector.
Physical	Fatalities						Not applicable.
	Seriously injured and chronically ill people						Not applicable.
	A lack of life's basic necessities						Not applicable.
Economic	Costs			◉			Financial damage which the affected banks have suffered is added together. This means the estimated damage is between 5 and 50 billion euros. If TARGET2 is shut down, however, settlement processes on a European scale (and therefore interbank transactions) will no longer be possible.
	Violation of vitality		◉				Government support (provided after all) or damage suffered by customers is estimated to lead to a 1-3% increase in the national debt. With regard to unemployment people will be broadly affected over a number of different sectors (< 50,000).
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life			◉			Affected citizens will temporarily not have any money, or will not have sufficient money available. The expectation is that this group will include > 1,000,000 people, based on a time limit of between 3 days and 1 week.
	Violation of constitutional democratic system	○					Distrust of politicians because they let it happen.
	Societal impact		○				Public unrest, demonstrations, large media campaigns. Emotions will be directed particularly at the banking sector.

◉ average to considerable uncertainty; ○ minor uncertainty

* Het Criterion 1.1.B. digitale ruimte is hier wel van belang, maar nog in bewerking en derhalve niet verder gekwalificeerd.

10.4 Other economic crime

10.4.1 Risk

Within this risk category the accent is on deliberate actions by criminal organisations. Issues such as large-scale crime and criminal interference in critical organisations are also dealt with.

The detailing is linked to scenarios which have already been developed in the National Risk Assessment (NRB), from which two have been selected for the NRP.

1. Criminal interference in the critical business community (NRB 2008/2009)
2. Foreign concern / criminal Trojan horse (NRB6)

Based on the scores in the NRB the 'criminal interference' scenario is considered the worst-case scenario and the 'Foreign concern turns out to be criminal Trojan horse' scenario is considered normative. In the NRP they are renamed 'Criminal subversion of critical business' and 'Criminal foreign concern'.

10.4.2 Capabilities

In the case of 'other economic crime' it is very important to identify or prevent risks as early as possible. Linking to the 2014 capability analysis, three capabilities are briefly explained in this paragraph.

Gatekeeper function

There are various bodies which fulfil a gatekeeper function in the economic system. These are financial service providers and their regulators (such as banks, AFM or the Dutch Central Bank, accountants), legal service providers (civil-law notaries, lawyers) and public administration if licences have to be issued. These parties arrange and monitor the access to certain services and provisions which are crucially important for the functioning of market parties.

In recent years various initiatives have been taken to reinforce the gatekeeper function with regard to the service providers in order to restore the balance between facilitating and verifying by service providers.

Whistle-blowers

Whistle-blowers can play an important role in exposing criminal activities. For that reason increasing attention has been paid in recent years to protecting whistle-blowers. This has resulted in the 'House for Whistle-blowers' Act which came into effect on 1 July 2016. This law regulates the possibilities and protection of employees who want to report wrongdoing.

Cooperation and information exchange

Finally, cooperation and information exchange is an important capacity for the bodies involved. A multitude of (structural) partnerships exist with a view to jointly addressing fraud, misuse and organised crime. One example is the structural link created between public administration, the police, the Tax and Customs Administration and the public prosecutor's office in the so-called RIEC/LIEC structure.[16]

10.4.3 Scenario variants

As already mentioned, the existing NRB scenarios are used as a basis.

Scenario variant 1. Criminal subversion of critical business

This scenario is included in NRB 2008/2009. The basis and context for the scenario at the time comprised activities by (Russian) oligarchs or tycoons that set up companies (abroad) as a cover for industrial espionage and money-laundering practices. One of the methods they used was to invest their money via hedge funds and private equity funds.

Summary of scenario line

In a foreign state (named Churitia) the political leader decided to target, among others, tycoons who had invested their (suspect) financial reserves via private equity funds and hedge funds in international companies, including Dutch ones. Due to various interests of the tycoons and the Churitian government pressure was increased on the network in which there used to be a large degree of interconnectedness between government and tycoons.

Research reveals that the suspects used illicitly gained money to buy stakes in hedge funds and private equity funds. Eventually majority interests were purchased in international companies and companies were also purchased. The suspects appear to include owners of majority interests (51%) in the Dutch power and oil companies (Koninklijke Easy Electronic and GasOil.Com) and the largest Dutch bank (the Lions Bank).

This information comes out and leads to demonstrations in The Hague against the interference of dubious investors in the Dutch economy. Although the government shares the concerns, it cannot do very much about it and takes the position that takeovers by foreign investors are part of our free market economy. The (diplomatic) relationships between the Netherlands and Churitia deteriorate.

[16] Regional Information and Expertise Centres [Regionale Informatie en Expertise Centra] (RIECs) and National Information and Expertise Centre [Landelijk Informatie en Expertise Centrum] (LIEC).

Table 10.4 Impact scores for the Criminal subversion of critical business scenario.

Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.			◉				The possibility of foreign, criminal concerns being active in the Netherlands is considered likely, but that these enterprises subsequently end up in state hands is considered unlikely.
Impact assessment							
Security interest	**Criterion**	**Limited**	**Substantial**	**Serious**	**Very serious**	**Catastrophic**	**Explanation**
Territorial	Territory						Not applicable.
	International position			◉			It primarily concerns political (embassies) and non-political relations between both countries which have come under pressure.
Physical	Fatalities	○					Is possible, but limited.
	Seriously injured and chronically ill people	○					Is possible, but limited.
	A lack of life's basic necessities						Not applicable.
Economic	Costs				○		The fact that Dutch interests end up in foreign hands is, in itself, not a problem. However it does cause damage if companies also actually leave / are tempted away from the Netherlands. On this basis the estimated damage is between 5 and 50 billion euros.
	Violation of vitality			○			Confidence in the economy is damaged, in which the assumptions that this will lead to a 1.2% slowdown. Unemployment (also among multinationals) increases by 0.3%. This represents approximately 30,000 people. It has been calculated that the debt ratio increases by approximately 1.6%. Finally, the value of the sector is included.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life	○					A limited impact is assumed due to, for example, demonstrations.
	Violation of constitutional democratic system			◉			A substantial part of the population distrusts official bodies (politicians, public administration, judicial system). In addition, demonstrations undermine day-to-day life.
	Societal impact			◉			There is broad resentment aimed at the 'economic elite'.

◉ average to considerable uncertainty; ○ minor uncertainty

The Churitian government takes action against the tycoons on the basis of their legal investigations and reports that the Churitian state is taking over the Churitian interests in Dutch companies. This means that the Dutch companies in question actually end up in the hands of the Churitian government. As a result, three Dutch multinationals lose land and other possessions with a total value of 750 million euros.

Scenario variant 2. Criminal foreign concern

This scenario is included in the NRB6. The scenario has been written to focus more attention on the effect of large-scale fraud and (cross-border) crime on national security. The scenario is inspired by the situation in the Middle East where conflicts and political upheaval have led to the release of large quantities of flight capital. Another tendency, on which this scenario is based, is the increasing subversion of mainstream commercial activities by cross-border criminal organisations.

Scenario line

Coralart, an investment holding company with its head office in Dubai, has, in a short space of time, developed into a major player on the Dutch market. The planned investments for the first ten years amount to twelve billion euros and include activities such as prestigious construction projects (such as a football stadium), joint ventures in the transport sector and logistics (in, for example, the Port of Rotterdam), and expansion into financial services. The company is initially very successful and also has a very strong reputation due to lobbying and media activities, injections into the Dutch economy and a series of investments in social projects in deprived areas. As a result it has become very popular among the general public and (local) politicians. The various business units also appear to comply with Dutch employment and business regulations, as shown by several (partially unannounced) inspections by various Dutch supervisory bodies such as the FIOD, FIU-the Netherlands, DNB and the AFM.

Two years after it was established in the Netherlands, however, the first cracks start to appear in the company's carefully constructed image. One of Coralart's logistical joint ventures was found guilty of regularly transporting drugs. This leads to more inspections and investigations. Despite the slow progress made and considerable political hindrance, a number of unlawful activities are eventually uncovered, ranging from criminal activities (trading in drugs, weapons and counterfeit products and human trafficking), the payment of bribes and large-scale parallel accounting to systematic money-laundering. Coralart is exposed and the empire collapses. The company turns out to have been set up as a vehicle for stolen goods from collapsed Arabic regimes. The formal management structure appears to have been completely infiltrated by criminal elements.

The collapse of Coralart leads to the loss of 20,000 jobs (of which half can be saved). The company's Dutch activities, with a turnover of 5 billion euros per year, are terminated. The same applies to the annual influx of 30 billion euros via the concern's financial division. In addition, numerous charity activities are cancelled and major construction projects are suspended. The downfall of Coralart also leads to considerable division and tense relationships within Dutch society and the political establishment. It transpires that there was a high degree of cooperation between leading politicians (including ministers), business people and the company's lobbyists. Some of these were aware of Coralart's criminal activities. All this eventually leads to the resignation of several ministers and political leaders. At the same time the loss of jobs and the suspension of the charity work causes anger in certain deprived neighbourhoods. This results in protests and vandalism. A great deal of friction is created between the established liberal media and local communities. Populist politicians who run campaigns promising to clean up the government rapidly gain support. On top of this nine people lose their lives due to criminal vendettas which occurred due to the termination of Coralart's illegal activities. Finally, new laws and control measures for foreign investment initially result in a decline in foreign investment.

Impact

The damage goes further than just economic damage. Due to the close ties that the criminal concern has with politicians and authorities, in addition to the services it provides to wider society, the unmasking and collapse of Coralart results in political instability and social unrest.

The following table shows the scores on the impact criteria.

Table 10.5 Criminal foreign concern impact score.

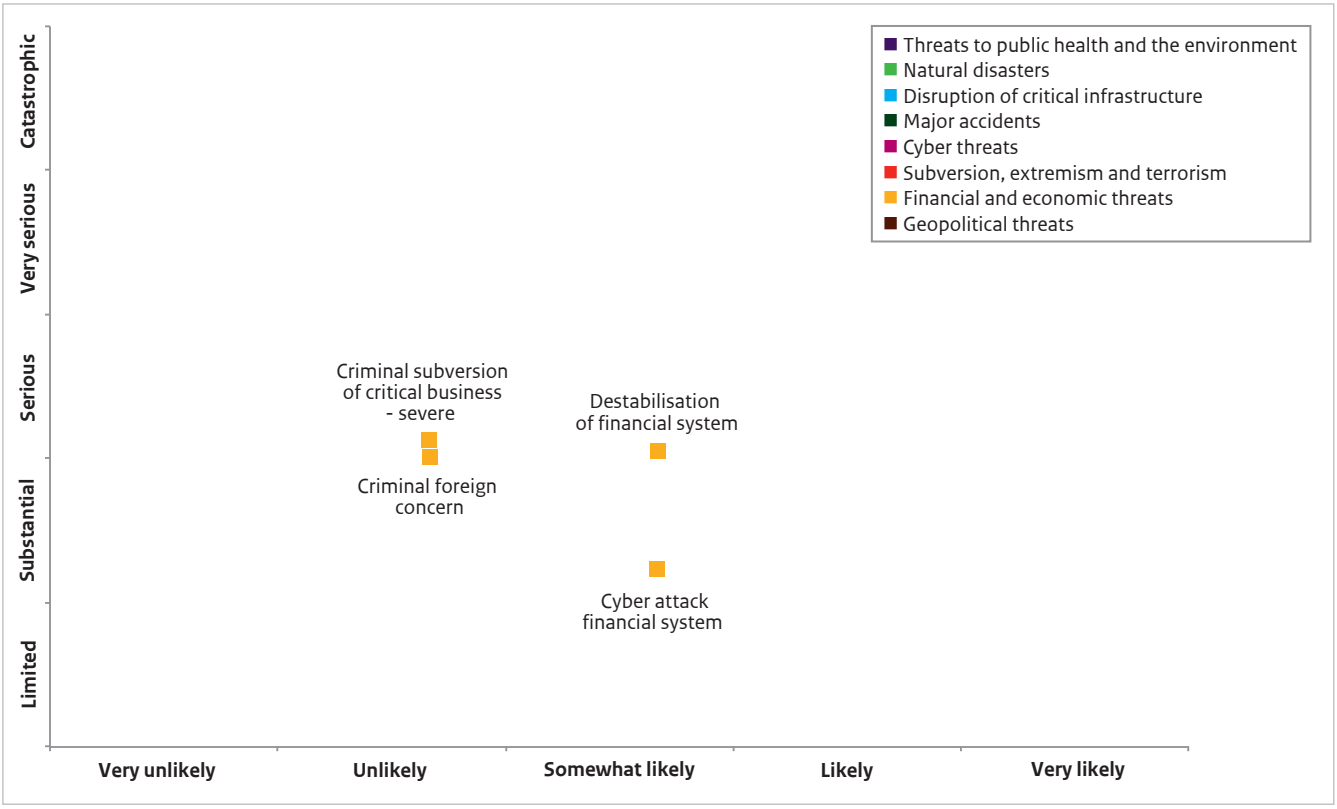
Likelihood assessment							
		Very unlikely	Unlikely	Somewhat likely	Likely	Very likely	Explanation
Likelihood of the scenario occurring between now and 5 years.			○				In the scenario the focus is on a lack of integrity up to ministerial level. That is considered unlikely.
Impact assessment							
Security interest	**Criterion**	Limited	Substantial	Serious	Very serious	Catastrophic	**Explanation**
Territorial	Territory						Not applicable.
	International position	○					
Physical	Fatalities	◎					A small number of fatalities as a consequence of criminal vendettas.
	Seriously injured and chronically ill people		○				As a consequence of stress, unrest, increase in drug use.
	A lack of life's basic necessities						Not applicable.
Economic	Costs				◎		The scenario shows that a total of 65 billion may be withdrawn. However, the question is whether it is possible to force criminal investors to sell their assets. For that reason a lower amount is assumed (< 50 billion).
	Violation of vitality	◎					This means 10,000 unemployed while the debt ratio is scarcely compromised.
Ecological	Violation of nature and the environment						Not applicable.
Socio-political	Disruption to daily life		○				Some of the people who end up unemployed will, to a limited degree, be less able to participate in social activities.
	Violation of constitutional democratic system			○			For example in the form of 'contamination' of officials, conflicts of interests in political decision-making and public administration, failure of the system.
	Societal impact			○			Broad social anger and resentment; also aimed at the elite.

○ average to considerable uncertainty; ◎ minor uncertainty

10.5 Conclusion and considerations

We have included the risk diagram of the current scenarios in this paragraph. The figure shows that the impact is estimated as not been that great, while the consequences of the scenario variants are primarily evident in the context of economic security and social political stability. However, it is clear that the probability of destabilisation occurring and a cyber attack in the financial system are both considered 'somewhat likely'.

Figure 10.1 Financial-economic threats risk diagram.



11 Autonomous developments

Autonomous developments mean processes and trends which, in themselves, are not a direct threat for national security, but which can have an influence on certain risks and threats. The term 'autonomous' indicates that this means developments which lie outside the sphere of influence of an organisation or government and which will occur irrespective of the risk management choices which individual organisations of authorities make. Autonomous developments are viewed from the broader, temporal (medium to long term) and geographical (global versus national) perspective than the individual themes and risk categories.
The systematic analysis of autonomous developments is part of the methodological approach of the NRP. The analysis provides an insight into the possible influence of these developments on the risks in the individual themes and risk categories, and can also help to identify new and emerging risks or mutual links between the various risks and threats.

The systematic analysis of trends and (autonomous) developments enables us to identify changes in existing risks and emerging risks on time.

In the NRP we distinguish between five categories of autonomous developments[17]:
- Ecological developments
- Demographic-societal developments
- International-political developments
- International-economic developments
- Technological developments.

[17] Many foresight studies are based on DESTEP, a classification into six categories of factors: demographic, economic, socio-cultural, technological, ecological and political-legal. These factors often relate to driving forces (not to trends and processes) without there being any international dimension. For that reason a slightly different classification has been chosen in the NRP.

In this chapter we discuss the most important developments per category in general terms and, insofar as important, the influence on the individual themes and risk categories. The observations also include any correlation between the various developments and their significance for our national security.
The most important findings of this chapter, also with regard to new (emerging) risks and the possible consequences thereof for national security, are discussed in Chapter 12.

11.1 Ecological developments

The most important ecological developments are *climate change, loss of biodiversity* and *increasing environmental pressure*.

The **climate is changing** because more and more greenhouse gases such as CO_2 and methane are being released into the air, as a consequence of the burning of fossil fuels (for energy and transport) and deforestation. As a result the temperature of the earth is increasing – and therefore sea levels as well – and there is a greater chance of extreme weather. The direct consequences of climate change for the risk in the Netherlands of floods, more extreme weather (more serious rainfall, storms and heatwaves), wildfires, (infectious) diseases and the environment are discussed in the *Natural disasters* and *Threats to health and the environment* themes.

The consequences of climate change also affect the critical infrastructure. On the one hand natural disasters and large-scale epidemics can lead to serious disruption to the critical processes, as shown by the impact assessment in the *Disruption to critical infrastructure* theme. On the other hand, measures to combat the consequences of climate change increase the risk of disruption. That applies primarily to power supplies (on which other critical processes are then dependent):

the transition to more sustainable sources of energy makes it more complex to control the network and can lead to an increase in technical disruptions. The more frequent occurrence of extreme weather, such as serious flooding due to heavy rainfall, has the same effect.
In our country a climate adaptation strategy is used to work on several fronts to optimise management of the consequences of climate change.

Globally, the effects of climate change are expected to be greater, meaning, for example, an increase in the number and the size of floods in densely populated coastal areas and river deltas, a greater possibility of forest fires, the expansion of desert areas and acidification of the oceans. A consequence of this will be more frequent shortages of food and (drinking) water in drier areas, leading to hunger, malnourishment and an increasing chance of diseases and epidemics. Although these effects will primarily be felt by countries which do not have enough money or technology to adapt to climate change, more prosperous countries may also be faced by this increasing risk.
Indirectly these phenomena can lead to an increase in migration (the consequences of migration are discussed in the next paragraph), conflicts between groups and countries, and claims to raw materials and life's basic necessities, such as food and clean water. They will therefore constitute a threat to our national security in the longer term. It is currently impossible to predict when this threat will occur and on what scale. One thing that is certain, however, is that climate change is regarded as one of the largest Global Risks[18].

Climate change can have all kinds of consequences. It influences a wide range of themes, varying from natural disasters to social and economic shifts.

This is something the international community is now fully aware of. In the Paris Agreement on climate change 195 countries made binding agreements to reduce greenhouse gas emissions (taking account of the differences between countries), so that the average temperature on earth does not increase by more than 2°C. However, even if this goal is achieved, the consequences of climate change in the coming decades will not directly decline and constant attention will have to be paid to monitoring these developments and to mitigation.

Besides the Paris Agreement, the Sendai framework[19] is also an international process designed to reduce risks of major disasters (prevent and limit consequences). Although this process relates to all kinds of disasters, the emphasis is on natural disasters and, in that respect, the relationship between climate change and natural disasters plays a key role.

With a view to reducing the consequences of climate change, research has been carried out into the techniques for removing the greenhouse gas CO_2 from the atmosphere and oceans or reversing the temperature increase in some other way. These techniques are referred to as **geo-engineering**. Although this research is still at a pioneering stage, techniques for influencing the weather are already being applied on a small scale. There is some doubt about the feasibility of using geo-engineering on a large scale and whether the benefits justify the possible, as yet uncertain negative effects.

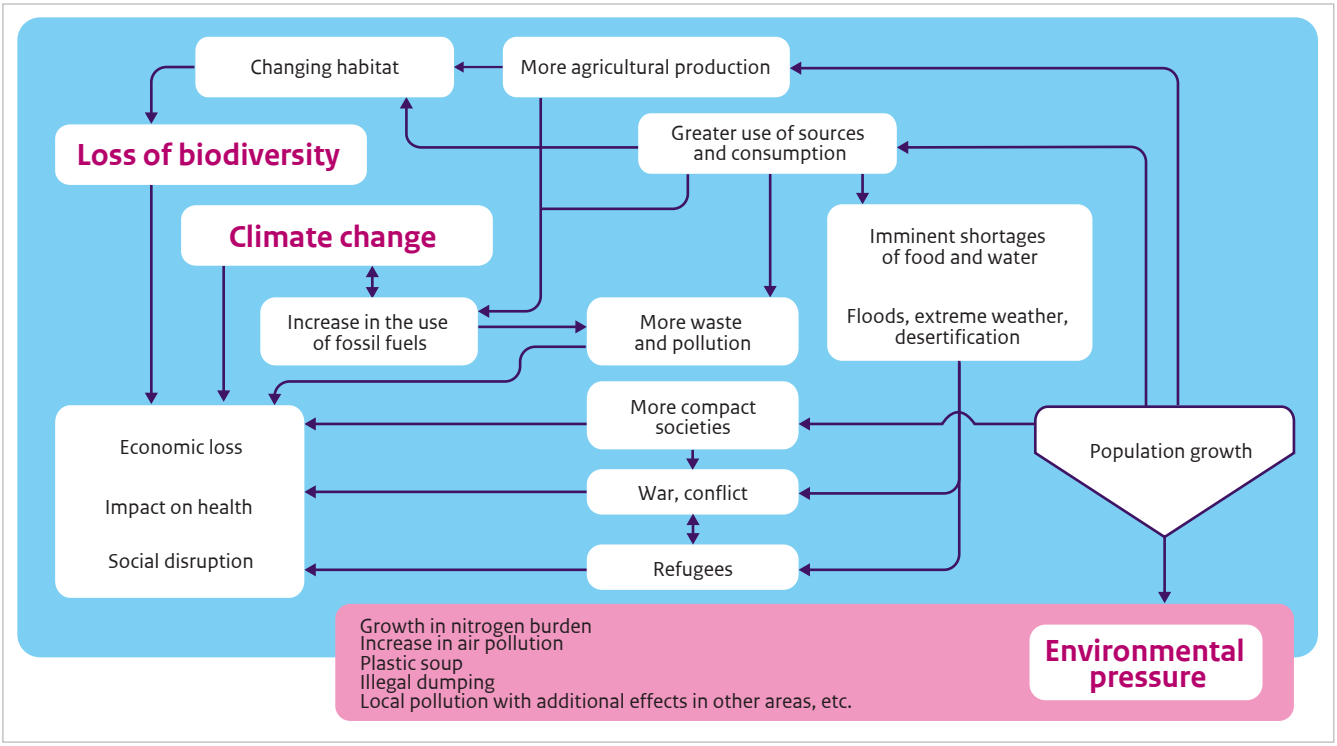
Climate change also leads to **a loss of biodiversity**. There are, however, other contributing phenomena such as intensive land use, environmental pollution, the nitrogen burden and fragmentation of ecosystems. Biodiversity is defined as: the number of different species of animals and plants. Biodiversity is important. For example, species and ecosystems are responsible for the production of oxygen, the decomposition of dead animals and plants, pollination of plants, water purification and the management of plagues. As far as humans are concerned, biodiversity means food, fuel (wood) and raw materials for clothing and medicines. Scientific research on biodiversity also regularly leads to technological innovation and greater well-being.
In comparison to Europe and the rest of the world the Netherlands have a low biodiversity (estimated at approximately 15%, compared to 70% on a global scale), caused by intensive agriculture, the nitrogen burden and urbanisation[20]. In the Netherlands it is primarily the diversity of heathland, dunes and agricultural areas which is declining while globally the loss primarily has to do with forests, grasslands and savannahs. Although low biodiversity does not constitute a direct threat to our national security in the sense of a destabilising disaster or crisis, it does represent an insidious violation of the ecological security, one of the five national security interests.

[18] World Economic Forum, Global Risks 2016, and other reports on global risks.

[19] The Sendai Framework 2015-2030 was launched during the UN conference on Disaster Risk Reduction in Sendai, Japan, on 18 March 2015. It describes seven goals and four priorities for action to reduce disaster risks.

[20] A biodiversity of 15% means that the populations of plant and animal species have an average size which is 15% of the original natural situation.

Figure 11.1 Diagram of the links and correlation between various ecological developments and consequences at global level.



The loss of biodiversity is closely related to **environmental pressure**. The environmental pressure increases along with the global population because people will consume more and use fewer efficient technologies[21]. In a practical sense it means contamination (the existence of substances in the soil, water and air which are harmful for humans or ecosystems) and the depletion of natural resources. Another term that is used is the ecological footprint[22].
In the Netherlands the environmental pressure has decreased in recent decades due to the intensive emissions reduction policy and promoting sustainability, and is no longer linked to economic growth. Nevertheless, problems still exist as described under the theme of *Threats to health and the environment* (including the disease burden due to exposure to particular matter and nitrogen dioxide in the air).
Global environmental pressure is increasing due to the growth of the world population and prosperity and the related increasing demand for water, fertile land and raw materials. That increase is evident in among other things:

- An increase in the nitrogen burden, which leads to a decrease in biodiversity.
- Increasing air pollution in large cities, primarily in non-Western countries. The incineration of residual waste from deforestation.
- Large-scale contamination of the oceans with plastic waste (the 'plastic soup'). In addition the decomposition of the plastic into small particles and the leaching of harmful substances constitutes a threat for the aquatic environment, flora and fauna and, in the long run, food provision (see also the *Threats to health and the environment* theme).
- The illegal dumping of (chemical and electronic) waste. This results not only in environmental pollution but also constitutes a health hazard in countries where people who live near waste dumps extract raw materials from the waste without any protection.

For the time being these problems are having almost no effect on the Netherlands but may – just as in the case of climate change – indirectly represent a threat to our national security in the long term.

Figure 11.1 is a general portrayal of the correlation between the various ecological developments and their consequences for people, society, nature and the environment at a global level. We wish to emphasise that this is a simplified portrayal of what are, in reality, complex relationships and effects.

[21] Derived from the definition of environmental pressure according to Ehrlich.

[22] The ecological footprint is the space needed for the production of everything we use and the absorption of the CO_2 which we emit, converted into the surface area of productive land.

11.2 Demographic-societal developments

In this category we consider, on the one hand, demographic developments (meaning the size, composition and distribution of the population) and, on the other hand, changes in the socio-cultural domain such as norms, values and attitudes.

Important demographic developments for our country in the coming decades are *ageing*, and other changes in the demographics, the *widening gap between population groups* and *urbanisation*.

According to the current prognosis, the population is set to grow by well over 1 million people between now and 2040. However, growth may be even higher, or indeed lower (a shrinking population at national level is conceivable), under the influence of socio-cultural changes and the development of net migration. One thing that is certain is that the population is ageing. The number of elderly people is set to double by 2040. This **ageing** is having major consequences for healthcare, the availability of all kinds of provisions, the employment market and the economy, but does not represent a threat for national security.

Ageing is not the only change in the composition of the population. Migration can lead to changes in the socio-cultural, ethnic and religious composition. Inequality between, for example, people with a high level or low level of education is also growing and these groups appear to be living more and more in separate worlds. The **widening gap between population groups** in the areas of income, health, employment opportunities, well-being and socio-cultural views and the possible (new) split which is emerging in society may have a detrimental effect on social cohesion and people's confidence in the government and social institutions.

A different development is urbanisation. The population, economy and prosperity are growing in the Randstad conurbation and several other urban areas, but shrinking in other areas. This is leading to pressure on the available space in urban areas which, in itself, is having consequences as regards the impact of floods and extreme weather incidents (see the *Natural disasters* theme) and the environmental pressure in these areas. At a global level the consequences of urbanisation due to population growth and increasing prosperity are having a greater impact which is being translated into increasing environmental pressure and an increasing need for raw materials, power, food and clean water, which is largely comparable with the effects described in paragraph 11.1.

Changes in the socio-cultural domain relate to individualisation (and the focus on individual interests), the decreasing confidence in the government and the authority of science and institutions, the increasing feeling of 'great discontent', the growing segregation, the network society, the increasing information pressure, the influence of social media, the pressure on the welfare state and the increasing polarisation between various population groups in the religious, ethnic, social and political fields. Insofar as they constitute a threat to national security the consequences of these developments have been analysed and defined under the *Subversion, extremism and terrorism* theme.

Although the phenomenon of **migration** is nothing new, it deserves particular attention due to the current and expected global developments and the correlation with various NRP themes and other autonomous developments.
As a consequence of wars, destabilisation (primarily in the Middle East and North Africa), increasing poverty, population growth and climate change, migration to Europe is expected to increase in the coming years. The significantly increased migration flow since the second half of 2015 is now leading to humanitarian crises, problems with care, integration and social cohesion in various countries and pressure on the stability of the European Union.
Large numbers of migrants from non-European countries may place even more pressure on society. If the influx of refugees exceeds our society's capacity to absorb, various national security interests may be compromised to a degree which is anything between substantial and serious. This applies primarily to social and political stability (due to differences in interpretations about social and statutory norms and values, manifestations of discrimination and xenophobia, increasing polarisation, decreasing solidarity and social cohesion, unrest and feelings of insecurity, the breakdown of social support for refugee care) and the international position of the Netherlands. Incidents (riots and breaches of the peace) may occur at local level and can cause situations which are unacceptable from a humanitarian point of view, as in the case of the Calais Jungle unofficial refugee camp. If the capacity to absorb is exceeded, there will be a risk of the number of illegal immigrants growing, as well as exploitation, exclusion from the employment market and crime. Consequences are conceivable on a limited scale for the healthcare system and the environment (in the sense of increased pressure on space). The consequences of increasing migration also feature in the *Subversion, extremism and terrorism* theme.

11.3 International-political developments

In the last few years a shift has been observed from a multilateral to a multipolar world order[23] and the expectation is that this process will continue during the coming years. The shift is accompanied by increasing fragmentation within the international system, more difficult relationships between great powers and other emerging countries, and a growth in tensions and (the threat of) conflicts in the world. The result is considerable pressure on the global and regional conflict management capacity. The use of geopolitical instruments such as the traditional battle to manage territory and seas, the defining of borders and spheres of influence and the power struggle for (scarce) raw materials appear to be increasing. On the other hand the increasingly strong mutual dependency between countries means there is a considerable demand and need for international cooperation. That cooperation is necessary in order to cope with complex global challenges such as the climate problem and the fight against crime, and to get a grip on the global financial system and technological developments. There are, for example, increasing demands at international level to curtail the development of autonomous weapons systems.

The most important international-political developments which may threaten our national security are *a shifting balance of power, increasing tensions between* great powers, *increasing regional instability* and a *stronger connectedness of internal and external security*. An increase in *hybrid* conflicts has also been observed.

The multipolar world order is characterised by **a shifting balance of power** and by **increasing tensions** *between great powers*. In the past decades a shift in power has taken place, with a reduction in the dominance of the West. What is more, the relationship between the US and the EU has worsened and the EU appears to be gripped by a crisis of confidence. At the same time China, Russia and a number of smaller, emerging powers are adopting the position of 'revisionist powers' that have no desire to conform to the status quo and whose primary objective is to strengthen their own position and not to promote democracy, a liberal system and (political) human rights.

China is focusing primarily on economic expansion and on boosting its influence, primarily in the non-Western world, by supporting economic development and promoting itself as a partner in the resistance to Western dominance (soft power instruments). Other emerging countries such as India, Brazil and Turkey are displaying more or less similar 'revisionist' behaviour, although their power and influence is considerably smaller than that of China. Russia has adopted a more geopolitical strategy through the annexation of the territory, and the intimidation, of countries of the former Soviet Union, limited economic sanctions (in response to sanctions by the EU) and the use of aggressive language, but is also facing a worsened economic position and the related risk of internal instability.
The US is having to deal with internal problems, such as the widening gap between population groups and the increasing distance between political and ideological groups, and the lessening of its influence in the world. Within the EU there is increasing division between countries on a number of issues and declining support for the EU among sections of the population in various member states. There are various reasons for this, namely fear of external threats, disagreement between member states with regard to how to tackle the refugee problem, considerable financial problems of a number of member states, resentment of government interference and 'the influence of Brussels' among citizens and increasing of nationalistic sentiments. Divisions mean that the EU is unable to adopt a tough stance on the world stage. As a result, the influence of the Netherlands in the world is also declining.

Along with these developments, multilateral economic and security organisations such as the United Nations (UN) and the Organisation for Security and Co-operation in Europe (OSCE) are finding it more difficult to function. It would appear to be the case that the prevention of conflicts and securing security policy interests are being based more on agreements intended to leave each other 'alone' and that cooperation is taking place more frequently on an ad-hoc basis and in the form of casual coalitions and bilateral and trilateral agreements. The risk of a lack of international cooperation and coordination is that malicious actors can operate more easily and anonymously and that certain threats are detected (too) late.
The direct effects of these developments on our national security interests are described in more detail in the *Geopolitical threats* theme and – where they concern subversion by state actors – the *Subversion, extremism and terrorism* theme.

[23] The multilateral and multipolar world order are two types of global scenarios of the international system which are the result of Armed Forces forecasting ('Forecasting; a guideline for the Armed Forces of the future [Verkenningen; houvast voor de krijgsmacht van de toekomst], Ministry of Defence, 2010). The two other global scenarios generated by this forecasting are the network and the fragmentation scenarios.

The shift to a multipolar world order is also characterised by **increasing regional instability**.
The great powers are sometimes directly or indirectly involved, but this is not always the case.
Parts of sub-Saharan Africa and West Africa, the Horn of Africa as well as Pakistan and Afghanistan are dominated by instability and internal conflicts. In the MENA region countries are facing the threat of falling apart due to religious and political sectarianism. There are areas where radical groups can set up bases without any opposition. Some countries in Central America are facing problems relating to fragility and crime.

The situation in Africa and the MENA region, located on the south flank of the EU, constitutes a threat for the EU and therefore the Netherlands. The growth in population and (the threat of) shortages of food and water, as well as instability and conflicts in many countries – of which some can be characterised as failing states – are exacerbating the migration flow to countries in the EU. The expectation is that the number of migrants is more likely to increase than decrease in the coming years. The possible effects of this on the Netherlands are described in the previous paragraph (*Demographic-social developments*). Another threat which is a consequence of the instability in Africa and the MENA region is that of increased terrorism and jihadism. The significance of this for our national security is detailed in the *Subversion, extremism and terrorism* theme.

The threat of terrorism has also become more complex due to the **stronger connectedness between internal and external security**, that is, between threats from within Dutch society and from abroad. For example, the presence in EU countries and in the US of population groups that have their roots in the MENA region is increasing the risk of manifestations of radicalisation and terrorism. The most vivid example is the rapid emergence of Islamic State (IS), which is not only destabilising the Middle East but is also creating dangers and risks in the West. This development has been, and is being, fuelled by the interference of the West in conflicts in the MENA region and surrounding countries, which is also increasing the negative attitude towards the West. Another risk takes the form of tensions between population groups in the Netherlands as a consequence of conflicts in their home country, for example between Kurds and Turks.

On the eastern border of the EU, the annexation of the Crimean Peninsula, the war in Ukraine and the intimidation by Russia, for example in eastern Europe, have resulted in tense relations between Russia and the West, and that situation is unlikely to change for the time being. Russia is also using various resources which can be characterised as a **hybrid threat**[24]. In response to this the West has imposed economic sanctions and NATO has increased its presence in, for example, Poland and the Baltic states.
The chapter on *Geopolitical threats* details the possible consequences of these tensions in a scenario with effects on the Netherlands. Activities which are used in hybrid conflicts are part of a scenario in the *Subversion, extremism and terrorism* theme.

All developments considered, the risk of 'the major conflict' – an armed confrontation between the great powers or a global threat of conflict as was the case during the Cold War – is small, but the risk posed by the effects of regional conflicts, including that of terrorism, is substantial. This situation is expected to stay that way for the coming years.

11.4 International-economic developments

A number of social and geopolitical economic developments do not (yet) constitute, in themselves, a threat, but they may affect national security in the long run.

For example, during the last few years increasing attention has been paid to the growing global **economic inequality**, including in the Netherlands. In 2014 the Netherlands Scientific Council for Government Policy [Wetenschappelijke Raad voor Regeringsbeleid] published a report of an investigation into the extent and consequences of economic inequality for the Netherlands.[25] The report states that the degree of inequality depends on the criterion used to measure it. Based on Gini coefficients, which is an inequality criterion commonly used at international level, it can be asserted that the Netherlands are now in a period of stabilisation following an increase in income inequality in the Nineteen Eighties. However, an assessment of the average of the highest and lowest 10% of incomes undeniably reveals increasing income inequality with the poor getting poorer and the rich getting richer.

[24] The term 'hybrid threats' means the integrated use of conventional and unconventional means, open and covert activities and the use of military, paramilitary and civil actors and resources to create ambiguity and exploit an opponent's vulnerabilities in order to achieve geopolitical and strategic goals. The use of manipulated information and deception are important aspects of hybrid tactics. Hybrid threats can largely occur under the warfare threshold.

[25] Monique Kremer, Mark Bovens, Erik Schrijvers, Robert Went (ed.), *How unequal is the Netherlands? A survey of the development and the consequences of economic inequality* [Hoe ongelijk is Nederland? *Een verkenning van de ontwikkeling en de gevolgen van economische ongelijkheid*]. The Hague: Wetenschappelijke Raad voor het Regeringsbeleid, 2014.

With regard to capital the divisions are even greater (just as in most other countries), with the 10% wealthiest people in the Netherlands owning more than half the country's assets. From an international perspective this is on the high side.

A high degree of economic inequality (and therefore not the absolute income) has all kinds of possible social, political and economic consequences, as revealed by the WRR survey. A high degree of income inequality is linked to less social mobility, declining solidarity between citizens and a loss of confidence in the rule of law and the parliament. A high degree of income inequality can also slow down economic growth in the Netherlands. However, these effects are not so great that they represent a direct threat to national security.

The continuing **relatively high unemployment** and the pressure on the lower end of the employment market may constitute a problem. In the years ahead the CPB expects a slight decrease in the unemployment, but levels are not expected to drop to below 5% (CPB, MLT 2018-2021). What is more, continued **automation and robotisation** will have consequences for the employment market because they may lead to jobs being lost at the lower end of the employment market. At the same time these developments may cause employment-related changes. Developments such as ageing, the influx of workers from Southern and Eastern Europe and the flow of migrants will all have an influence on employment.

Another development concerns the **low interest rate**. Interest rates have already been going down for decades and the CPB expects them to remain low for a long time yet. The main underlying cause is said to be the mediocre economic situation with the most important driver of the decrease being ageing (and not the policy of the European Central Bank). Low interest rates are having major consequences for the Netherlands' financial-economic situation. Positive and negative consequences will occur, as described in more detail in the theme Chapter entitled *Financial-economic threats*.

The *shifting balance of power* and *tensions between great powers* discussed under *Geopolitical developments* also have consequences at a financial-economic level. A **shift in economic and political influence** is taking place at global level to the detriment of the West and in favour of a large group of non-Western countries, headed by China and India. As a result the West, and therefore the Netherlands, has less international influence and, at the same time, pressure is being brought to bear on Western standards and values.

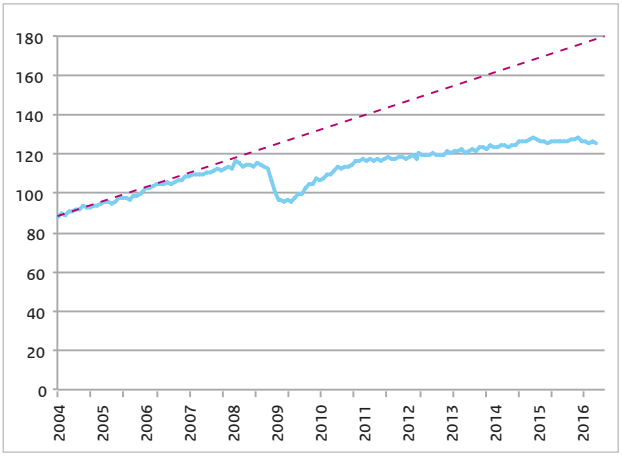
In this context of geopolitical developments we are seeing an increase in the use of economic influence as political leverage, either directly via sanctions or indirectly via threats. In the past ten years there has been a significant increase, at international level, in the use of (the threat of) **economic sanctions**. One example is the aforementioned use of economic sanctions by the EU against Russia and the ensuing economic response by Russia. The expectation is that economic sanctions will be used more often in the future, for example China may also use economic pressure as a political tool. As an open economy and democratic society the Netherlands are relatively vulnerable to such foreign economic pressure, even if it takes place indirectly, for example in the form of sanctions between the US and China.
We are also witnessing the increasing use of s**trategic economic policy** by other states. These conduct activities to disrupt competition which are aimed at securing and protecting national economic interests, such as the provision of state support, the purchasing of raw materials and engaging in economic espionage. Account also has to be taken of an increase in protectionist measures. According to the *Global Trade Alert* more than 6,000 protectionist measures have been taken since 2008, with India, Russia, the US, Argentina and Brazil being the top 5 countries to do so. The countries most affected are China, the EU member states and the US.

As an open trading nation the Netherlands are very dependent on the unrestricted functioning of world trade. The increase in protectionism is expected to have a disproportionally severe effect on the Netherlands, all the more so given that, at an economic level, the Netherlands will (have to) cooperate more and more with countries where the state traditionally has a strong role. For example, according to an estimation using the CPB SAFFIER II model a 1 percent decrease in the growth rate of world trade will lead to a 0.2 percentage point drop in Dutch GDP.

Although the economy initially appeared to be recovering following the financial crisis, a slowdown in world trade appears to have been taking place since 2011 (see Figure 11.1). Moreover, the difference with the trend-based growth which was expected before the drop in world trade is increasing all the time.

Given the shifting balance of power process, our country has less capacity to improve standards which might limit the market-distorting actions of other states. The OECD may, for example, start to play a less coordinating role when it comes to mitigating protectionist measures because the emerging powers are not members. The emerging economies are opting more and more frequently for alternative forms of cooperation.

Figure 11.2 World trade (index figures)*



*CPB World Trade Monitor

A final issue is **globalisation** and the increasing concentration (centralisation) of international-economic developments within certain sectors. This is leading to an interconnectedness of systems and increasing complexity. In addition, the concentration of production in, for example, the food sector or of the production of medicines and vaccines is causing a great dependency on a limited number of actors.

11.5 Technological developments

The fact that we now find it almost impossible to imagine life without the computer illustrates the immense impact of the introduction of this technology on our daily life. Although it is clear that technology can cause drastic changes in society, the effects of specific technologies are still very difficult to predict. New technologies offer opportunities to promote prosperity, the economy, health and security and to strengthen capabilities, but may also imply new risks and threats. These risks can be predicted to a certain extent. However, the complexity, unverifiability and speed of development means there will also be unforeseen effects, of which the impact is a *priori* difficult to assess. It is precisely due to these uncertainties that it is important to focus on technological developments and therefore a wide range of technology surveys are being carried out and reports drawn up regarding the latest promising technological advances, or the greatest technological risks.

The National Security Technology Survey [Technologieverkenning Nationale Veiligheid] (2014)[26] describes five technology areas and the applications, developments, opportunities and risks within each of those areas in the coming years: nanotechnology, biotechnology and gene technology, neurotechnology, materials technology and information technology. What is more, developments are taking place on the interfaces between these areas of technology which may lead to unexpected innovations, referred to as converging technologies. Although it is useful to examine the developments within and between specific areas of technology, it continues to be difficult to predict which technologies are actually going to make a difference and where potential risks to national security may arise. Consequently, a summary or overview of all important technological developments is almost never exhaustive and is, to a certain extent, selective. Nevertheless, in order to identify the possible impact of technological developments on the various national security interests we have opted not to discuss a number of developments or trends within specific areas of technology, but instead to examine a number of more general aspects which help to define the impact of technology on various national security interests. These aspects are driven and stimulated by technology and are all applicable to several areas of technology, but cannot be fully linked to one or more specific technologies.
The aspects which we discuss in this paragraph are: *manageability, dual-use technologies, availability and easy accessibility of technological innovations, connectedness and dependency of systems, big data and the increasing intelligence of systems.*

It still appears to be difficult for governments to supervise or influence (technological) innovations. Innovations can set social transitions in motion which are **difficult to control**. For example, innovations may outgrow the traditional roles in society and create new flows of funds. Two current examples of such innovations, the two digital platforms, Airbnb and taxi service Uber, prove that these developments do not have to be highly technological. A feature of these companies is that they link users (digitally) to enable them to exchange services (so-called peer-to-peer transactions). With their innovative business models they are putting pressure on traditional providers of comparable services. Both services are extremely popular, but the authorities are struggling to impose suitable regulations. On the one hand the government is

[26] Van Vliet, H. and Mennen, M. (eds). (2014) National Security Technology Survey. An exploration of opportunities and threats of technological developments for national security [Technologieverkenning Nationale Veiligheid. Een verkenning van kansen en dreigingen van technologische ontwikkelingen voor de nationale veiligheid]. The National Network of Safety and Security Analysts.

aware of the need for future-proof legislation and regulations while, on the other hand, rules can also have a delaying or hindering effect on innovations and can quickly become obsolete.

Dual-use technologies are technologies which have both a peaceful and military application, for example, certain chemicals which are used in the chemical industry can also be used as raw materials for chemical weapons. They have a military use, but can also be misused by malicious actors. Not only are these technologies in themselves a risk (due to the possibility of misuse or incorrect use), the lack of appropriate legislation and regulations to prevent misuse adequately can constitute a problem, with one example being drone technology. Although drones are used in a military context, small and affordable consumer versions are already available on the market. The risk of these drones for air traffic is currently being investigated by the European Aviation Safety Agency. This technology can also constitute a new risk with regard to protecting VIPs. Drones (which are readily available) could be equipped with weapons and even cameras with face recognition in order to select the target.
A related development is the emergence of the phenomenon of hybrid warfare. This hybrid threat blurs the border between war and peace and the battlefield is no longer a clearly defined area. Conflicts will occur more frequently in the cyber domain (with, for example, criminal hackers being used as a proxy of a state actor). This will also lead to a blurring of the distinction between military and civil applications of technology. New technical possibilities, for example in the cyber domain, are expected to play an important role in this form of warfare in the future. This issue has been addressed within the theme of *Geopolitical threats*.

Not only are the technological innovations themselves important, but also the fact that this knowledge and technology is becoming more and more a**pproachable and accessible** for many (non-expert) users. This is increasing the risk of negative side-effects of the use of certain technologies. The problem with generally available knowledge of technologies is that an expert is often needed to assess this knowledge properly in its context and to apply it responsibly. Experts can estimate consequences and possible additional risks, but uninformed users will probably not be able to do so. The relative ease to access technological knowledge will also increase the risk of use by malicious actors. In the field of biotechnology, for example, it is becoming increasingly possible for do-it-yourselfers to tinker with biochemical structures. As a result, malicious actors will find it easier to obtain synthesised, pathogenic viruses.

One important innovation which was clearly mentioned in various technology surveys is the Internet of Things: networks of sensors which (linked to the Internet) collect data and exchange it for the purpose of monitoring, controlling and optimising systems and processes. This **increasing connectedness and mutual dependency between systems** constitutes a possible risk for national security. For example, the failure or manipulation of critical infrastructure due to a cyber attack can have far-reaching consequences. This risk is heightened by the disappearance of analogue alternatives for digital systems and processes. This is examined in more detail in the Cyber threats and Disruption to Critical infrastructure themes.

In the field of information technology, the availability of data and the capacity to process this into meaningful information (**Big Data**) is increasing rapidly and significantly. More and more data of all kinds is being created and processed into meaningful information and a lot of information is becoming more easily accessible to the general public. This is creating opportunities for, among other things, citizen participation in enforcement and detection, disaster management, etc. There are also downsides however. For example, celebrities and VIPs are becoming more susceptible to blackmail now that their private lives are common knowledge, or big data analysis may make it possible to isolate and harm certain groups. This increasing digitisation can also lead to a gap between population groups, namely those who do and those who cannot use it (see also under *demographic developments*).

Another technological trend is the **increasing intelligence of systems**. Artificial intelligence will be used more and more to automate expertises. The expectation is that this inbuilt intelligence will enable systems to operate more and more autonomously. One example of this is the self-driving car. Also, dangerous and risky work will be performed less and less by people and more by robots instead, with one example being working with hazardous substances. Increasing robotisation also implies certain risks. The fact that systems are more complex and that we are placing more and more trust in their capabilities means that operators have less knowledge about the entire process. As a result they have no overview and that makes it more difficult to respond adequately if the system fails or becomes self-controlling (see, for example, the *Major Accidents* theme).

The artificial intelligence of systems also raises questions with regard to the ethical basis on which these systems will function. The question is whether it is possible to draw up rules to govern the ethics of artificial intelligence and autonomous systems. This question is particularly relevant in the context of autonomous weapons systems. There are increasing demands at international level to curtail the development of autonomous weapons systems in order to prevent any new arms race.

12 Conclusion and considerations

12.1 Introduction

In this chapter we present the results of the risk analysis from the theme chapters and the findings from the autonomous developments in a comparative perspective, based on the objective of the NRP which is to equip Dutch society more effectively to deal with (the threat of) potential disasters and crises and choose the right priorities for that purpose.
The most important questions are:

- Which types of risks constitute the greatest threat, as regards the impact and likelihood, also given the capabilities which are already being used (per risk category)?
- Which national security interests are affected most for one or more risk categories?
- Which of the analysed risks constitute a possible current or perceived threat?
- What are the uncertainties (types, extent) in the results of the risk analysis and to what extent must these be taken into account in the risk assessment and the decision-making?

In this chapter we present the results and provide an interpretation of the results. In addition, we explore in more detail a number of issues from the theme analyses and the autonomous developments. By doing so we link together the results of the individual themes.

12.2 Risk diagram

In order to be able to place the risks of various themes and risk categories in a comparative perspective we use the scenarios from the various chapters and the assessment method (NRA methodology) described in Chapter 2. These scenarios jointly cover the spectrum of the most important risks for national security and serve as illustrations of the threat-related themes.

The outcomes of the assessment with the NRA methodology are presented in the **All Hazard risk diagram** (Figure 12.1). In this diagram the overall impact is shown on the vertical axis, calculated on the basis of the eleven individual impact scores and an equal weight of all impact criteria (for example the number of fatalities counts just as much as the violation of the democratic system)[27]. The scale of the impact increases logarithmically, from *limited* to *catastrophic*, in accordance with the classification into classes as described in Chapter 2. The likelihood is shown on the horizontal axis. This axis is also a logarithmic: very likely is ten times higher than likely, etc.

With regard to the interpretation of the likelihood we wish to point out that the various sorts of risks generally have a different dynamic, meaning that the experts estimated the likelihood in various different ways. Developments that influence the occurrence of natural disasters, whether this involves natural processes (such as the increase in the earth's temperature) or the realisation of investments and measures for protection purposes (such as dyke reinforcement), are spread over a period of time of several decades or more. The likelihood of these types of disasters can often be estimated quite accurately on the basis of data, historical cases and models and are interpreted in terms of once per 10 of 100 year. The same applies to the risks under the themes of *Threats to public health and the environment* and *Major Accidents*, although the time-scale applicable to these types of disasters is shorter.

[27] A detailed explanation of how the risk diagram was constructed, the way in which scores are calculated and the approach to uncertainties in the impact and likelihood can be found in the Guidelines. In the past, sensitivity analyses were carried out with various weighting profiles for impact criteria. These profiles were related to political views and global scenarios of the general public. The analysis demonstrated that the scoring methodology is robust enough for the risk diagram to be based on equal weights of the impact criteria.

On the other hand social and also geopolitical developments are characterised by a high dynamics over time and by latent processes that can ultimately lead to an escalation (incident). As a result, the likelihood of the related events and scenarios cannot usually be expressed as a probability (for example 1% or once per 10 years) and the assessment has to be based on predictability, indications, signals and an expert estimate of how observed trends will continue to develop in the future.

The figure below includes the risk diagram which shows the results of the various risk categories, expressed in scenarios. A larger version of the risk diagram is shown in Annex 3.

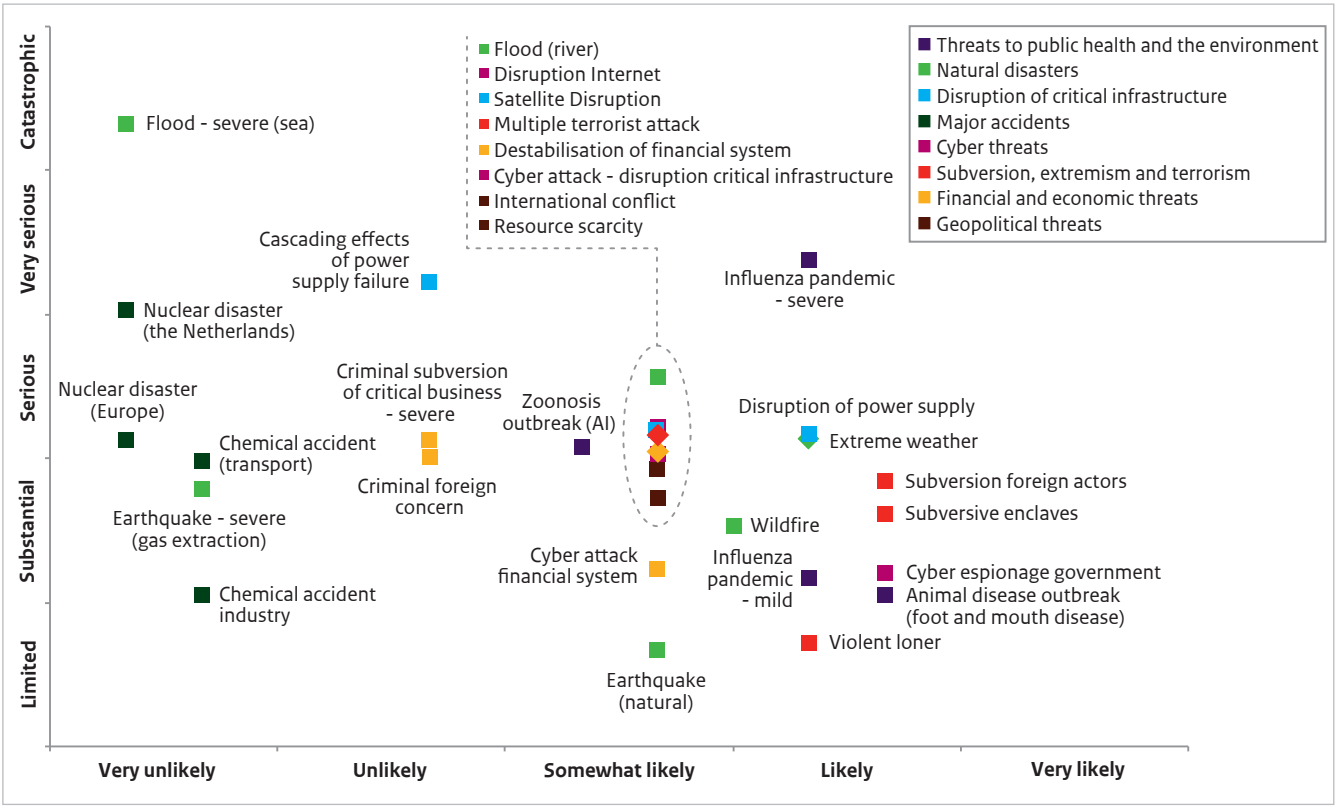
Interpretation

A number of general observations can be made on the basis of the risk diagram. The risk categories which can be found on the **left-hand side of the diagram** have a low likelihood. These are 'physical disasters', such as a nuclear disaster, a catastrophic flood from the sea, a major earthquake (with more than 100 fatalities) and chemical accidents. The likelihood of such worst-case disasters is extremely low. However, when these disasters occur they have an impact on a national scale and (very) seriously compromise several national security interests. Particularly the types of disasters at the top left have major social consequences and lead to disruption.

This finding is supported with examples of disasters which actually occurred, such as the flood as a consequence of the Hurricane Katrina, which battered New Orleans and the surrounding area, and the nuclear disaster at Fukushima in 2011. In both cases the disaster itself was not only disruptive (lot of victims, material damage, failure of critical infrastructure and social dismay), but so were the consequences over a longer period of time: The impact on the economy, the loss of confidence in government and official bodies and the effects on the life of many victims who are 'away from home' for a long time and have to build a new life.

In the case of both these types of disasters the impact was partly determined by cascading effects which occurred as a result of the failure of various critical infrastructure. The place of the Cascading effects of

Figure 12.1 Risk diagram including the scenarios which serve as illustrations of the threat-related themes.



power supply failure scenario in the diagram clearly shows that the impact of this failure is also, in itself, already high, irrespective of the cause. There are several possible causes for such a failure, not only a large physical disaster but also an isolated technical or deliberately caused disturbance. For that reason the likelihood of this scenario type is higher than that of a flood or nuclear disaster, although it is still unlikely that it results in serious disruption.

The impact of chemical accidents is lower because, unlike in the event of a serious flood or nuclear disaster, it does not result in a large area being unusable or inaccessible for a prolonged period of time and substantial affection of critical infrastructure, neither does any large-scale evacuation take place. Nevertheless, there may well be numerous victims, damage and social and psychological consequences, as demonstrated by the disaster in Tianjin in 2015 and, on a smaller scale, the fireworks disaster in Enschede (2000).

The categories and scenarios with a higher likelihood can be found on the **right-hand side of the diagram**. These include the phenomenon of undermining the democratic system, cyber espionage and an animal disease crisis. Animal disease crises, such as an outbreak of foot and mouth disease or swine flu, are quite a regular occurrence and that explains the high likelihood. Such crises can have a disruptive effect at regional level and for the livestock sector, but the impact will be limited on a national scale. Cyber espionage – including, for example, cyber crime – and activities which undermine the functioning of the democratic system and its institutions are already taking place. They still have a low overall impact, but can seriously affect specific national security interests such as the physical safety or the social and political stability. If several developments persist, the overall impact can be serious in the near future.

In the top right of the diagram is the serious influenza pandemic scenario, which is characterised by both a relatively high likelihood and a large impact. This high impact differs in terms of some aspects from that of the 'physical disasters' discussed above. For example, a pandemic (a global infectious disease crisis) is, by definition, an international disaster (outside threat) that can hamper disease control and measures to limit the consequences. A serious pandemic is also characterised by numerous fatalities and ill people with the potential consequence of large-scale incapacitation of personnel, which in turn can lead to economic damage, failure of critical infrastructure and the functioning of society. In contrast to a flood this is a disruption of limited duration.

A relatively large group of risk categories can be found in the **middle of the diagram**. Their occurrence is considered to be somewhat likely and, if they occur, that will certainly affect national security, but not all national security interests to a high degree. In this part of the diagram are scenarios relating to the disruption to critical infrastructure (with the exception of cascading effects), cyber threats, extremism and terrorism, geopolitics, criminal interference in the economy and the smaller variants of natural disasters and health threats.

12.3 Impact

12.3.1 Overall impact

Insight into the seriousness and the character of the impact with which the various national security interests are affected for each risk category is also important. This insight is relevant to identify possible measures which can be taken to make the Netherlands more resilient. For that reason impact-based assessments are made in addition to the All Hazard risk diagram. Figure 12.2 shows the overall impact (the total impact of the different criteria together) followed by an assessment of the impact scores for each national security interest.

Interpretation

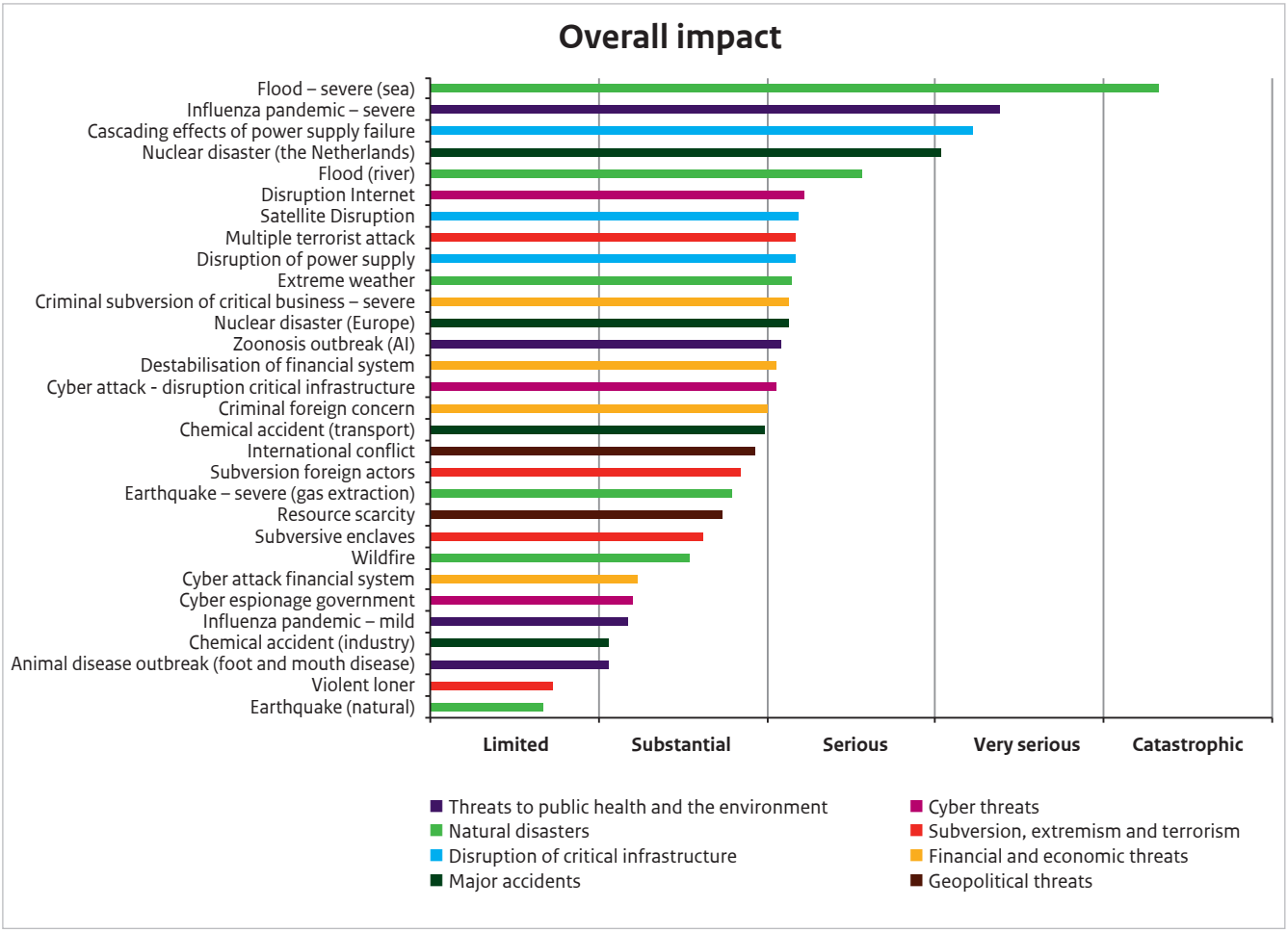
From figure 12.2 it can be deduced that numerous scenarios have an identical overall impact score. There is a large group for which the impact is 'serious'. Five scenarios have a greater overall impact. These are:

- Flood from the sea
- Severe influenza pandemic
- Cascading effects of power supply failure
- Nuclear disaster (the Netherlands)
- Flood from the river

The cause of this high impact has already been described in the clarification of the risk diagram. Figure 12.2 makes it more explicit that these types of disaster, which may often have a low likelihood, are nevertheless the most disruptive as regards the overall impact.

Insight into the violation of the five individual national security interests is also useful because such an analysis can provide a direction for the reinforcement of specific capabilities in relation to a security interest.

Figure 12.2 Total impact.



12.3.2 Territorial security

This interest can be affected in two ways. On the one hand, the consequence of a flood and a serious nuclear disaster is that part of our territory will be unusable or inaccessible for a long period of time.

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

12.3.3 Physical safety

We interpret the impact of this interest by the numbers of victims (fatalities, seriously injured and chronically ill including psychological disorders) and a lack of basic needs. Large numbers of victims come about primarily in the event of natural disasters, serious accidents and threats to health, such as a pandemic.

In addition, a major (multiple) terrorist attack can cause a substantial number of victims, whether they are committed with firearms, explosives or CBRN agents. The scenarios within the theme of Disruption to Critical Infrastructure, including a cyber disturbance to critical processes, as well as some natural disasters, can create a major lack of life's basic necessities such as drinking water or heat (gas/electricity).

12.3.4 Economic security

It is evident that the scenarios within the theme of Financial-economic threats affect economic security. In such instances there is both a violation of the vitality of the economy (large unemployment, failing sectors, decreasing confidence in the economy and financial system) and financial damage. Economic damage in terms of high costs occurs in almost all risk categories.

12.3.5 Ecological security

Of all scenarios in the risk diagram, only a major flood and a wildfire cause a (serious) violation of nature and the environment. The observations about autonomous developments (Chapter 11) show, however, that a number of global, often insidious developments have negative effects on nature and the environment with possibly greater consequences for ecological security. We discuss this aspect in the paragraph on developments and future threats at the end of this chapter.

12.3.6 Social and political stability

This national security interest comprises disruptions to daily life of the population, the violation of democratic institutions and standards and values and destabilisation of the social climate in our society. The disasters that affect critical infrastructure, or which lead to a large area having to be evacuated, will quickly result in a serious disruption to daily life. This implies that large groups of people will not be able to participate normally in society (work, school, social activities) for a certain period of time.

The structural violation of the democratic constitutional system and the standards and values of our open society features in the scenarios that fall under the themes of 'Geopolitical threats', 'Subversion, extremism and terrorism', 'Financial-economic threats' and the 'Cyber espionage' risk categories.

Scenarios in other risk categories will, at most, lead to a short-term disruption to the functioning of institutions. However, this will not lead to a structural violation. 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 the social climate. In particular, situations in which a large degree of uncertainty dominates the further continuation of events, in which there is a feeling of culpability towards (governmental) bodies or companies, or which result in various opposing groups (based on different interests or viewpoints), can lead to outbreaks of violence (riots or revolts, as well as looting) or a structural violation of the social cohesion.

12.4 Developments and possible threats for the coming years

Apart from the disasters, threats and crises described in the various themes and related scenarios in this NRP, other developments can also constitute a threat for national security. Developments, processes and trends with a broader temporal (medium to long-term) and geographical (global) perspective than the individual themes in themselves do not constitute a direct threat for national security, but can have an influence on certain risks. They are characterised by considerable uncertainties, as a result of which their influence in terms of impact and likelihood cannot easily be determined. These developments largely lie outside the direct sphere of influence of an individual organisation or a single country.
For that reason it is all the more important to continue monitoring these developments and their effects properly, and to consider policy and development of capabilities which can address these risks in an international context.

Climate change increases the risk of natural disasters (floods, extreme weather, wildfires), large-scale epidemics and disruption of critical infrastructure. In our country work is being carried out using various approaches on the basis of a climate adaptation strategy with a view to control the consequences of climate change. For instance, the local effects of extreme weather incidents clearly show that climate adaptation requires permanent attention.
The effects of climate change on a global scale are expected to be substantial. In various parts of the world the number and the impact of natural disasters may increase and there will be more frequent shortages of food and (drinking) water. These phenomena may indirectly lead to an increase in migration, conflicts between groups and countries, and to a 'battle' for raw materials and natural resources. They will therefore constitute a threat to our national security in the longer term. It is currently impossible to predict when this threat will occur and on what scale.
Also, the **loss of biodiversity** and the growing **environmental pressure** (pollution of the environment and depletion of natural sources due to the growth in the world population and increasing need for prosperity) constitute a threat for the longer term. Our country has a low level of biodiversity. Although this does not constitute a direct threat to our national security in the sense of a disruptive disaster or crisis, it does represent an insidious violation of ecological security. At global level the increasing environmental pressure is having the same effect as that of climate change.

One of those effects is **migration**. Migration is increasing worldwide, both of people who were fleeing conflicts and those who are looking for a better future. The expectation is that these will be joined in the future by so-called climate refugees. If the influx of refugees exceeds our society's capacity to absorb, various national security interests may be compromised. This applies primarily to social and political stability due, for example, to differences in interpretations about social and statutory norms and values, manifestations of discrimination and xenophobia, increasing polarisation, decreasing solidarity and social cohesion, unrest and feelings of insecurity and the breakdown of social support for refugee care.

Another trend which might be detrimental to the social cohesion in society is that of the **widening gap between population group**s in the areas of income, health, employment opportunities, well-being and socio-cultural views. In addition, we can also highlight a number of **trends in the socio-cultural domain**:
The individualisation (and the focus on individual interests), the decreasing confidence in the government and the authority of science and institutions, the increasing feeling of 'great discontent', the growing segregation and information pressure, the influence of social media, the pressure on the welfare state and the increasing polarisation between various population groups in the religious, ethnic, social and political fields.

At economic level the gap between groups in society is growing (**economic inequality**), both globally and in the Netherlands. A high degree of income inequality is linked to less social mobility, declining solidarity between citizens and a loss of confidence in the rule of law and the parliament. The decreasing solidarity can also be exacerbated by the persistence of **relatively high unemployment** and the pressure on the underside of the employment market, which is partly increasing due to continuing **automation and robotisation**. A high degree of income inequality can also slow down economic growth in the Netherlands.

From the perspective of geopolitics a change is observed from a multilateral to a multipolar world order. This is accompanied by greater fragmentation within the international system, **a shifting balance of power**, more difficult relationships between superpowers and other emerging countries, and a **growth in tensions**, (the threat of) conflicts and **increasing regional instability** in the world. The Netherlands could be dragged into a conflict due to its relationships with its allies. It should be noted, however, that the likelihood of an armed confrontation between superpowers or a threat of a global conflict as in the Cold War, is extremely small.

In contrast, regional conflicts can be expected to have indirect effects, like the aforementioned increasing migration flow.
With regard to geopolitical developments the phenomenon of **hybrid threat**, meaning the integrated use of conventional and unconventional means, open and covert activities and the use of military, paramilitary and civil actors and resources to exploit an opponent's vulnerabilities in order to achieve geopolitical and strategic goals, requires specific attention. The use of manipulated information and deception are important aspects of hybrid tactics. In recent years an increase in hybrid conflicts has already been observed.

In this context of geopolitical developments we are also seeing an increase in the use of economic influence as political leverage, either directly via **economic sanctions** or indirectly via threats, and the use of **strategic economic policy** by other states: Anti-competitive activities aimed at securing and protecting national economic interests. As an open trading nation the Netherlands are very dependent on the unrestricted functioning of world trade. The increase in protectionism is expected to have a disproportionally severe effect on the Netherlands, all the more so given that, at an economic level, the Netherlands will (have to) cooperate more and more with countries where the state traditionally has a strong role.

Although the economy initially appeared to be recovering following the financial crisis, a slowdown in world trade appears to have been taking place since 2011. Moreover, the difference with the trend-based growth which was expected before the drop in world trade is increasing all the time.

For a number of sectors **globalisation** and increasing concentration (centralisation) in the international-economic area can constitute a threat. Centralisation in, for example, the food sector and among producers of medicines and vaccines, is creating greater dependency on a limited number of actors and that implies risks for the availability of essential substances and resources. The increasing complexity and interconnectedness of systems and the financial world hamper adequate control of risks and any crises that may occur.

Technological innovations are also having an effect on national security risks. Smarter devices are being used more and more to improve processes and to find sustainable solutions for certain problems. However, such technological developments imply new risks. The emergence of the Internet of Things (IoT) is creating **increasing connectedness and mutual dependency between systems**, as a result of which the failure or manipulation of critical infrastructure due, for example,

to a cyber attack can have greater and greater consequences. At the same time digitisation in all kinds of fields continues to play a role, resulting in a greater dependency of society on, for example, the Internet. This increasing digitisation can also lead to a gap between population groups, namely those who do and those who cannot use it.
It still appears to be difficult for governments to supervise or influence (technological) innovations. Innovations can set social transitions in motion which are **difficult to control**. For example, innovations may outgrow the traditional roles in society and create new flows of funds. Legislation and regulations relating to technological innovations are difficult to create because developments are taking place at such a fast rate and it is difficult to predict which technologies are really going to make a difference and which are a potential threat to national security. In addition, knowledge and technology are becoming more accessible for a broad audience and this is increasing the risk of **negative side-effects** of the use, or even **misuse**, of certain technologies.

12.5 In conclusion

By describing the context and features of the different risk themes, the assessment of the risks and the underlying (impact) analyses, the NRP offers the possibility of viewing various potential disasters, threats and crises which could disrupt our society in a comparative perspective.

In addition, the results provide input for the capability assessment. The NRP presents an overview of the risks, based on the current situation, including what the Netherlands are already doing to manage the risks and eliminate threats (read: the existing capabilities). It also describes trends and developments which, in the future, may lead to a change in the current risks or cause new risks to arise. The capability assessment will reveal whether the current capabilities are considered sufficient, or whether certain capabilities have to be reinforced or developed.

The most important observations based on the results are the following:

- It is evident that a large-scale flood, a nuclear disaster, a pandemic and a long-term power supply outage (including cascading effects) are more destabilising than others (given their high impact). For this reason it is obvious to put effort in prevention of these disasters to occur wherever possible. The analyses show that the Netherlands are already doing a great deal to manage these risks and that, partly for this reason, the likelihood of such disasters is extremely low.
- Various other risks such as cyber threats, disruption of certain critical infrastructure, manifestations of extremism and terrorism, geopolitical threats, criminal interference in the economy, some types of natural disasters (such as extreme weather) and zoonosis outbreaks have a lower overall impact, but can have a serious detrimental effect on specific national security interests such as physical safety, or social and political stability. Those specific interests can provide a relevant basis to strengthen capabilities.

- A number of types of disasters and threats have a relatively high likelihood and a limited impact. It is important to determine what the possible triggers or developments might be that would exacerbate the impact (in the future) of these types of disaster. For example, cyber espionage and activities which affect the functioning of the democratic system and its institutions have not yet manifested themselves on a (very) serious scale. However, their impact may be greater if certain developments continue. Some of these risks may be less disruptive on a national scale (compared to other threats), but may still be regarded as very serious incidents at regional level. Taken the capability assessment into account, the challenge is to achieve proper coordination with the safety regions.

In addition to these results, analysis of (autonomous) developments, their mutual relationship and their possible influence provide insight on national security. We can illustrate this using the following two important increasing risks:

- The increasing connectivity and mutual dependency between systems can lead to the more rapid occurrence of (greater) cascading effects. Besides the mutual interconnectedness of various critical infrastructure, the focus is on digitisation with accompanying cyber threats.
- Based on international and geopolitical developments, the hybrid threat phenomenon has emerged as a relevant risk to our country.

Such developments can increase certain risks in the long term, or introduce new risks. This need to be taken into account in the capability assessment.

13 Annexes

Annex 1. Classification of themes and risk categories

In the NRP each theme is subdivided into several risk categories. A risk category includes a set of potential disasters and threats of more or less equal nature. For example, extreme weather (Natural disasters theme) includes heavy storms, intensive rainfall, snowstorms and black ice. These types of weather are all characterised by a limited duration, a limited affected area (often a part of the country or a region), lots of inconvenience and disturbance to daily life, a limited number of victims and large physical damage. Heat and drought often last for a longer period, affect the entire country and partially have other consequences. For that reason they constitute a separate risk category within the Natural disasters theme.
The safety regions apply three layers for the classification in the RRP denoted as the social theme, the crisis type and the incident type. A social theme is comparable to a 'theme' in the NRP, a crisis type is comparable to a risk category and the incident types are more detailed developments of a crisis type. For example, the 'Incidents with toxic substance in the open air' crisis type covers the following types of incidents: 'Road transport incident', 'Water transport incident', 'Rail transport incident', 'Pipeline transport incident' and 'Stationary facility incident'.
Table B1.1 shows the theme classification of the NRP and of the RRP next to each other.

A number of themes in the NRP and RRP overlap, namely themes involving crucial tasks at both national and regional level and responsibilities for the risk and crisis management, such as a large-scale nuclear accident. Some themes and the crisis types they refer to are primarily regional (for example fires in vulnerable objects), while others are typically national (such as geopolitical threats and economic security). Figure B1.1 shows an overview of the overlap and differences between typically national and regional themes.

Figure B1.1 Overlap and differences between national and regional themes.

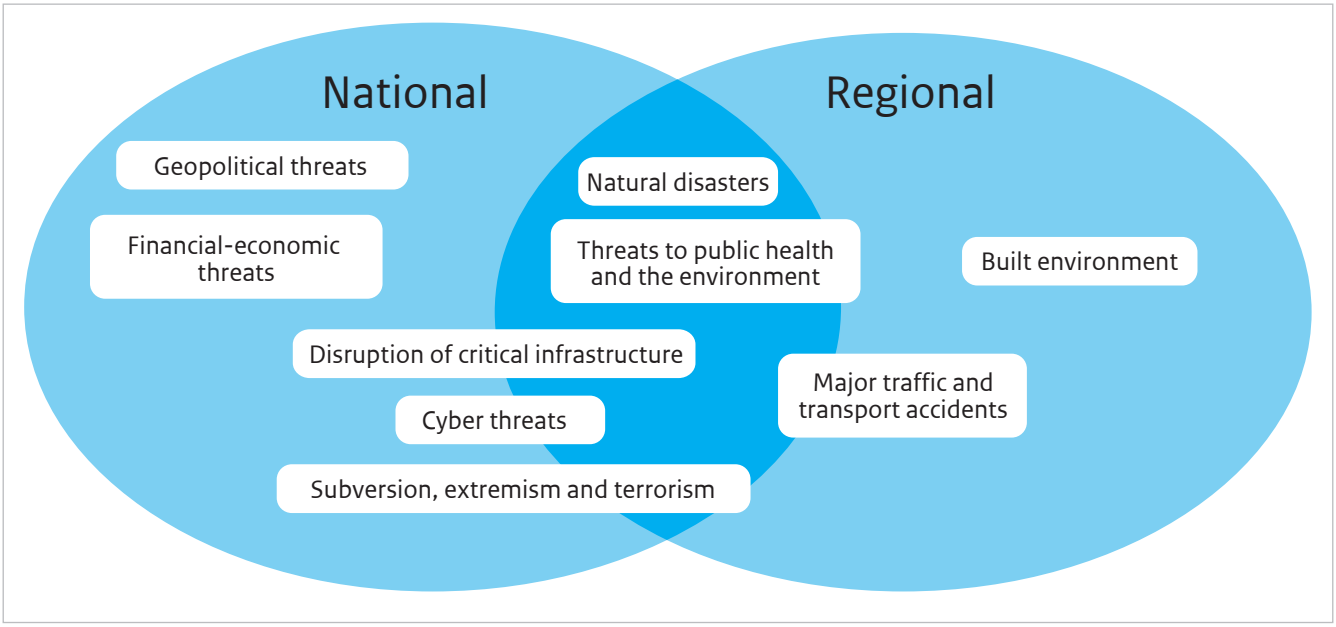


Table B1.1 Overview of the overlap and differences between national and regional themes.

NRP thematic classification		Safety regions thematic classification (RRP)	
Societal theme	**Risk category**	**Societal theme**	**Crisis type**
Natural disasters	Flood	**Natural environment**	Floods
	Extreme weather		Extreme weather conditions
	Wildfire		Wildfires
	Earthquake		Earthquakes
	Heat and drought		Extreme weather conditions
	Solar storm		Plagues
			Animal diseases
Threats to public health and the environment	Human infectious diseases	**Public health**	Epidemic
	Animal diseases and zoonoses		Threat to public health
	Environmental disasters		
	Food crises		
	Antibiotic resistance		
Major accidents	Nuclear disasters	**Technological environment**	Nuclear incidents
	Chemical accidents		Incidents with flammable/explosive substance in open air
			Incidents with toxic substance in open air
	Transport accidents	**Traffic and transport**	Aviation incidents
			Incidents on or under water
			Traffic incidents on the land
			Incidents in tunnels
		Built environment	Fires in vulnerable objects
			Collapses in large buildings and structures
Disruption of critical infrastructure	Independent disruption to critical infrastructure (power supplies, drinking water, ICT, payment transactions)	**Critical infrastructure and provisions**	Disruption to power supplies
	Common causes (simultaneously)		Disruption to drinking water supply
	Cascading effects		Disruption to waste water discharge and purification
			Disruption to waste processing
			Disruption to food provision

Table B1.1 Overview of the overlap and differences between national and regional themes. *(continuation)*

NRP thematic classification		Safety regions thematic classification (RRP)	
Societal theme	**Risk category**	**Societal theme**	**Crisis type**
Cyber threats	Disruption to industrial automation and control systems		Disruption to telecommunications and ICT
	Disruption Internet capacity		
	Cyber espionage		
	Cyber crime		
Subversion, extremism and terrorism	Large-scale public order disruptions	**Social environment**	Crowd panic
	Extremism and terrorism		Disruption to maintain public order
	Subversion the democratic system and open society		*Terrorism*
Financial and economic threats	Destabilisation of financial system		
	Criminal subversion		
	Cyber crime in the financial sector		
Geopolitical threats	Resource scarcity		
	Power shifts within the international system		
	Increasing tensions between superpowers		

Annex 2. 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 requirement. 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, multidisciplinary expertise and therefore collectively span the National Security work field. This structure guarantees the NRP's *All Hazard approach* as well as the methodological and cross-disciplinary analysis uniformity.

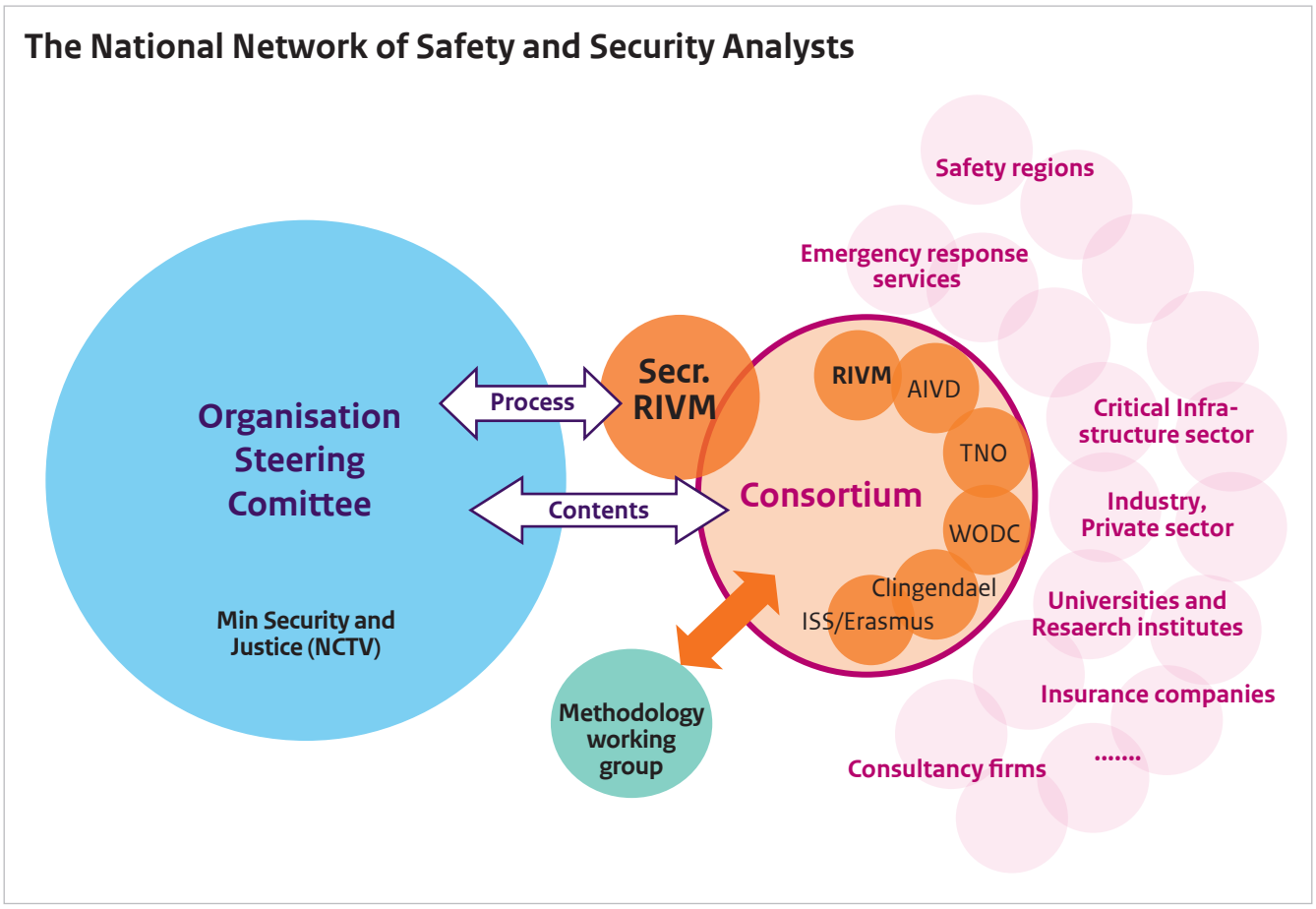
The six core organisations, united in the Task Group, share responsibility for the material quality of the NRP and other products. Specific, supplementary expertise is provided by the other organisations in the network. The organisations in the core and the ring make experts and analysts available to 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 control, 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 accommodated within the RIVM.

The methodology working group was set up in 2007. This working group, which operates under the responsibility of the Ministry of Security and Justice, developed and maintained the NRA methodology. As regards the production of the NRP the working group is involved in supporting the risk assessment, particularly regarding proper and accurate application of the methodology.
The ANV's tasks are:

1. To produce the National Risk Profile.
2. To produce other in-depth theme studies and surveys, ad hoc analyses and other studies relating to national security.
3. To advise the SNV about the relevant developments and new risks which constitute a potential threat to national security.

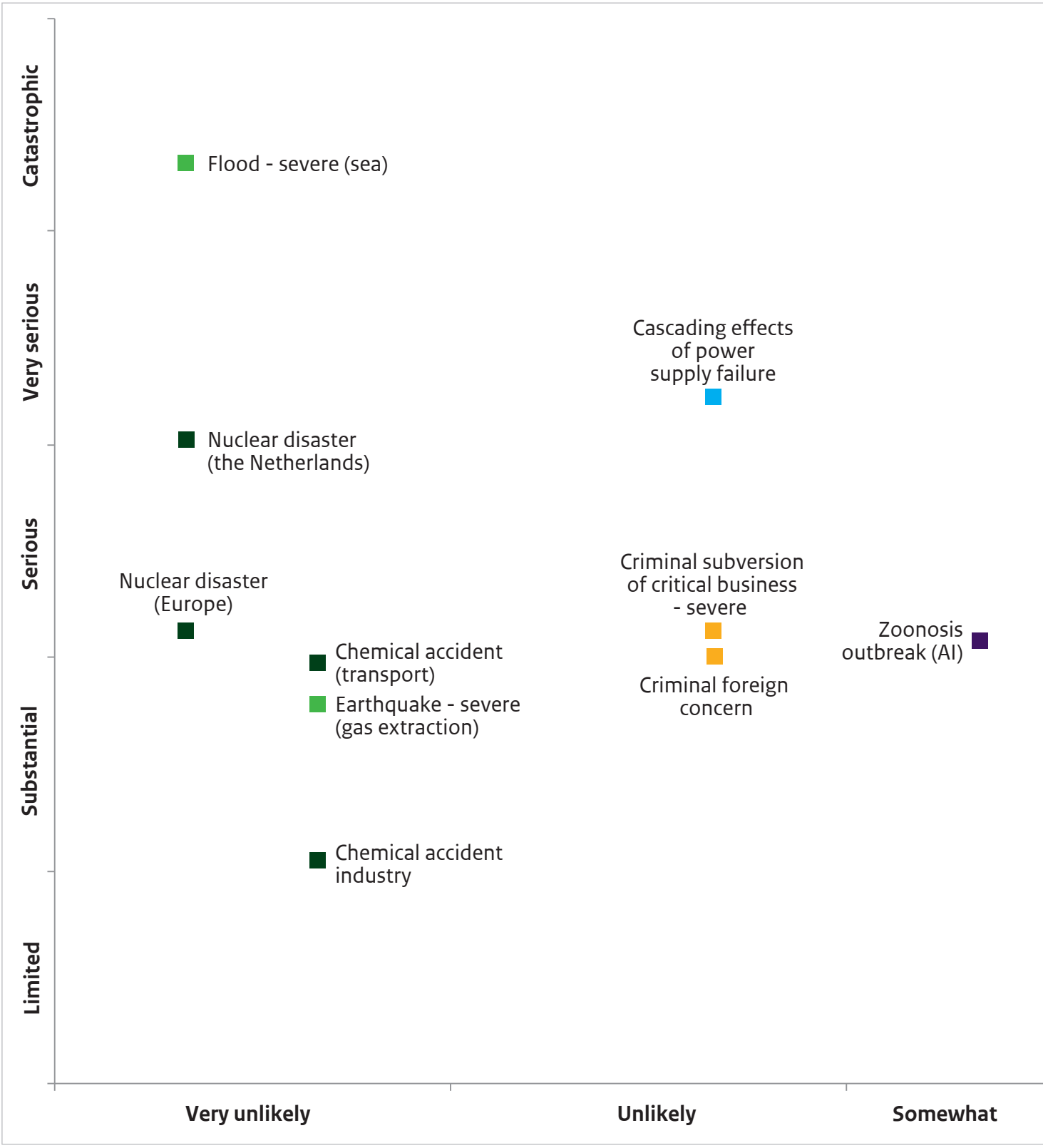
A diagram of the organisational structure is shown in figure B2.1.

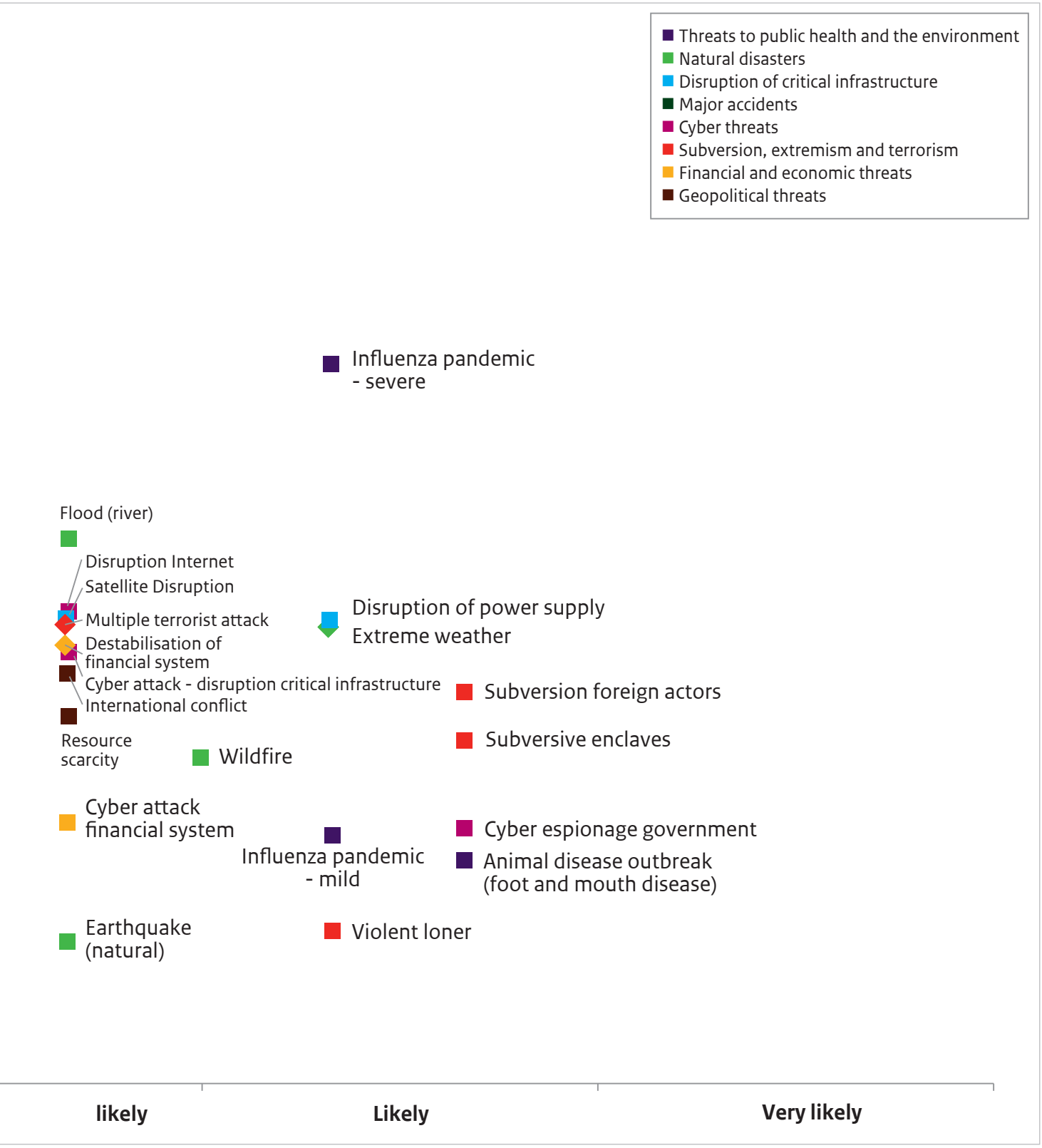
Figure B2.1 The National Network of Safety and Security Analysts network structure; the ring of organisations around the Task Group is dynamic and the organisations referred to serve as an example.



Annex 3. Risk diagram

Figure B3.1




Threats to public health and the environment
Natural disasters
Disruption of critical infrastructure
Major accidents
Cyber threats
Subversion, extremism and terrorism
Financial and economic threats
Geopolitical threats
Influenza pandemic - severe
Flood (river)
Disruption Internet
Satellite Disruption
Multiple terrorist attack
Destabilisation of financial system
Cyber attack - disruption critical infrastructure
International conflict
Disruption of power supply
Extreme weather
Subversion foreign actors
Subversive enclaves
Resource scarcity
Wildfire
Cyber attack financial system
Influenza pandemic - mild
Cyber espionage government
Animal disease outbreak (foot and mouth disease)
Earthquake (natural)
Violent loner
likely
Likely
Very likely

The National Network of Safety and Security Analysts
ir. L. Gooijer (editor)

Government of the Netherlands

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)

November 2016

009835