Working with scenarios, risk assessment and capabilities

in the National Safety and Security Strategy of the Netherlands

October 2009

Contents

1 Introduction

This is the revised guide to the national safety and security strategy. The purpose of the guide is:
- to describe the method used for scenario development, national risk assessment and capability analysis;
- to establish and justify the choices made;
- to provide a guide for people who have to work with the national safety and security strategy.

This guide makes clear to people who have to work with the national safety and security strategy how this method works. It should also serve as a foundation for those drawing up incident scenarios and for those carrying out the national risk assessment and capability analysis in 2009 and later.

This guide primarily pays attention to the main features of the method of the National Safety and Security Strategy. In chapter 3, we look at the scenario development. In chapters 4, 5, 6 and 7, we look at the structure of the national risk assessment, the assessment of the impact, the assessment of the likelihood and the significance of the risk diagram. In chapter 8, we look at the third phase of the method, i.e. the capability analysis. In the appendices, you will find background information about a number of subjects.

The method and this guide were written by a working group, consisting of:

- Dr. Hans Bergmans - National Institute for Public Health and the Environment
- Ir. Jasper van der Horst - Aon Global Risk Consulting
- Dr. Leon Janssen - Environment and Nature Planning Bureau
- Dr. Erik Pruyt - Technical University of Delft, Technical Faculty, Administration and Management, Policy Analysis Section
- Dr. Vic Veldheer - Social and Cultural Planning Bureau
- Drs. Diederik Wijnmalen - TNO Defence and Security
- General Intelligence and Security Service
- Ir. Mark Bökkerink – Ministry of the Interior and Kingdom Relations
- Drs. Pamela van Erve – Ministry of the Interior and Kingdom Relations
- Drs. Juliette van de Leur – Ministry of the Interior and Kingdom Relations

Following the national government, the local government and the safety regions use a comparable method for risk analysis and analysis of capabilities. This method, laid down in the 'Handreiking Regionaal Risicoprofiel' (Assistance Regional Risk Profile), is applied in the stocktaking of possible disasters and crises at a regional level and the aggregation into a regional risk profile. This profile forms the basis of the regional policy plans.

1.1 Reader's guide for working group members

This guide contains practical information for participants in the various working groups in which scenarios are devised, in which impact and likelihood scores are assigned to the scenarios, and in which work is done on capability analysis. The guide also contains background information and information supporting the choices made.

For a diagram of the national safety and security method in general, please refer to Chapter 2 in particular, section 2.2 in which the different roles of those concerned are explained.

In Chapter 3, which concentrates on the development of a scenario, sections 3.1, 3.2, 3.4 and Appendix A are important to scenario working group members.

Chapter 4 contains a general introduction to the system for risk assessment. Section 4.3 and Appendix A are the most relevant for working group members.

The 10 impact criteria are described in Chapter 5. Section 5.3 is the key section for working group members who are going to allocate scores. The scores are filled in in this section. Section 5.2 contains an explanation of how they should be filled in.

The likelihood estimation is explained in Chapter 6. Section 6.3 is of most interest to working group members.

The result of the scoring is explained in Chapter 7.

An explanation of how capability analysis is carried out is given in Chapter 8. All of it is relevant for working group members who are working on capability analysis. Appendix A is relevant for them too.

2 National Safety and Security

This chapter describes the context of the national safety and security method. First of all, the concept of National Safety and Security and the aim of all this work are examined. This is followed by a summary of how the national safety and security method is organised, and who has a role in the various stages.

Threats to our safety and security are changing and are becoming increasingly interconnected. Relatively simple threats can lead to societal disruption due to increasing dependencies. This means that the response to existing and new threats is harder to formulate and implement by a single ministry or organisation. An approach is required that is holistic and coherent, that can consider all threats: no longer must specific (known) threats underpin planning and policy, but the extent to which national safety and security is threatened or could be threatened must be taken as the starting point.
In order to implement this approach, the Cabinet established the National Safety and Security Strategy in 2007. The strategy aims to protect society and the population on its own territory against internal and external threats. Our national safety and security cannot be dissociated from the security of other countries, in particularly our European partners and NATO allies. Partly for this reason, the domestic security policy to which this strategy mainly relates and Dutch international security policy are closely linked.

National safety and security is at issue when vital interests of the Dutch state and/or society are threatened in such a way that there is a question of – potential – societal disruption. Vital interests are defined as:

- territorial safety (threatened through a breach of our territorial integrity);
- physical security (public health);
- economic security (undisrupted working of the economy);
- ecological security (living environment);
- social and political stability (e.g. respect for core democratic values and the functioning of democratic institutions).

2.1 The National Safety and Security method

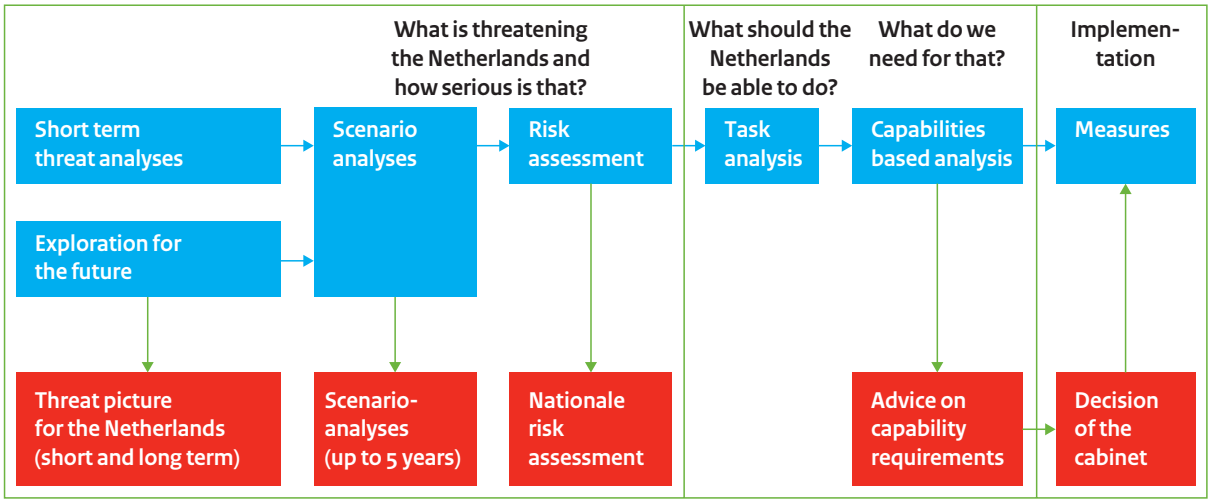
The method described in the strategy will enable the Cabinet to determine better than in the past which threats jeopardise national safety and security and how to anticipate those threats, irrespective of their origin or nature. Furthermore, the method not only makes it possible for the Cabinet to make better-substantiated decisions about where to set priorities and how to do this, but also to consider those choices in relation to one another.

The method for strengthening national safety and security consists of three phases:
1 National analysis of threats and assessment of risks (what could befall the Netherlands?)
In this phase, a distinction is made between risk analysis and risk assessment. During the analysis, known and new threats are identified and developed. This analysis relates primarily to the medium to long term (up to about 5 years). In addition, analyses must be performed with regard to long-term threats (from about 5 years upward) and in short term threats (up to about 6 months). The outcomes of the long-term and short term forward studies can both lead to devising medium-term scenario analyses in the 'thematic in-depth study'. In this case, it is possible to opt for a scenario that can occur in the next five years, or for a scenario that can occur within a five-year period situated in the more distant future, for example in 20-25 years' time. The thematic in-depth study results in scenario descriptions that form the foundation of the national risk assessment (NRA), the assessment of threats in terms of vital interests and likelihood, and the positioning of these risks in relation to each other.
2 Capability analysis (do the Netherlands have the necessary capabilities?)
Based on the risk assessment of all the scenarios analysed, an investigation is conducted to find out

which capacities are already available and which of these could contribute to a reduction of the impact or the likelihood. A recommendation will then be drawn up for the Cabinet about the capabilities that need to be reinforced. In this phase, a decision will be taken about what more the Netherlands (government, people, businesses and civil society) could do than it does already.

3 Monitoring (how and where is national safety and security reinforced?)
The Council of Ministers then decides whether national safety and security should be improved by reinforcement of capabilities and if so, where and how. Political/administrative choices are then converted into policy, legislation and concrete actions.

Figure 2-1: The National Safety and Security method



The method is established in such a way that it is possible to use it across the entire spectrum of national safety and security. The National Safety and Security method is not a regulation, it is a means of safeguarding vital interests. The method is an aid that gives policy makers a framework – in addition to other frameworks – to weigh up the threats, and be able to make policy choices more effectively.

2.2 Stages and roles in the method

This section describes who plays a role in which of the various stages in the method and how that role is interpreted. In doing this, a distinction is made in any case between the role of the specialist departments, inter-departmental liaison committees and of the coordinator and manager of the method.

The National Safety and Security Strategy is used by central government. Due to the inter-departmental contribution to the method, the Interdepartmental Working Group on National Safety and Security (IWNV) and a Steering Group on National Safety and Security (SNV) are involved in every step of the method. The different roles in the various stages of the method are described in greater detail below.

The national risk assessment method

- The Ministry of the Interior and Kingdom Relations / Threats and Capabilities (D&C) Programme is responsible for drawing up and maintaining the method as part of the National Safety and Security Strategy. Where necessary, experts are brought in to advise working groups and review teams.
- The method is presented to the IWNV and specified in the SNV.

Scenarios

- Specialist departments are responsible for the development of scenarios in their own policy fields. Where necessary, use is made of expertise present in other ministries, authorities, private individuals, knowledge centres and planning bureaus.
- The choice of the scenarios to be devised and those actually devised is submitted to the IWNV and the SNV.

Risk assessment

- The assessment of each scenario in terms of likelihood and the ten impact criteria which reflect the five vital interests is carried out by a balanced group of experts. The amalgamation of the scores calculated in the risk diagram, the other diagrams and the susceptibility analyses is done by the Threats and Capabilities Programme (D&C) based on the arithmetic method described above.
- The results are presented to the IWNS and the SNV.

The capability analysis

- The capability analysis takes place in a working group that includes all relevant experts and interests. The specialist department with prime responsibility sets up the working group.
- The reporting of the capability analysis of the various thematic in-depth studies form the basis for the findings report including the opinion for the Council of Ministers concerning the capabilities to be reinforced.

The findings report

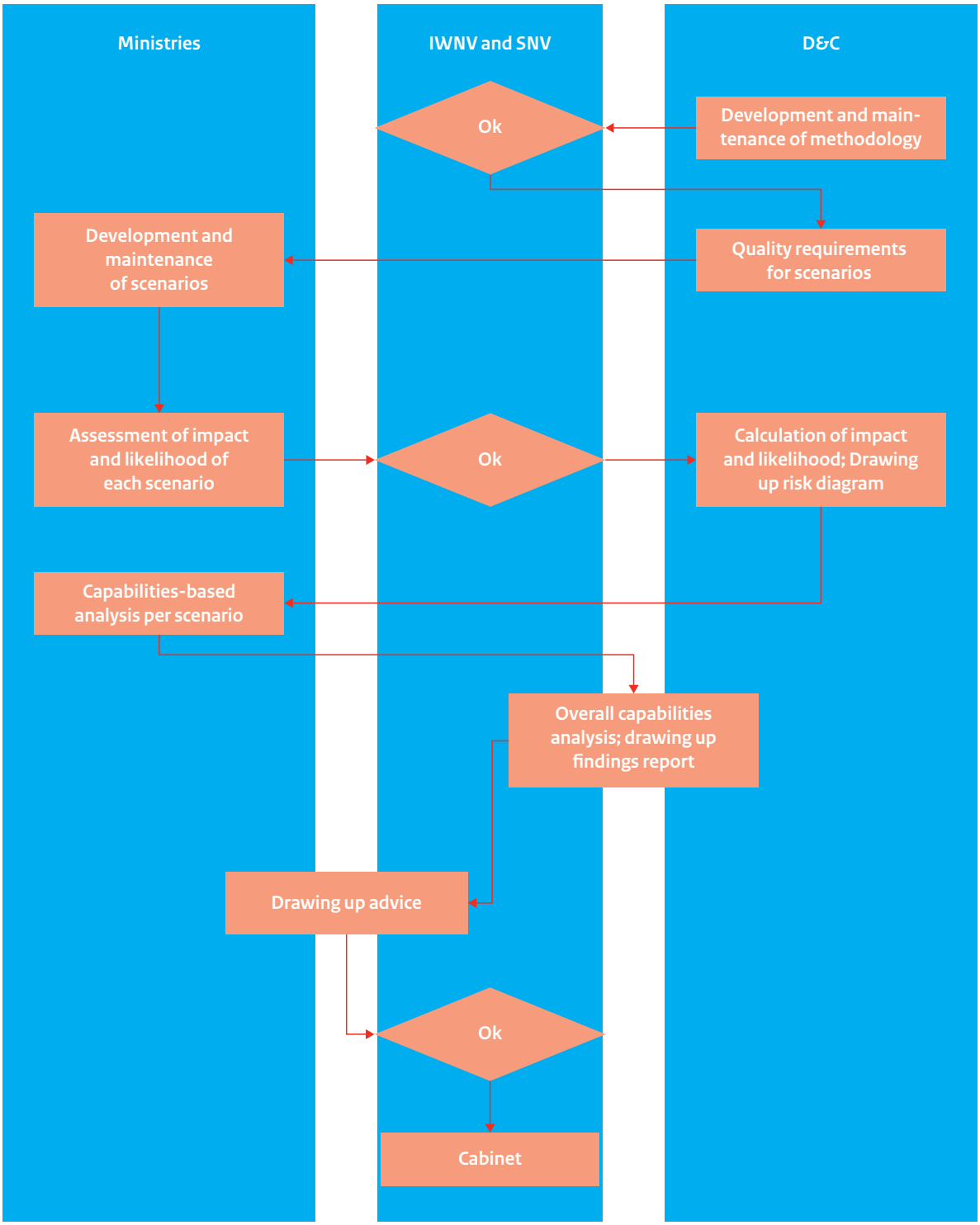
- The findings report is written by a group of representatives from the IWNV and is derived from the results of the scenarios and the risk assessment.
- The method is presented to the IWNV and the SNV.

Advice to the Council of Ministers

- Based on the findings report and the consultation with the IWNV, the policy advice to the Council of Ministers is drawn up (facilitated by D&C). The advice is adopted by the SNV and sent via the Council for Security and Legal Order of the National Security Council to the Council of Ministers. After these groups have approved the policy advice, the Minister of the Interior and Kingdom Relations sends the findings report to the Lower House of Parliament on behalf of the Cabinet.

Figure 2-2 shows this process in graphic form.

Figure 2-2: Stages and responsibilities in the method



3 Scenarios

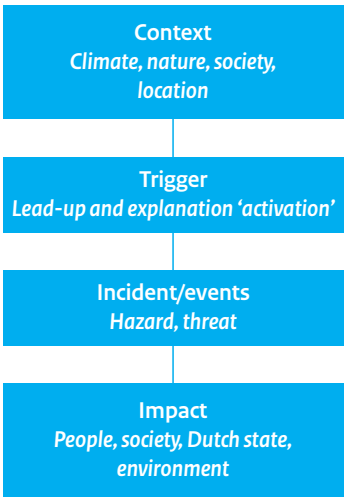
This section describes what we mean by a scenario in the context of the national safety and security method. After that, we examine the process that can be gone through in order to reach this scenario. Finally, a description is given of the constraints and requirements these scenarios must meet.

This first part of the national safety and security method is the elaboration of scenarios that could be a threat to national safety and security in the medium term (up to five years). The choice of the scenarios to be devised is made partly on the basis of the outcomes of the strategic outlook (potential scenarios with a timescale longer than five years) or the outcomes of the short-term horizon scan (up to six months). There may be other reasons for wishing to devise a scenario.

A scenario may be used in various ways. Below, we describe how scenarios are used in the context of the national safety and security method. A scenario offers a way of communicating about obtaining a joint picture of future uncertainties and factors that influence decisions that have to be taken today. In the case of the National Safety and Security Strategy, that means the policy decisions referred to in Chapter 2 about additional investment in the various phases of the safety chain (pro-action, prevention, preparation, repression and aftercare).

In the context of the national safety and security method, a scenario is a description of:

- the incident, i.e. (the nature and scale of) one or more inter-related events that have consequences for national safety and security and therefore have an impact at national level;
- the lead-up to the incident, consisting of the (underlying) cause and any underlying insidious process, and the trigger which actually creates the incident or brings the insidious process to the surface;
- the context of the events, indicating general circumstances and the degree of vulnerability and resistance of people, object and society, to the extent relevant to the incident described;
- the consequences of the incident, indicating nature and scale with an overall description of the response and the control measures;
- the effects of the incident on the continuity of vital infrastructure.



The figure shows the relationship between the various components of the scenario.

3.1 How a scenario is obtained

In order to develop a scenario, input is required from various specialist fields. Of course, this is determined by the nature of the scenario and the choice of the reason, the context, the progress and the consequences of the scenario. Often a contribution is required from experts.

A scenario is often developed by a multi-disciplinary working group. In any case, representatives of the various (specialist) departments have a seat in the working group. It is recommended that the chair of the working group should be drawn from the specialist department most affected. The secretary may be provided from the Threats and Capabilities Programme of the Ministry of the Interior and Kingdom Relations.

The working group may decide to develop the scenario itself, or an external party may be asked to develop the scenario. In that case, it is advisable for the working group to set the terms of reference within which the scenario is to be developed. In both cases, it must be ensured that the scenario

devised offers sufficient leads to be able to carry out the risk assessment in the next stage. It is also recommended that the 10 impact criteria are borne in mind when developing the scenario. Something similar applies for the capabilities analysis: the scenario must be concrete enough so as to be able to assess which capabilities are necessary, which are already available and whether there are capabilities that need to be reinforced.

The input of experts can be guaranteed by including these experts in the working group. One possibility is to ask for one-off input from experts – or at a limited number of carefully chosen times.

Appendix A looks in greater depth at the way in which expert input can be arranged. This appendix is relevant for anyone working with scenario analysis, as well as for those doing the risk assessment and the capability analysis.

3.2 Requirements of a scenario: impact and likelihood

Not all scenarios are suitable for use in the National Safety and Security Method. First of all, we shall examine the requirements imposed on a scenario in order for it to be relevant to national safety and security. After that, we examine the requirements imposed on a scenario with regard to usability, and considerations are given for choosing a scenario in relation to the complete set of scenarios.

An important initial assumption is that all scenarios are possible in principle ('it could happen') but do not have the same likelihood.

A second initial assumption for the development of scenarios is that from the outset, there is an expectation that the scenario has an impact on a national scale, and on at least one of the vital interests) (territorial safety, physical security, economic security, ecological security, and social and political stability). In doing this, the list of separate impact criteria (see Chapter 5) serves as a guide.

In addition, the following general requirements apply to a scenario:

- it must be a plausible story, with factual supporting information; or put another way: a report of events that could occur in the (near) future;
- the incident scenario must be described consistently (according to a schematic structure), and may vary in seriousness from fairly serious to the most serious imaginable;
- it must be representative of one of the security themes chosen;
- it must be structured consistently and logically;
- it must be psychologically expedient, so that it can be sold to and accepted by others;
- it must set the time horizon and the policy field or security topic to which it relates, including specific questions that are on the agenda.
- The incident scenario must be so specific that is possible to deduce from it which capabilities will have to be brought to bear in that scenario;
- it must take account of existing policy on measures for the various stages in the safety chain. However, that does not mean that all policy is perfect or is implemented flawlessly; it must take account of shortcomings observed or anticipated.

Each of the scenarios in the entire set must be unique, and cover the potential scenario scope in terms of risk gradation; the scenarios are 'compression points' in the continuum of variations and possibilities. This can be achieved, among other things, per sub-theme, by thinking up a number of sufficiently distinctive variants or totally different scenarios. Scenarios may differ, for example, in scale and intensity of the events, geographical location, likelihood, and possibly other circumstances. Where there are variants on a scenario, the relevant capability should be examined to discover which threat level will suffice (specific view of capability). If different scenarios are devised, then they can be used to examine which different capabilities are affected, if at all (broad picture).

3.3 Time horizon for incident scenarios

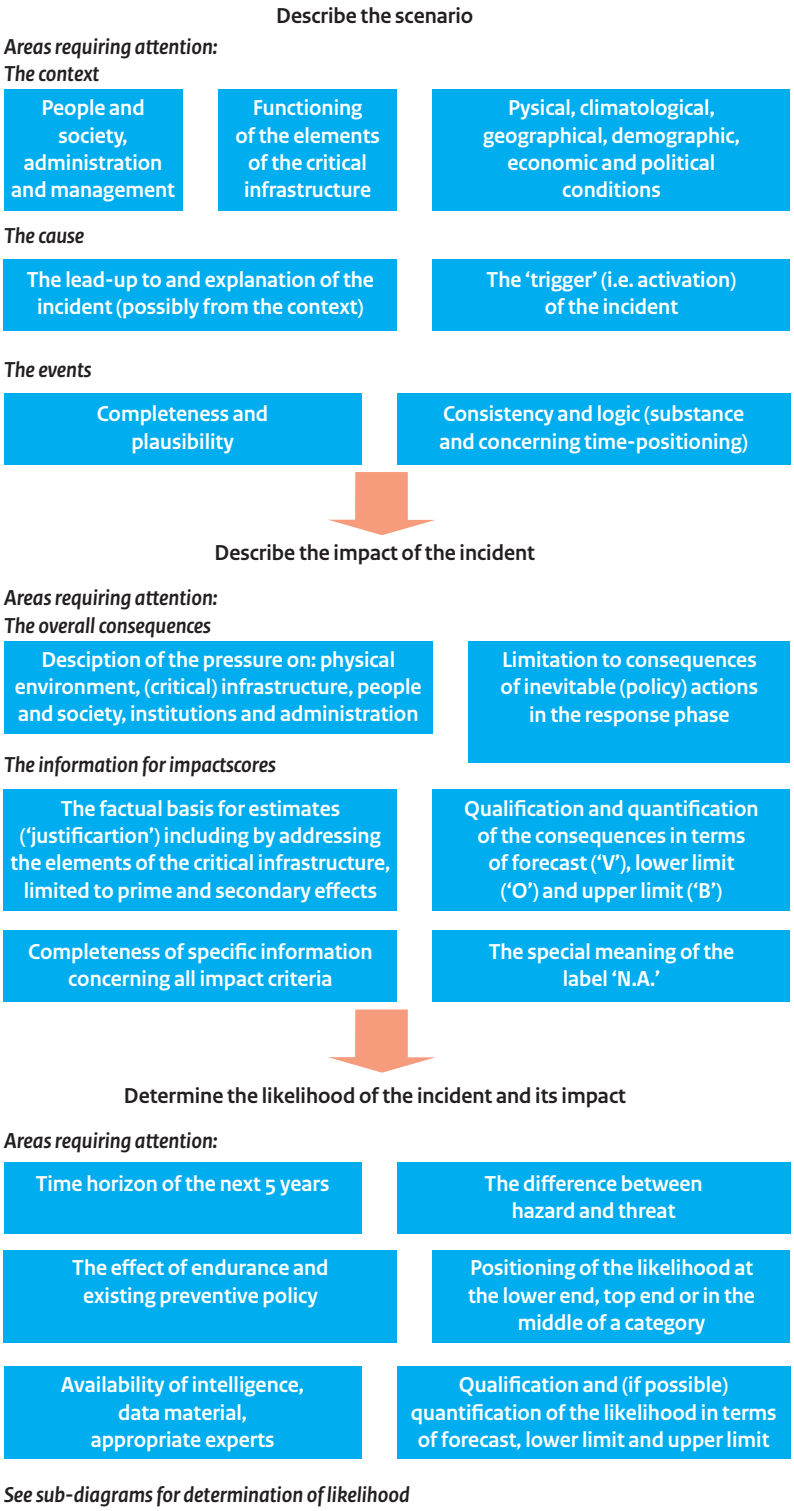
The incident scenarios identified (both hazards and threats) can be split into two groups:
- incidents that are already realistic right now with a certain likelihood; examples of this are major floods or a pandemic;
- incidents which are subject to developments, and where the described impact will only become realistic in the longer term; examples of this are scenarios based on the impact of the ageing population or climate change.

The conditions that the selection of incident scenarios needs to meet are the same for both types of scenario:
- the likelihood of occurrence makes it necessary to consider the allocation of the necessary capabilities already in the next five years, or to make preparations for this;
- the impact of the scenario makes it necessary to consider the allocation of the necessary capacities already in the next five years, or to make preparations for this.

For this reason, the option of developing scenarios for two time periods is offered: for the next five years, and for a five-year period in the longer term (between 20 and 25 years from now). The scenario development for the period in the long term should, of course, be based on the currently available knowledge and predictable trends.

3.4 Diagram for development of scenarios

The above guidance is shown concisely in the following diagram:



4 The national risk assessment

After the scenarios are devised, they can be assigned scores for their likelihood and impact in the national risk assessment (NRA). In this chapter, after a brief introduction of the risk assessment and its place in the overall method, we examine the method and the risk concept used. After a description of the end product, the steps are described in order to reach a national risk assessment. In the following chapters, we examine the impact criteria scoring (Chapter 5), the likelihood scoring (Chapter 6) and the end product (Chapter 7).

4.1 Definition and position

In the risk assessment, the threats that have been developed in the thematic in-depth studies are measured against a yardstick based on a predefined model. The risk assessment is suitable for an all hazard approach. Scenarios for floods, pandemics and long-term failures of utility supplies, for example, and for incidents caused maliciously, are described in an unambiguous manner, backed up by figures, and aggregated. In this way, the risks to national safety and security are rendered comparable and ranking becomes possible.

The likelihood that this scenario will occur in the next 5 years is examined in the risk assessment as well as its impact on the five vital interests. The impact breaks down into a tangible component (e.g. property damage, number of victims) and an intangible component (e.g. public indignation that an – impending – event causes). The perception factor is expressly considered in the risk assessment too.

The risk assessment is then the basis for the analysis of the available capabilities and advice to the Cabinet about the capabilities to be reinforced, and therefore contains guidance for decision-making about the extra use of capabilities (in nature and scale) to tackle the threats analysed in the scenarios.

4.2 General characteristics of the method

The method that has been developed for assessing risks on a national scale presupposes that threats to national safety and security are described in the form of scenarios. Basically this is the most important information for the application of the method.

Besides being scenario-based, the method has the following characteristics that are relevant for the objective of the national safety and security strategy.

- *All types* of threat to national safety and security can be dealt with, but a number of distinctions need to be made between 'natural' threats ('hazards', in the form of flooding, for example) and those triggered by humans, 'malicious' threats ('threats', in the form of terrorist attacks, for example);
- The method is *scientifically sound*, and consists of a combination of tried and tested sub-methods on the one hand, and new elements on the other, developed to meet the requirements (including uniformity and comparability) of the national risk assessment;
- the method is as *transparent* as possible, seeking a balance between comprehensibility and simplicity on the one hand, and on the other hand the capability to facilitate what is, in itself, a complex assessment;
- An analysis of the *sensitivity* of the results to changes in seriousness (e.g. lower and upper limits of scores on impact and likelihood) and importance (different perspective of the importance of the impact criteria) is a component of the NRA;
- the method offers the ingredients and the method to rank scenarios from a multi-disciplinary perspective by risk, leaving scope for *administrative input* about what is considered more or less important and for other aspects of policy judgement;

In particular because of the scientific basis and the transparency, but potentially also because of characteristics that are potentially subject to criticism, the method was subjected several times during its development to a review.[1] These reviews lead to improvements. Actual application to 'real' scenarios also led to further fine-tuning. The method can be further developed in future too.

The following issues are dealt with in sequence in the remaining paragraphs of this chapter:
- an explanation of the concept of 'risk' and the way in which the method in general deals with it;
- a summary of the steps that have to be gone through to apply the method; these steps are then each explained in a separate chapter.

4.3 The concept of risk

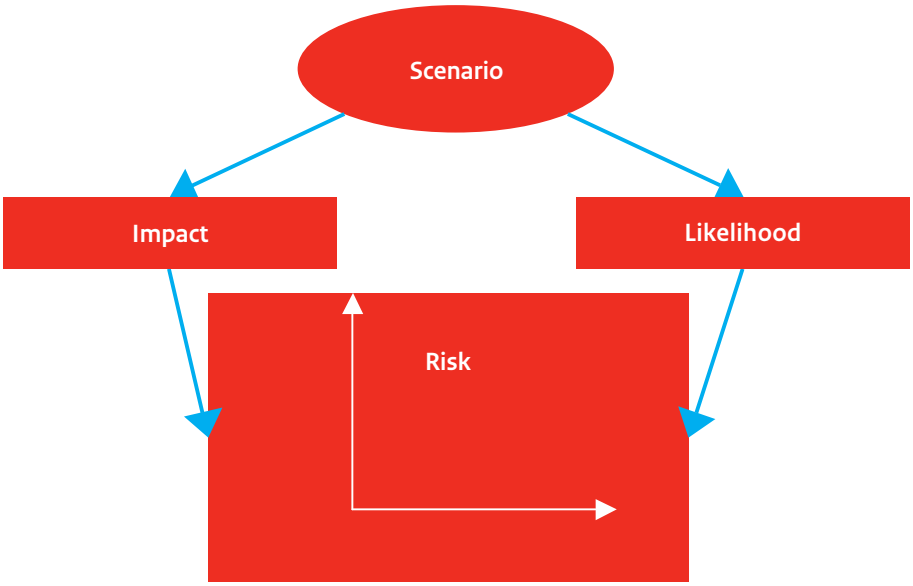
The method is oriented towards an assessment, and then ranking of risk. Because each scenario has a specific risk type (of a certain scale and with a certain impact), the method is therefore oriented towards and assessment and then ranking of the selected scenarios.

The concept of 'risk' is defined as a composition of the 'impact' (total of the consequences of the incident scenario) and 'likelihood' (a forecast about the occurrence of the incident scenario). Actions or counter actions that have already been taken, or the society's resilience are discounted in the impact and/or likelihood assessment. We deliberately avoided the traditional 'risk is likelihood times consequence', because this tends to suggest a strictly quantitative interpretation and because reducing 'risk' to a single number conceals two fundamental dimensions. Furthermore, it can be argued that in our risk assessment, impact and likelihood are not always weighed equally, although this is an assumption underlying the formula 'risk is likelihood times consequence'.
It is often difficult to estimate the likelihood of occurrence based on historic data, because there is none, or because circumstances are not comparable, or because the incident scenario consists of a complex totality of events. In particular, incidents caused deliberately frequently require a qualitative assessment of probability based on 'intelligence'. Quantifying the consequences of an incident is also often impossible because not everything can be expressed in money terms (especially damage to national reputation) or because there is a lack of data, or that data is not sufficiently reliable.

Figure 4-1 indicates that the assessment of impact and probability initially happens separately, described in Chapters 5 and 6 respectively. After the scenarios have been assessed for these two risk components, they are merged, and an overall picture of the various types of risk is created (Chapter 7).

[1] On 20 July 2007, a review was undertaken by experts including from TNO, RIVM, KIWA, VU, Stichting Impact and RPB. On 2 November 2007, a review was held, specifically for the criterion of psycho-social impact. Participants were drawn from institutions such as University of Twente, VU, University of Tilburg, Stichting Impact, BZK-ERC, SCP, RIVM. Furthermore, the method was submitted to different types of experts: including on 10 January. 2008, during the 19th International Conference on Multiple Criteria Decision Making, to international experts in the field of multicriteria analysis, on 29 January 2008, during the National Safety and Security Congress, to international experts on National Security, and on 13 May 2009, during the WRR Onzekere Risicos Congres to Dutch uncertainty and risk experts.

Figure 4-1: Each scenario is assessed on the two risk components



4.4 Products, quality requirements and coherence

Products

The end product of the risk assessment components is a report including the following components, plus their supporting evidence:

- a brief description of the scenarios devised;
- a brief description of the risk assessment method used;
- the scores (i.e. the impact and likelihood values calculated) of the scenarios used in the risk assessment;
- risk diagram(s) showing the scores of all scenarios along an impact and a likelihood axis;
- a sensitivity analysis.

4.5 The steps in the method

The risk assessment comprises the following methodological steps, on the assumption that the scenario development has already been done:

- **Check on completeness of the scenario description;**
  The scenario must contain the information enabling assessment of the impact and the likelihood.
- **Assessment of the impact of the scenario;**
  Each scenario is analysed and assessed on ten impact criteria. These impact criteria are directly related to the five vital safety and security interests. The individual impact scores are merged into a final score per scenario of the impact.
  The multi-criteria analysis necessary for this step in turn requires a number of steps that must be gone through. These are addressed in Chapter 5.
- **Assessment of the likelihood of the scenario;**
  Each scenario is analysed and assessed for likelihood that it will happen. In doing so, a distinction is made between scenarios describing a natural form of hazard (assuming that historic data is available to some extent), and scenarios describing a threat caused deliberately (and where it is plausible that an assessment of likelihood must be based mainly on intelligence and forecasts). The likelihood is expressed qualitatively to the minimum extent, and wherever possible quantitatively. The line of reasoning that is adopted is described in Chapter 6.

- **Assessment of the risk of the scenario;**
  Assessments of the impact and likelihood of all scenarios are brought together in a two-dimensional risk diagram. Sensitivity analyses are used for this because a high level of subjectivity is involved in the assessment of probability, the level of impact and the relative importance of the various types of impact. This works through to the risk diagram and the assessment of the total risk, which is described in Chapter 7.
- **Presentation of the analysis result.**
  Despite the aggregated character of the risk, attention must be paid to the underlying findings. These involve in any case identification of the main 'impact drivers' per scenario and an indication of the robustness of the final score on impact.

Key areas requiring attention and tips for the use of expert opinion for carrying out risk assessment can be found in Appendix A.

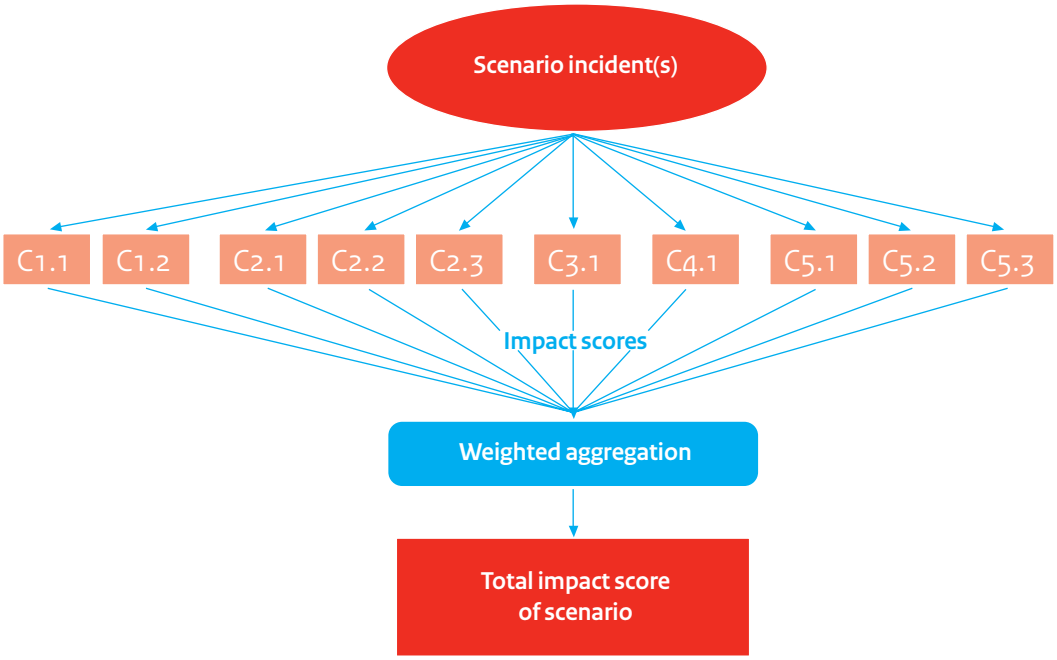
5 Impact assessment and aggregation

In this chapter, the 10 impact criteria are first introduced and the methodology of scoring the 10 impact criteria is explained. Then comes an explanation of the 10 impact criteria and information concerning the scoring. Finally, we look at the calculation of the impact and the calculation method used.

5.1 General profile – character of the impact criteria

The chosen impact criteria for the national risk assessment are an immediate reflection of the objective of the National Safety and Security Strategy: protection of the vital interests of the Netherlands. Each of the five vital interests is converted into between one, and a maximum of three, impact criteria. The ten chosen criteria are jointly considered representative for being able to assess and rank every possible incident scenario based on impact (damage, loss, cost, etc.)

Figure 5-1: the steps to reaching an overall impact score



The 10 impact criteria belonging to the five vital interests are shown below.

Vital interest	Impact criterion
1. Territorial safety	1.1 Encroachment on the territory of the Netherlands 1.2 Infringement of the international position of the Netherlands
2. Physical security	2.1 Fatalities 2.2 Seriously injured and chronically ill 2.3 Physical suffering (lack of basic necessities of life)
3. Economic security	3.1 Costs
4. Ecological security	4.1 Long-term impact on the environment and on nature (flora and fauna
5. Social and political stability	5.1 Disruption to everyday life 5.2 Violation of the democratic system 5.3 Social psychological impact

The following steps lead to an impact score for a scenario:
- the events and the impact in the scenario are analysed against each of the ten impact criteria;
- this analysis leads to the determination of an impact score (label) per impact criterion;
- the ten individual impact scores are merged using an aggregation procedure into an overall impact score; this is done in a number of ways which differ from each other in the method of weighting the importance of the criteria and the labels.

The impacts on the different criteria are measured in the same way for all potential incident scenarios. Example: for the measurement (estimation) of the encroachment on the territory of the Netherlands (1.1), it does not matter whether the Netherlands loses authority over Limburg for two months due to an occupation by a foreign power, or because the river Maas bursts its banks and all of Limburg is under water for two months. Both incidents are assessed in the same way for this criterion (1.1). The difference in assessment of both incidents is expressed in the difference in the assessment of the other impact criteria (for example, violation of the democratic system, damage to the environment or social psychological impact).

5.2 The interpretation of the impact scores

For each of the ten criteria, the impact is rendered measurable by using five categories:
A – B – C – D – E.

These are classified as follows:

A	Limited consequences
B	Substantial consequences
C	Serious consequences
D	Very serious consequences
E	Catastrophic consequences

Each category is characterised by a range (e.g. 0 to 10 fatalities). In all cases, the ratio between successive categories should as far as possible be kept equal. If numbers are used, then if possible a fixed factor should be used (in the case of duration, approximately a factor of 5, in the event of quantities or area, a factor of 10).

It is possible that impact criteria do not apply at all to a specific incident scenario. In this case, the category score is marked 'X'. Here are two examples to clarify the difference between category X and category A:
- a terrorist attack on persons or property in general has no influence on environmental safety. Therefore, for the criterion of long-term impact on the environment and nature (flora and fauna) (4.1), the value 'not applicable' would be assigned (instead of classification in category A, which also contains a 'zero' value). The consequence of this is that this impact criterion is completely ignored.
- A major riot leads to a number of people being seriously injured, but no fatalities. The value for fatalities is A (0 to 10 fatalities) instead of X ('not applicable'), because in theory, this incident could cause deaths. So it does apply, but in this specific scenario, is assigned a zero value, which leads to the value A being assigned.

If more than one value label from the label assignment matrix are used, then the highest value of each of the labels that are assigned individually should always be taken as the one to be used .

A table is given for each criterion. In this table, the following values need to be entered:
- V (forecast value: it is most probable that it falls in this box, but could be more or less)
- O (lower limit: it will almost certainly be equal to or greater than O) and
- B (upper limit: it will almost certainly be equal to or less than B).

The V, B, and O can be in the same box if the lower limit and upper limit are close to the forecast value.

Example

Area → / Time period ↓	Local Max. 100 km² (<0.25% of area)	Regional 100-1,000 km² (0.25-2.5% of area)	Provincial 1,000-10,000 km² (2.5-25% of area)	National > 10,000 km² (>25% of area.)
2 to 6 days;				
1 to 4 weeks	O	V		
1-6 months		B		
½ year or longer				

The reason for choosing particular values must be given. This must be consistent with the narrative. Three values must be given: A lowest possible value (O), a maximum value (B) and the forecast value (V). This additional information is used to provide greater certainty about the results (sensitivity analyses). The reasons may be given in a separate appendix.

5.3 The impact criteria – definition, score matrices

The 10 impact criteria are described below, and it is stated how each impact criterion can be scored. The appendix provides a format in which the scores associated with a specific scenario can be interpreted.

For a correct score, and to substantiate the impact, it is important to assess whether vital infrastructure is harmed, and to what extent this occurs (time, number of people). This is particularly relevant for determining economic damage/cost and for the impact on everyday life.

In the table below, it should be indicated which of the vital products/services below is harmed in the scenario (failure, 1st and 2nd order effect). This summary must then be related to the scoring of the various impact criteria.

- ☐ Electricity
- ☐ Natural gas
- ☐ Oil & fuels
- ☐ Telecommunications (fixed and mobile)
- ☐ Internet access
- ☐ Radio and satellite communication and navigation
- ☐ Postal and courier services
- ☐ Broadcasting
- ☐ Drinking water supplies
- ☐ Food supplies/safety
- ☐ Emergency care/other hospital care
- ☐ Drugs, sera and vaccines
- ☐ Management of water quality
- ☐ Controlling quantity of water
- ☐ Maintenance of public order
- ☐ Maintenance of public safety
- ☐ Administration of justice and detention
- ☐ Law enforcement
- ☐ Diplomatic communication
- ☐ Information provision by government
- ☐ Armed forces
- ☐ Main airport Schiphol
- ☐ Main port Rotterdam
- ☐ Main roads and main waterway network
- ☐ Railways
- ☐ Transport, storage and production/ treatment of chemical and nuclear materials
- ☐ Government financial payments
- ☐ Payments traffic/payments structure

5.3.1 Territorial safety

'Undisrupted functioning of the Netherlands as an independent state in the broadest sense, or territorial integrity in the strict sense.'

Criterion 1.1 Encroachment on the territory of the Netherlands

'The actual or functional loss of, or the loss of use of, or the loss of authority including parts of the Kingdom of the Netherlands and territorial waters (including overseas territories).' [2]

Functional loss is mainly deemed to mean the loss of the use of buildings, homes, infrastructures and land.

Examples of potential threat triggers are: rivers bursting their banks, terrorist attack in the Netherlands, secession of a region, outbreak of animal disease, attack by foreign power, damage or loss of authority over and/or possession of Dutch embassies, chemical/biological/nuclear contamination.

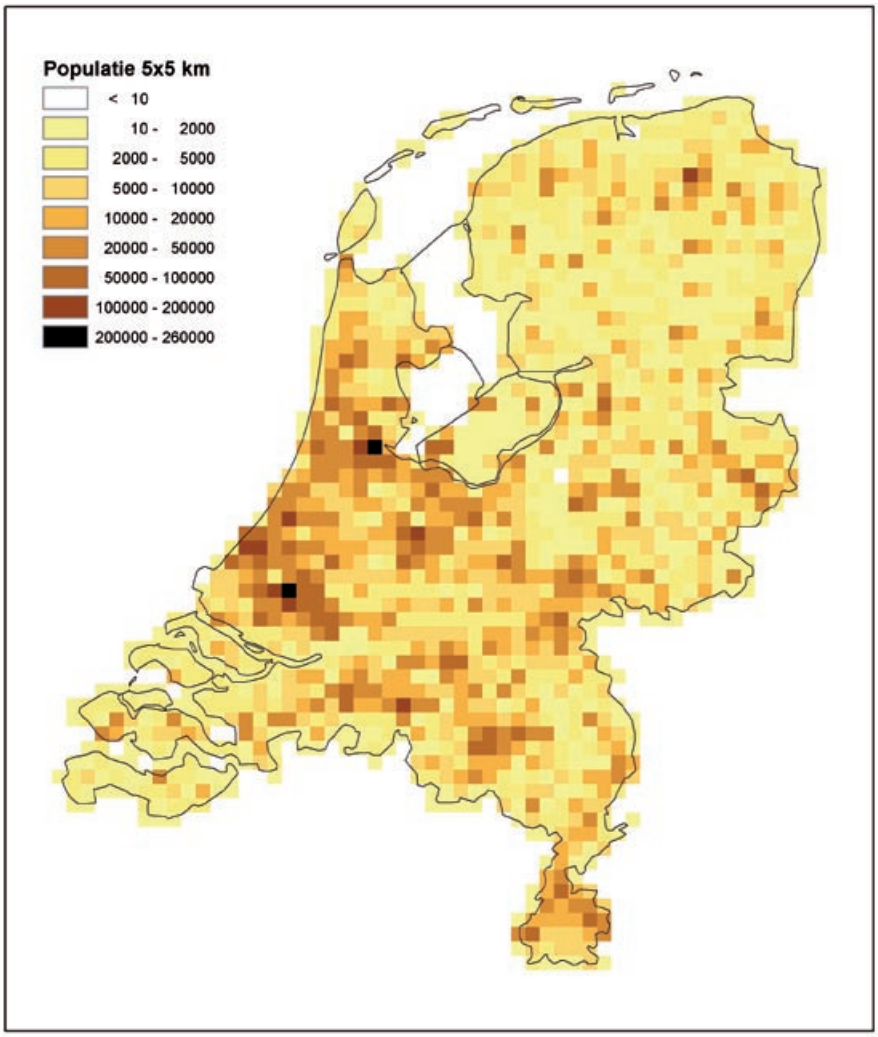
The following are used as indicators for measuring impact:
- the area of the territory at risk or affected (geographical demarcation);
- the period of time for which the region is at risk or affected;
- the population density of the region concerned.

area → / time period ↓	local max. 100 km² (< 0.25% of area)	Regional 100-1,000 km² (0.25% - 2.5% of area)	Provincial 1,000 – 10,000 km² (2.5% - 25%of area)	National > 10,000 km² (> 25% of area)
2 to 6 days;	A	A	B	C
1 to 4 weeks	A	B	C	D
1 -6 months	B	C	D	E
½ year or longer	C	D	E	E

The result of the impact score may be corrected based on the population density in the threatened or affected area:
- if population density > 750 persons/ km² then +1 (e.g. B becomes C)
- if population density < 250 persons/ km² then -1 (e.g. D becomes C)

[2] At present, the scenarios and analyses are mainly focused on the Netherlands. This criterion is the exception, as it covers the territory of the Kingdom of the Netherlands and territorial waters (including overseas territories).

A map with population densities in the Netherlands is shown below (source RIVM).



Criterion 1.2 Infringement of the international position of the Netherlands

'Harm to the image or influence or actions of the Netherlands abroad.'

Examples of potential threat triggers are: terrorist attack on embassy(ies), collapse of international organisation(s), Srebrenica scenario, increasing number of Dutch people misbehaving abroad, statements by Dutch people or Dutch media that are regarded by groups as (extremely) inflammatory.

There can be other causes that can have a negative effect on the workings of Dutch embassies and representations abroad: floods, diseases, other accidents without malicious acts. In these cases (possibly serious) nuisance could be caused, but the integrity of the international position or influence of the Netherlands would not be harmed. Usually, other embassies (of friendly countries and/or organisations) would take over their tasks temporarily. These cases do not give rise to a relevant impact score for this criterion, but might under criterion 1.1.
Conversely, these causes could lead to a relevant impact score if these events take place in the Netherlands, and therefore affect foreign embassies and representations. This could influence the image of the Netherlands.

There are several indicators for interpreting this criterion. They are divided into categories as follows:

1 Actions
- demonstrations aimed against the Netherlands/EU/NATO/The West;
- threats against embassies/representations (including property and/or staff) and/or other targets belonging to the Netherlands/EU/NATO/The West;
- negative publicity and/or hate campaigns in the media and/or on websites against the Netherlands/EU/NATO/The West;
- pronunciation of one or more 'fatwa's' against influential/important people in the Netherlands/EU/NATO/The West.

2 Political relations
- expulsion of diplomats and/or termination of diplomatic relations with Netherlands/EU/NATO/The West;
- refusal or cancellation of important visits by representatives of the Netherlands/EU/NATO/The West to other countries, or by foreign representatives to the Netherlands/EU/NATO/The West;
- formation of a bloc against the Netherlands/EU/NATO/The West.

3 Non-political relations (NB: the financial loss of this falls under criterion 3.1)
- boycott of goods from the Netherlands/EU/NATO/The West;
- refusal or cancellation of trade agreements and other commercial treaties with the Netherlands/EU/NATO/The West;
- boycott of cultural events (e.g. performances, exhibitions, sport) organised by the Netherlands/EU/NATO/The West abroad, or in the Netherlands/EU/NATO/The West by other countries;
- refusal or cancellation of cultural agreements with the Netherlands/EU/NATO/The West;
- declining tourism to the Netherlands/EU/NATO/The West.

The classification is based on:
- the number of indicator categories that are applicable;
- the number of indicators per relevant category that are applicable;
- the seriousness with which the indicators are affected.

The gradation 'limited' applies if, per relevant category, a maximum of one indicator applies, and this indicator is not applicable to a serious extent.
The gradation 'considerable' applies if, across all the relevant categories, more than half the individual indicators mentioned apply, irrespective of the seriousness.
The gradation 'average' applies to the other (intermediate) cases.

Number of indicator categories → / extent ↓	max. 1 indicator category	max. 2 indicator categories	max. 3 indicator categories
limited	A	B	C
average	B	C	D
considerable	C	D	E

5.3.2 physical safety

'Undisrupted functioning of the people of the Netherlands and their environment.'

Loss of life is measured, as is physical or mental trauma, and suffering of victims. This interest is expressly interpreted as physical or mental; these kind of effects can also restrict social functioning. Expressions of human emotions such as anger, worry and grief fall instead under criterion 5.3 provided that they are not the result of illness(es).Prevention of participation in (social) interaction as a result of impediments imposed from the outside (e.g. closures, bans, blockades), fall under criterion 5.1.

Criterion 2.1 fatalities

'Fatal injuries, immediate or premature death within a period of 20 years.'

Examples of potential threat triggers are: accident at chemical plant, large-scale dyke failure, terrorist attack, outbreak of an epidemic, large scale riots.

The following are used as indicators for measuring impact:
the number of deaths as a consequence of the incident;
the time of death.

number → / time ↓	< 10	10-100	100-1,000	1,000-10,000	> 10,000
Immediate death (within 1 year)	A	B	C	D	E
Premature death (within 2-20 years)	A	A	B	C	D

if both categories are applicable, the score for the higher impact category applies.

Criterion 2.2 Seriously injured and chronically ill

'Injury cases belonging to category T1 and T2 [3], and people with long-term or permanent health problems such as respiratory conditions, serious burns ors skin complaints, hearing damage or post-traumatic stress disorder. Victims belonging to category T1 or T2 must be given immediate medical assistance and treatment within 2 hours (T1) or must be continuously monitored and treated within 6 hours (T2).
Chronically ill people are those who experience restrictions for a long period (> 1 year): need medical assistance, cannot be part, or only to a limited extent, of the labour market, experience restrictions in their social functioning.'

If, after an incident, a number of victims belonging to category T1 or T2 cannot be given adequate assistance within 2 hours (T1) or within 6 hours (T2), since they cannot be reached by emergency services or due to lack of appropriate facilities, that number should be considered as 'immediate deaths', and included in that category. In the description of the scenario, it must be indicated how many victims come under categories T1 and T2, even if they die due to the lack of prompt assistance, because this is a point requiring action in the strategic planning.

Examples of potential threat triggers are: accident at chemical plant, terrorist attack with biological or chemical weapons, large-scale rioting, Srebrenica-scenario.

The number of chronically ill and seriously injured people is taken as an indicator for measuring the impact.

Number	< 10	10-100	100-1,000	1,000-10,000	> 10,000
	A	B	C	D	E

[3] T1 and T2 are triage categories from emergency medicine procedures

Criterion 2.3 Physical suffering (lack of basic necessities of life)

'Exposure to extreme weather and climatic conditions, as well as the lack of: food, drinking water, energy, shelter or other basic necessities of life'.

Examples of potential threat triggers are: terrorist attack on drinking water supply or energy supplies, release of radiation as a result of a disaster at a nuclear reactor, natural disaster.

The following are used as indicators for measuring impact:
- number of people affected;
- time period.

number → / time period ↓	< 10,000 people	< 100,000 people	<1,000,000 people	>1,000,000 people
2 to 6 days;	A	B	C	D
1 to 4 weeks	B	C	D	E
1 month or longer	C	D	E	E

5.3.3 Economic safety

'Undisrupted functioning of the Netherlands as an effective and efficient economy.'

Criterion 3.1 Costs

'Euro in terms of repair costs for damage sustained, extra costs and loss of income.'

Examples of potential threat triggers are: large-scale flows of refugees, pandemic with massive numbers on sick leave, contagious animal diseases (foot and mouth disease), armed conflict in region from which the Netherlands obtain raw materials, large-scale failure of payments systems, collapse of financial markets.

The following are used as indicators for measuring impact:
- damage to property and costs;
- health damage and costs;
- financial losses and health costs;
- costs of combating the incident, providing assistance and repair.

Impact is based on the total loss sustained in money; the losses in the individual categories 1-4 are added together.

Costs in €	< 50 million	< 500 million	< 5 billion	< 50 billion	> 50 billion
	A	B	C	D	E
1. damage to property					
2. health damage					
3. financial loss					
4. cost of combating the incident and repair					
Total economic loss					

Explanation of the individual indicators for damage and costs of an incident:

1 damage to property
- damage to buildings, homes and infrastructure objects;
  valuation concept: rebuilding value (including clean-up costs)
- damage to inventory, machinery, plant, vehicles, stocks; loss of livestock
  valuation concept: replacement value
- Reconstruction costs of (ICT) data files.
  Costs: total cost of using administrative/ICT employees

2 Health damage
- costs of paying death benefit;
- extra health care costs;
  Cost factors
  - gross cost of hospital admission (including treatment and ambulance)
  - long-term care in nursing homes, convalescent clinics
  - possible correction for reduction in normal demand for health care if the health care system is operating at full capacity
- Extra costs of incapacity for work and (surviving) relatives pensions
  Cost factors
  - *payment of incapacity benefit to victims;*
  - *(early) retirement pensions to (surviving) relatives*.

3 Financial loss
- Business interruption costs as a consequence of property damage and/or labour shortage and/or unusable premises; repair period is the yardstick for duration of commercial loss.
  Valuation concept
  - *net value-added (excluding depreciation)*
  - *gross value-added - employee absences, unusable premises*.
- Consequentials business interruption costs as a result of lack of demand or of supply (equipment, raw materials, energy supplies); or failure of communications/transport/utility services;
  Valuation concept
  - *gross value-added, possibly with correction for substitution effects (replacement demand or new demand)*
- Direct financial loss as a result of claims, fines or 'expropriation' (e.g. nationalisation of company), or direct financial losses to private individuals (e.g. compulsory purchase of home).

4 Cost of controllting the incident
- Extra costs of using operational services to controll the incident, emergency aid, accommodation and evacuation;
  Costs
  - *total cost of operational services*
- Clean-up and repair costs as a result of damage to nature and the environment.
  Costs
  - *total cost of using repair workers*

The following indicators can be used when estimating costs

Indicators for estimating costs of economic security

Damage to property

Homes (including contents):		Infrastructure objects:	
Low/medium/high-rise	€ 170,000	pumping station	€ 750,000
single-family house	€ 240,000	sewage plant	€ 10,000,000
farmhouse	€ 400,000	bridge, viaduct	€ 5,000,000
offices	€ 100-200,000 /m²	railway line	€ 1.350,000 / km

Health damage

- costs of health care permanent incapacity for work/seriously injured € 100,000
- costs of health care, half-year incapacity for work/slightly injured € 5,000
- incapacity benefit (permanent, average income, 38 yrs.) € 650,000
- death benefit (average income, 38 yrs., 2 children;) € 160,000
- (based on actuarial models)

Financial loss

- ratio of direct operating loss versus indirect operating loss 2:1 (based on discussion note Public Works Dept. HIS-SSM)
- € 550 per m² of business premises per year (based on Gross Domestic Product)

Concepts:

- replacement value of capital goods: 'new value of capital goods minus depreciation' at the time of the incident
- Gross value-added: 'contribution of capital and labour (equal to fixed costs plus profit)' during repair period
- Net value-added 'gross value-added minus depreciation' during repair period

5.3.4 Ecological security

'Undisturbed continued existence of the natural environment in and around the Netherlands.'

Criterion 4.1 Long-term impact on the environment and on nature (flora and fauna).

'Long-term or permanent harm to the quality of the environment, including air, water or soil pollution, and long-term or permanent disruption of the original ecological function, such as the loss of biodiversity of flora and fauna, loss of special ecosystems, invasion by foreign species.'

Examples of potential threat triggers are: incidents where large amounts of (eco)toxic substances are released into the environment, such as an accident in a chemical plant or in a nuclear reactor, an oil spill on the North Sea, or an armed conflict with use of nuclear, biological or chemical weapons; incidents where natural areas are exposed to major physical damage, for example due to fire, incidents that are a consequence of climate change such as disruption in the management of surface water (floods) and the consequences thereof (such as silting of the bed), freak weather (tornadoes).

Harm to ecological security/safety is measured using two aspects:

A. harm to designated wildlife and scenery conservation areas, and
B. harm to the environment in the broad sense, even outside designated wildlife and scenery conservation areas.

N.B.: For the scoring of harm to ecological safety/security, both impact criteria must be assessed and the scores shown on the tables. The highest scoring impact is deemed to be the impact for criterion

4.1. Both impact scores will be taken into consideration for exploring the actions to be taken, and the capabilities required. Therefore, it is necessary that data for both impact criteria be provided and justified.

A Impact on wildlife and scenery (flora and fauna)

Harm to designated wildlife and scenery conservation areas (subsequently referred to as 'nature areas'), where an 'all or nothing' effect is assumed: where the harm occurs, ecosystems can be lost. A distinction is made into three types of nature area that differ from the policy viewpoint: nesting grounds of meadow birds ('high nature value farmland'); the National Ecological Network sites (EHS): which are National Ecological Network sites except those that also belong to Natura 2000, which are subsequently referred to as 'National Ecological Network areas' and the nature areas designated in the Natura 2000 regulation, also designated as 'Natura 2000 areas'. For an overview of the three types, see the maps in figures 5.2 and 5.3.

Fig. 5-2: Overview of the nesting grounds of meadow birds, known as 'high nature value farmland'. These nesting grounds of meadow birds are shown on the map in dark blue and green

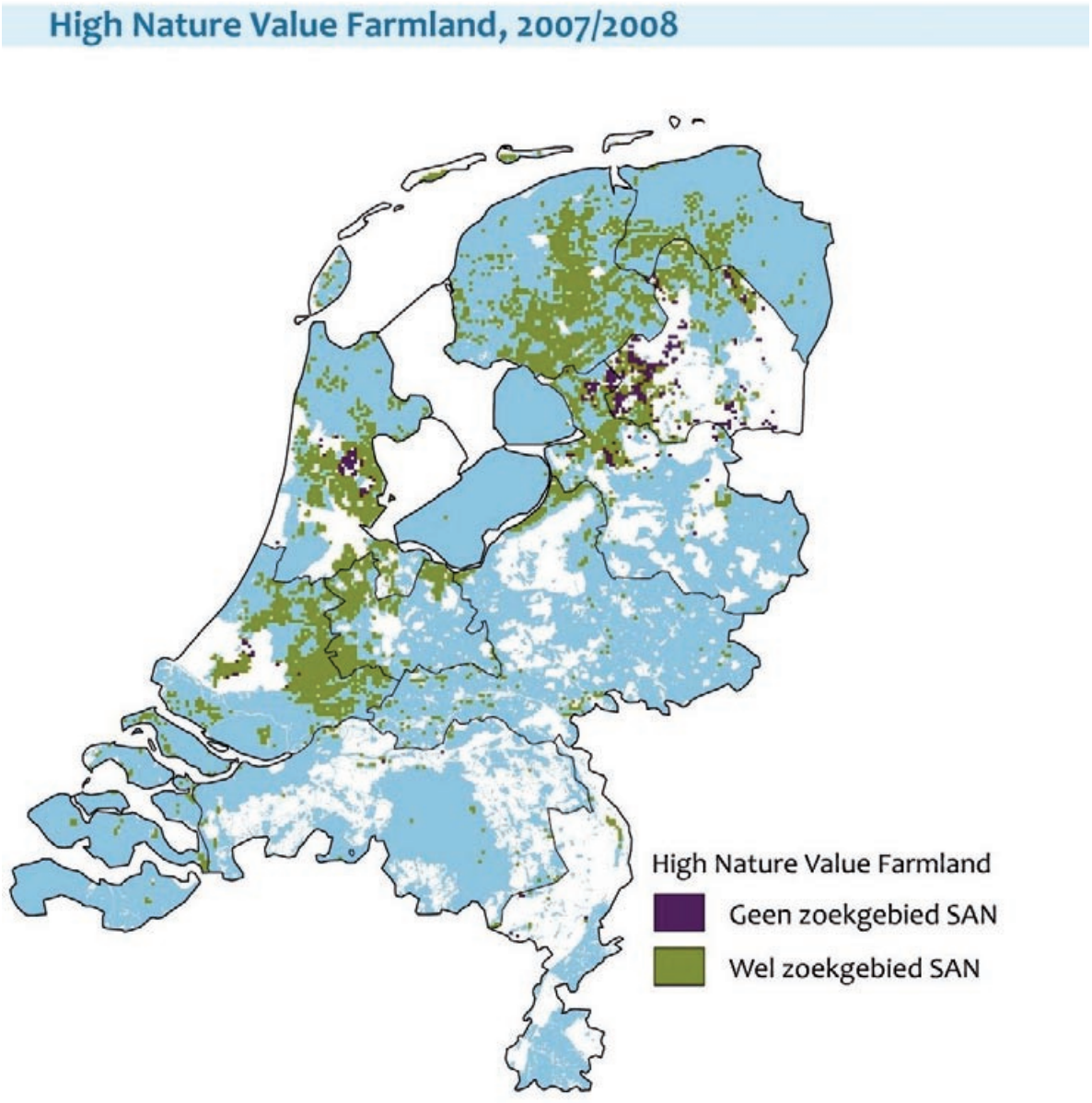
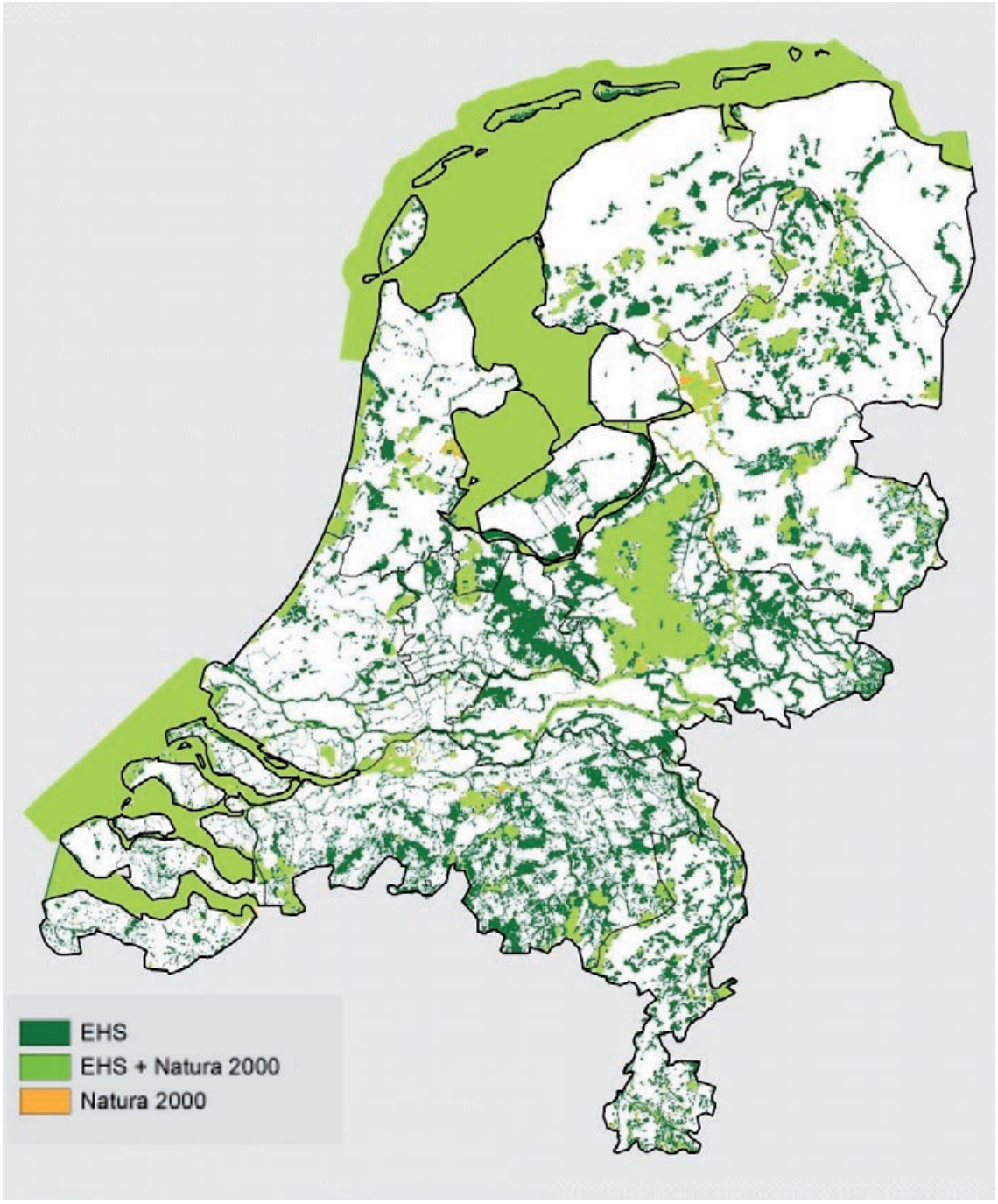


Fig. 5-3: Overview of the National Ecological Network areas (EHS)), excluding the Natura 2000 areas (shown on this map in dark green); and the Natura 2000 areas, whether they belong to the National Ecological Network or not (shown on this map in light green and orange).



The harm to nature areas must be defined as the actual damage caused: *the loss of a nature area that belongs to one of the three types mentioned*. The fact that a nature area is lost, counts as a consideration, the seriousness of the loss is expressed using the type of nature area that has been lost, and the size of the area lost. Another factor that plays a role in determining the seriousness of the harm is the duration of the harm. In addition, there is a consideration in relation to harm to the Waddenzee, a nature area with a unique role.
Considerations about the nature and potential value of an ecosystem that may be created after the incident have no role to play: considerations that 'for a lost ecosystem, another one will take its place' are left aside from this discussion.

The following are used as indicators for measuring impact:
- Type of nature areas that lie in the affected zone: Whether the zone affected contains nature areas that belong to the nesting grounds of meadow? birds, to the National Ecological Network (EHS) or to Natura 2000. Harm to such areas is considered to have greater seriousness and in that sequence.
- Relative area of the zone affected: for each of the types, it must be determined what percentage of the total area present in the Netherlands is affected.[4].
- Duration of the harm: the harm is only scored if it is expected to last for more than a year. If it is estimated that the duration will not exceed a year for any of the types, this impact criterion is scored as not applicable.

Relative size → / Policy category ↓	<3%	3-10%	>10%
Nesting grounds of meadow? birds	A	B	C
National Ecological Network (EHS) areas	B	C	D
Natura 2000 areas	C	D	E
Waddenzee	C	D	E

If the harm is expected to last longer than 10 years, then the seriousness of the impact must be scored one step higher.
The Waddenzee is regarded as being of unique importance, since it has a function as a breeding ground for marine life. For this area, the matrix row of Natura 2000 areas applies, i.e.: 3% and 10% of the Waddenzee is equal to 7200 ha (8.4 x 8.4 km) resp. 24,000 ha (15 x 15 km).
For harm to two or more of the policy categories mentioned, the highest label value of the individual labels is used.

B Impact on the environment in the general sense, (even outside the aforementioned wildlife and scenery areas)
Harm to the environment in the general sense will generally lead to impacts that should be scored under one or more of the other impact criteria. Examples are:
- If the harm is so serious that it involves a functional loss of the area concerned, then this comes under impact criterion 1.1.
- Impact of chemicals released on public health: fatalities, chronic illnesses, physical suffering comes under impact criterion 2.
- A large number of environmental impacts which are classified under impact criterion 3; for example, this applies to costs of/for:
  - rehabilitation work on environmental damage;
  - evacuation of people and animals (farm animals and pets) as a consequence of environmental impacts;

4 In this regard, the following values apply: for nesting grounds of meadow birds: 3% = 7500 ha (8.5 x 8.5 km), 10% = 25,000 ha (15 x 15 km); for National Ecological Network (EHS) sites: 3% = 10,400 ha (10 x 10 km), 10% = 43,710 ha (21 x 21 km); for Natura 2000 sites: 3% = 8,750 ha (9 x 9 km), 10% = 29,000 ha (17 x 17 km).

- loss of usability of the environment for agriculture, livestock farming, fisheries and for 'ecosystem services;'
- loss of other 'uses' of the environment, such as availability of surface water for water purification, recreational functions (for example swimming water, tourism)

• Harm to the environment which can have a disruptive effect, e.g. with an impact on air quality, and which means that (some groups of) people can no longer move around freely outdoors (impact criterion 5.1)

In the scenario, specific attention must be paid to these considerations.

Within the impact criterion ecological security, attention must also be paid to harm to the environment.
Serious harm to the environment is if:
• the harm occurs for a period of at least one year; and
• the harm has an intervention value that applies for a chemical contamination incident.
The seriousness of the impact is scored using the absolute area of the zone affected.

Absolute area	local (max. 30 km^2)	regional (30 – 300 km^2)	provincial (300 – 3,000 km^2)	National (> 3,000 km^2)
	A	B	C	D

For permanent damage to the environment (< 10 years), these scores must be increased by 1 step.

5.3.5 Social and political stability

'Undisrupted continuing existence of a social climate in which individuals can function undisturbed and groups of people can live together peacefully within the framework of the Dutch democratic constitutional state and shared values.'

Criterion 5.1 Disruption to everyday life

'Harm to freedom of movement and association in public places and in public areas, whereby participation in normal social intercourse is hindered.' Participation in social intercourse in the context of this criterion is inhibited by external factors, such as shops or utilities being closed, a ban on going outside, blockades, etc.. If harm (physical, mental) to a person's own health is presenting participation in social intercourse, that comes under criterion 2.2.

Examples of potential threat triggers are: harm to critical infrastructure such as electricity outages, mass deaths among the population due to pandemic, occupation, large-scale riots, breaches of dykes, terrorist attack, large scale influx of refugees.

The following five indicators are used for measuring impact:
• not being able to attend school;
• not being able to go to work;
• not being able to use public amenities such as those for sports, culture or health care;
• reduced accessibility due to roads being blocked and absence of public transport;
• not being able to make essential purchases due to shop closures

These indicators are assessed on the basis of:
• number of people affected;
• time period;
• number of indicators applicable.

number → time period ↓	< 10,000 people	< 100,000 people	< 1 million people	> 1 million people
1-2 days	A	A	B	C
3 days to 1 week	A	B	C	D
1 week to 1 month	B	C	D	E
1 month or longer	C	D	E	E

The result of the impact score is corrected based on the number of indicators applicable:
- in the case of maximum 1 indicator applicable, then -1 (e.g. D becomes C);
- in the case of at least 3 indicators applicable, then +1 (e.g. B becomes C).

Criterion 5.2 Violation of the democratic system

'Harm to the workings of the Dutch government and its institutions, and/or harm to rights and freedoms and other key values associated with Dutch democracy and laid down in the Constitution.'

This criterion concerns disruption to the nature (i.e. democratic rights and freedoms), character and the workings (institutional processes and policy, administrative and executive organisations) of a democratic Netherlands.

Examples of triggers for threats: disruption of the demographic structure of society, disruption of social cohesion due to discrimination, creation of a parallel society, attack on Parliament, occupation by a foreign power, public hate campaigns, incitement to and/or other expressions of antidemocratic (extremist) activities and/or views.

The following six indicators are used for measuring impact:
- harm to the working of *political representation;*
- harm to the workings of the *public administration;*
- harm to the workings of the *financial system;*
- harm to *public order and security;*
- harm to *freedoms and/or rights* (religion, free speech, association, right to vote, etc,..);
- harm to accepted Dutch *values and norms* as customary in social intercourse or established by legislation.

Violation of integrity is a form of violation of the workings of society.

The classification is based on:
- the number indicators applicable;
- the time period;
- the extent to which an indicator is violated;

number indic. → time period ↓	max. 1 out of 6 indicators	max. 2 out of 6 indicators	≥3 out of 6 indicators
Days	A	B	C
Weeks	B	C	D
Months	C	D	E
1 or more years	D	E	E

The result of the impact score is corrected, on the basis of the degree of harm, by an indicator: if an indicator is affected by more than 50%, then +1 (e.g. C becomes D).

Criterion 5.3 Social psychological impact

'Behavioural reaction by the population, which is expressed in fear and anger, sorrow or disgust, and which is covered by the media. These expressions can come from people directly affected, and from the rest of the population, and must be perceptible (i.e. audible, visible, readable).'

Behaviour that expresses fear can be, for example running away or avoidance behaviour, actions that deviate from the normal pattern, the taking of manifestly ill-advised decisions.
Behaviour that expresses anger concerns, for example, protests, demonstrations, disturbance of public order, vandalism, broadcasting via the media (partly fed by media coverage) of feelings of alienation.
Fear and anger combined with distress and disgust can lead to panic and mass hysteria.

Examples of potential threat triggers are: terrorist attack, political assassination, kidnapping, hostage-taking or attack on political leaders, members of the royal family, dominance of an undemocratic political party, coup d'état, explosion at a nuclear power station, pandemic with massive numbers of deaths.

There are a number of indicators underlying the above-mentioned phenomena. These are the 'drivers' (decisive indicators) of fear and anger. The scoring mechanism is based primarily on two factors – the applicability of these drivers and the intensity of their application. In addition to this, the scale of the perceptible expressions is used as a reinforcing or mitigating mechanism.

The indicators are divided into three categories: the perception of the incident, the pattern of expectations relating to the incident, and the possibilities for taking action. These indicators contribute in equal measure to anger or fear, or sometimes both. Despite the different number of indicators per category, the categories are each considered equally important. The categories partly overlap, and will therefore frequently occur in combination.
The three categories consist of the following indicators:

1 Perception of the incident among the people affected and among the rest of the population:
   - unfamiliarity with the nature or the cause of the risk;
     ➔ this leads primarily to *fear*
     (the greater the unfamiliarity, the greater the fear);
- uncertainty about the level of threat or hazard and about the possibility that you personally may be affected by it;
     ➔ this leads primarily to *fear*
     (the greater the uncertainty about your own exposure to a threat/hazard and the perception of the scale thereof, the more worried you become);
   - extent of (unnaturalness) of the causes of the incident;
     ➔ This leads to both *fear* and *anger*
     (the more unnatural the cause and the incident itself, i.e. the more malicious the impact on people, the less resigned they are and the more worried they are about the consequences about what else will happen and the more angry they are with the perpetrators);
   - extent to which vulnerable groups – such as children, old people, sick people, the poor – are affected disproportionately.
     ➔ this leads primarily to *anger*
     (the more these groups are affected, the greater the feeling of injustice, and the more angry they become).

2 Pattern of expectations about the incident and its consequences on the people concerned and the rest of the population:

- extent of perceived blame (failure) by relevant companies and (public) bodies regarding the occurrence of the incident or the occurrence of the unwanted consequences of it (relationship to prevention);
  ➔ this leads primarily to *anger*
  (the greater the feeling that there is culpable blame, the more angry people become);
- degree of loss of trust in the response from the authorities and the companies concerned (NB not the emergency services), with regard to the control of the incident on the one hand, and provision of information about the incident and its causes on the other hand (relationship with preparation and initial response);
  ➔ This leads to both *fear* and *anger*
  (the greater the lack of this trust and appropriate information, the more angry people are about betrayed expectations and disappointment, and the more angry people are about a/the? loss of mental certainty/ stability?what is mental certainty?confidence in the government?);
- extent of loss of trust in the action of the emergency services in the management of the incident, for example in the case of response time targets not being met, capacity shortages, inappropriate/ unjust actions etc. (relationship with preparation and initial response).
  ➔ This leads to both *fear* and *anger*
  (the greater the lack of this trust, the more angry people are about betrayed expectations and disappointment, and the more angry people are about loss of mental certainty/stability??).

3 Possibilities for people affected by the incident to take action:

- degree of unfamiliarity and/or inexperience with possible forms of coping with the specific situation (forms of lack of knowledge);
  ➔ this leads primarily to *fear*
  (the greater the lack of knowledge about positively influencing their own situation, the more worried people become);
- extent of personal inability to control their own situation (forms of self-reliance).
  ➔ This leads to both *fear* and *anger*
  (the less the self-reliance, the more worried people become due to the greater feeling of dependence on others for help, and the more angry when that help is not provided in time, or precisely because they have reached this situation of dependence or it has been made impossible to act themselves).

Per indicator, it must be stated whether the indicator is applicable or not. Not applicable means that there is no logical relationship with the incident or its causes.

- If the indicator does apply (in principle), there are four intensities with which it can apply:
- 'None', i.e. the indicator is not (noticeably) present in this scenario, and therefore does not influence the creation of fear and/or anger;
- 'limited', i.e. the indicator is present to a slight extent, and if considered in isolation, is not enough for the expression(s) of fear and/or anger;
- 'normal', i.e. the presence of the indicator is clearly recognisable, and if considered in isolation, is not enough for the expression(s) of fear and/or anger;
- 'considerable', i.e. a strong presence of the indicator is recognisable, and if considered in isolation, makes a dominant contribution to the expression(s) of fear and/or anger.

The intensity to which an indicator applies can be decisive for the occurrence of fear or anger, but should not be confused with the scale of the expressions of fear and anger. The latter is only used as a correction mechanism in the second instance.

The categorisation is based on the number of indicator categories that are 'significant', and a final judgement about 'gradation' that is based on the intensity of individual indicators.

An indicator category (perception, pattern of expectations or possibilities of action) is *significant* if:
- there is at least one indicator with a 'considerable' intensity in the category,

or
- if the following two conditions are met simultaneously:
  - at least half of its indicators score a 'limited', 'normal' or 'considerable' intensity, and
  - there is at least one indicator with a 'normal' intensity in the category.

A category that consists, for example, of indicators whose application is 'limited', is not significant.

If all indicators are not applicable (N/A) or do not occur ('none') then this whole criterion scores 'N/A' (label 0).
The final judgement, the gradation, relies on certain intensities of the individual indicators not being present in the categories:
- 'low' if there are no relevant indicators with 'normal' or 'considerable' intensity;
- 'high' if one of the following two situations arises:
  - There are either two or three significant categories and these each contain one indicator with 'considerable' intensity,
  - there is only one significant category and of these, all indicators have a 'considerable' intensity;

'average' in the other cases.

number of significant categories → final gradation ↓	0 significant categories	1 significant category	2 significant categories	3 significant categories
Low	A	-	-	-
Average	A	B	C	D
High	-	C	D	E

(the lines are combinations of situations that cannot occur).

The result of the impact score is corrected:
- if the scale and duration of the perceptible expressions of fear and/or anger are low, i.e. < 10,000 people lasting max. 2 days, then -1 (e.g. C becomes B);
- if the scale and duration of the perceptible expressions of fear and/or anger point to major impact, i.e. > 1,000,000 people (in 2 or more cities) for at least one 1 week, then +1 (e.g. C becomes D).

In all cases, a maximum period of consideration of 1 month is used. After that, it is increasingly difficult to interpret behaviour, as meant under this criterion, as a direct consequence of the incident.

5.4 Calculation of the aggregate impact score: multicriteria analysis

5.4.1 Input and conversion to scores X, A, B, C, D and E

As described in section 5.3, the scenario working groups score the incident scenarios that are drawn up for various indicators to put the ten impact criteria into practice. The forecast values (and possibly the lower limits and upper limits) of these indicators are converted using matrices (see section 5.3) to ordinal scores X, A, B, C, D or E on each of the ten criteria. These ordinal scores form the input for the actual multicriteria analyses. The table below contains the forecast values of the impact scores of the 33 scenarios of the NRA 2008.

Table 5.1: input data (X, A, B, C, D, E, scores) of 33 scenarios on the ten criteria (NRA 2008)

	Crit.1.1	Crit.1.2	Crit.2.1	Crit.2.2	Crit.2.3	Crit.3.1	Crit.4.1	Crit.5.1	Crit.5.2	Crit.5.3
S01	X	X	D	C	A	D	X	B	X	E
S02	X	X	E	D	E	D	X	E	C	E
S03	X	X	C	X	A	C	A	A	X	A
S04	E	B	D	E	E	E	E	E	B	E
S05	E	B	D	E	E	E	E	E	A	E
S06	X	X	B	A	D	C	X	D	B	B
S07	X	C	A	A	D	C	X	D	B	E
S08	X	A	A	B	X	D	X	E	D	E
S09	X	A	A	A	X	A	X	B	B	C
S10	X	A	A	A	X	B	X	A	A	A
S11	X	A	A	A	X	A	X	A	X	D
S12	X	A	X	X	X	B	X	C	X	E
S13	X	A	A	A	X	A	X	A	C	E
S14	X	X	A	A	D	C	X	E	X	X
S15	X	X	A	B	C	B	X	E	X	X
S16	X	X	B	A	X	C	X	D	X	X
S17	B	A	B	B	A	D	B	E	A	E
S18	X	A	A	A	C	C	X	D	A	B
S19	X	C	B	A	E	D	X	E	E	E
S20	A	X	B	B	A	C	X	D	A	C
S21	A	X	B	B	B	D	X	E	E	D
S22	A	X	A	A	B	B	X	B	D	E
S23	X	X	A	A	X	A	X	A	E	E
S24	X	E	B	A	X	C	X	E	E	E
S25	X	A	A	A	X	A	X	D	B	E
S26	X	X	X	X	X	X	X	D	D	E
S27	X	B	A	X	X	B	X	X	A	E
S28	X	D	C	B	X	E	X	B	E	E
S29	X	A	X	X	X	A	X	X	X	A
S30	X	E	A	A	X	E	X	B	E	E
S31	B	X	A	A	C	A	B	C	X	C
S32	A	X	B	C	A	B	C	X	X	D
S33	E	C	B	A	A	E	X	D	C	E

Using the multicriteria analysis, the impact scores of the risk scenarios on the ten criteria are aggregated into a relative final judgement about the level of seriousness of the overall impact of each of the scenarios (see figure 5-1).

5.4.2 The 'Weighted Sum' method

After a test phase in which various methods are used, the methodological working group opted to use the 'Weighted Sum' method. In the Weighted Sum method, the ordinal labels X, A, B, C, D and E are first converted to a numerical value using value functions. In the NRA, 3 different type of value functions are used: exponential value functions with base 3 (where the labels X, A, B, C, D and E relate to each other as powers of 3 and E has the value 34=81, but where they are next standardised to E=1: X = 0/34=0; A = 30/34 = 1/81; B = 31/34 = 3/81, etc.), exponential value functions with base 10 (where the labels relate to each other as powers of 10 and E has the value 104=10000, but where they are also standardised to E=1: X = 0/104=0, A = 100/104 = 0.0001, B = 101/104 = 0,001, etc.), and linear value functions (where the distance between the labels is equal and E again has the value 1 and the interval [0..1] can therefore be divided into five equal parts: X = 0, A = 1/5, B = 2/5, C = 3/5, D = 4/5, E = 5/5). The

NRA primarily considers the outcomes of the Weighted Sum method with an exponential value function with base 3.
The other two value functions are mainly calculated to examine the sensitivity of the results in the event of different methodological choices.

Table 5-2: values of the label quantifications (three value functions)

Labels	Exponential value function with base 3	Linear value function	Exponential value function with base 10
X	0.00000 (= 0/81)	0.0	0.0000 (= 0/10000)
A	0.01235 (= 1/81)	0.2	0.0001 (= 1/10000)
B	0.03704 (= 3/81)	0.4	0.0010 (= 10/10000)
C	0.11111 (= 9/81)	0.6	0.0100 (= 100/10000)
D	0.33333 (=27/81)	0.8	0.1000 (= 1000/10000)
E	1.00000 (=81/81)	1.0	1.0000 (= 10000/10000)

These quantitative scores per criterion are then multiplied by the corresponding relative weights of the criteria, after which the products are totalled. This yields the weighted sum.

Final score scenario$_i$ = weight C1.1 x value of the label of scenarioi on C1.1
+ weight C1.2 x value of the label of scenarioi on C1.2
+ ...
+ weight C5.3 x value of the label of scenarioi on C5.3

The outcomes of the weighted sums lie between 0 (lowest final score) and 1 (highest final score): The higher the final score, the greater the total impact of the scenario on the ten criteria.
The numeric values of the weighted sum method with exponential value functions with base 3 are plotted on the logarithmic Y-axis of the risk diagram (see figure 7-1).

6 Likelihood assessment

In order to compare the chosen incident scenarios with each other, besides determining the impact, the likelihood of the scenario also has to be assessed. In this chapter, first of all the overall initial assumptions are set out, and the selected likelihood categories are explained. Next, a practical guide is given to the scoring of the likelihood for the malicious and unintentional scenarios.

6.1 General assumptions

In determining the likelihood of the incident scenario, the following initial assumptions are used.

- To determine likelihood, a breakdown into five categories is used (categories A-E). The classification matches the principles chosen to determine impact. Category A represents an incident scenario that is deemed very unlikely, while Category E represents an incident scenario that is deemed very likely. The ratio between the categories should be kept equal as far as possible; this applies both within the 'likelihood categories', and the 'impact categories', separately and in combination. Wherever it is possible to make quantitative estimates, the interval between the categories is (approximately) a factor of 10 for both likelihood and impact. The consequence is that the total 'outcome space' for likelihood and impact is equivalent.
- For categories A-D, the possibility is available of breaking them down into three sub-categories: low – medium – high, in order to create a greater and more continuous outcome space.
- For each incident scenario, the (sub-)category breakdown needs to be determined for:
  - the forecast value for the likelihood of the incident (V);
  - the lower limit for the likelihood of the incident (O);
  - the upper limit for the likelihood of the incident (B).
- The likelihood of the incident scenario is determined primarily by the trigger. For this reason, it is important that the incident scenario should include a good description of the cause, where a distinction is made between hazard scenarios (not malicious or unintentional) and threat scenarios (malicious, intentional).
- The likelihood of the incident scenario is determined to a secondary extent by the consequence (impact) of the incident scenario. So it is also important for the assessment of likelihood that the consequences of the incident scenario are described accurately and comprehensively enough in qualitative terms.
- Disasters which threaten safety and security on a national scale usually have a low likelihood of occurrence, or concern threats which the Netherlands has not faced before. This requires that when determining the likelihood, a clear and uniform line of reasoning is followed where, besides trigger and impact, the context regarding the potential hazard/threat is also clearly described. The context within which the incident scenario occurs relates, on the one hand, to the management actions already taken, and on the other to relevant environmental factors, trends relating to climate and the environment, political developments, etc.
- For all incident scenarios, it is true that when determining the likelihood, incomplete data/information will have to be used to a greater or lesser extent. This means that, depending on the type of incident, one or more of the information sources shown below will have to be used:
  - historic (similar) events, case histories;
  - statistics, combined if necessary with probability model calculations;
  - failure data - combined with network analyses/decision trees;
  - strategies and actor analyses;
  - expert opinions;
- For each incident scenario, an estimate will have to be made of uncertainty about the determination of the likelihood category, with a distinction being made as to the source of the uncertainty and the unreliability of the estimate.
- The likelihood is expressed as the likelihood that the scenario will occur within five years.

6.2 Breakdown into likelihood categories

For estimating the likelihood, the following breakdown into categories applies. In this regard, a distinction is made into 'hazards' and 'threats'. This is done because for threat scenarios, people's intentions must be taken more into account.

Table 6-1: category breakdown of likelihood of hazards

Category	% per 5 years		Quantitative (%)	Qualitative description of the hazard
A	< 0.05	A-low A-medium A-high	< 0.005 0.005 – 0.02 0.02 – 0.05	very unlikely
B	0.05 – 0.5	B-low B-medium B-high	0.05 – 0.1 0.1 – 0.25 0.25 – 0.5	unlikely
C	0.5 – 5	C-low C-medium C-high	0.5 – 1 1 – 2.5 2.5 – 5	possible
D	5 – 50	D-low D-medium D-high	5 – 10 10 – 25 25 – 50	likely
E	50 - 100	E	50 - 100	very likely

Table 6-2: categorical breakdown of likelihood of threats

Category	Qualitative threat description
A	no concrete indication and the event is not deemed conceivable
B	no concrete indication, but event is deemed far-fetched but conceivable
C	no concrete indication, but the event is conceivable
D	the event is deemed very conceivable
E	concrete indication that the event will take place

The chosen categorisation is determined by two factors:

1 The incident scenarios will mostly cluster in the lower part of the likelihood scale. To make a further distinction between these 'low likelihood' events, a logarithmic scale is used, with the result that this part of the scale is 'stretched'. The absolute interval for the transition from category A to B to C to D to E always increases by a factor of 10.
2 The difference between the categories (based on a factor of 10) also gives a degree of robustness with regard to the estimation of likelihood that does justice to the inaccuracy of the estimation of likelihood. In only a limited number of the scenarios will reliable statistical data be able to be used. In many cases it will be necessary to use incomplete data combined with expert opinions.

When the likelihood is determined on the basis of qualitative categorisation, the chosen category will be designated in principle as the middle of the category. Example: an individual threat scenario is assessed as 'the event is considered very credible', and is assigned category D-medium. There will be a move from this if the requested lower limit and upper limit lead to an asymmetric picture.
Example: lower limit category C; forecast value category D, upper limit category D. In this case, the forecast value shifts to category D-low.

6.3 Determining likelihood category

6.3.1 Information sources

Because we are focusing on 'disruptive' incidents, there will be a lack of case histories for a large proportion of the incident scenarios. Besides that, particularly for threat scenarios, malicious terrorist action cannot be characterised by experience from the past. The result is that the determination of the likelihood of the individual incident scenarios is based on several information sources:

- historic (similar) events, case histories;
- probability model- and design calculations;
- failure data elementary incidents - combined with network analyses/decision trees;
- expert opinions, scenario- and trend analyses.

In the best case, when determining the likelihood of an incident scenario – for example in the case of large-scale accidents – it will be possible to make direct use of available case histories, and thereafter the result will be amended based on an estimate of the changed conditions (society or environment) by experts.

The determination of likelihood for very large-scale accidents (for example a disaster at a nuclear power station) is based on failure frequencies for basic events (failure of pumps, etc.) in combination with logical decision trees.
For major natural disasters – like hurricanes, extreme high water levels in rivers – the likelihood assessment will be based on frequency distributions with regard to the natural phenomenon (wind strength, water levels, etc.) in relation to the (probabilistic) model calculations used in relation to the ability to withstand the natural phenomenon (strength of buildings, height of dykes, etc.).

Particularly for threat scenarios, the determination will mainly be guided by expert opinions about scenarios, social trends and threat analyses.

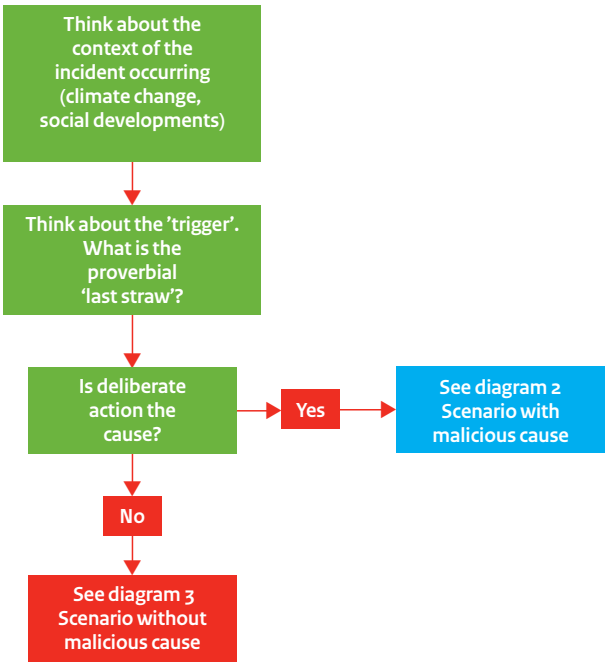
Where expert opinion is used, predominantly due to a lack of quantitative information, the assessment of the likelihood will have to be done via an established protocol (see Appendix A).

6.3.2 Malicious or unintentional action

The incremental plan (including diagrams) below shows the path that can be used to assess the likelihood. This is closely related to the context and triggers from the illustration in Chapter 3.

1 Determine whether the incident scenario is based on malicious action or not. In the event of malicious action, this is a threat scenario, and diagram 2 applies. If there is no indication of malicious action, we are looking at a hazard scenario and diagram 3 applies.

Determining likelihood (diagram 1, all hazard)



6.3.3 Likelihood of a threat scenario (or malicious action)

To determine the likelihood of occurrence of threat scenario (see diagram 2), the term plausibility is often used. To determine the likelihood, the above-mentioned qualitative classification is used. The assessment of the category is based on the available knowledge and data from the intelligence service (AIVD) and others.

The threat scenario assumes that the forecast (terrorist) threat will be successful. For this reason, the likelihood is primarily determined by two factors:

- the likelihood that a specific threat leads to an attack; this aspect is determined by the type of threat and the capabilities and intentions of terrorist groups;
- the likelihood that the attack will be successful; this aspect is determined, in particular, by the vulnerability of the expected targets.

Note: In the description of the threat scenario, the nature and the impact of the threat are actually decided. Example: an attack on a metro station (nature) with the result of tens of fatalities and hundreds of people injured (impact). The line of reasoning for the likelihood of threats actually completely matches the line of reasoning for the likelihood of hazards. The difference is that the nature of the threat and the impact are actually totally dependent events (the terrorist's aim is to achieve the planned impact), while for a hazard incident, usually several impacts are conceivable.

To determine the likelihood of the potential threat, here too, the context in which the threat scenario arises needs to be taken into account. This context can be very complex and is not just connected with social developments in the Netherlands and the integration issues that are relevant in that regard, but also international developments and the role of the Netherlands, and the military presence abroad.

The assessment of the likelihood of a specific threat scenario leads to the determination of a category (A,B,C,D,E).

Depending on the assessment of the vulnerability of the potential target(s) of the threat scenario, the category may be amended.
To determine vulnerability, a three category classification has been adopted.

Score	Description of vulnerability
Low	A high level of resistance to the threat. Policy is converted into a comprehensive programme of administrative measures, including ensuring compliance.
Average	Adequate resistance to the threat, but with a few weak points regarding measures and/or compliance.
High	Insufficient or no resistance to the threat. No policy, or policy inadequately converted into actions.

If vulnerability is assessed as high: category is increased by an increment (e.g. C becomes D).
If the vulnerability is assessed as low: category is decreased by an increment (e.g. C becomes B).

Below, you will find a more detailed explanation of determining the vulnerability score depending on the type of scenario or the target threatened.

To determine the vulnerability score, the threat scenarios are broken down into the following categories:
1 External threat:
   - Locations;
   - Buildings;
   - ICT systems;
   - persons.
2 Threat from within (infiltration)

The vulnerability score diagram creates insight into the level of vulnerability for the categories selected.

Diagram: Vulnerability score

		Vulnerability HIGH	Vulnerability LOW
External threat	Locations	Multiple, uncontrolled, entrances; incomplete fence Public roads at location No security cameras	Completely enclosed location; limited number of entrances; Access control and registration; Security cameras or other intrusion surveillance
	Buildings	Multiple entrances Inadequate control and registration; No intrusion surveillance Multiple users	Enclosed building, one guarded entrance Identification and registration (personnel, visitors, contractors) Building technical/electronic anti-intrusion measures Compartmentalisation/zones
	Means of transport	No security No specific driver training No procedures with regard to route, parking, incidents, etc.	Intrusion security, immobilisers GPS Driver security training Procedures with regard to route, route changes, incidents, parking, etc. Use of guarded parking
	ICT systems	No information policy Large number of Internet accesses to systems Limited/no policy and compliance regarding anti-virus protection, firewalls, passwords Not BS 7799 certified No disaster plan; no proper back-up Incompetent staff members or understaffing	Information policy on paper and communicated Access to systems controlled, secured Anti-virus security, firewall, compliance with password policy BS 7799 certified Disaster plan present and exercised Active commitment to exchange of security information

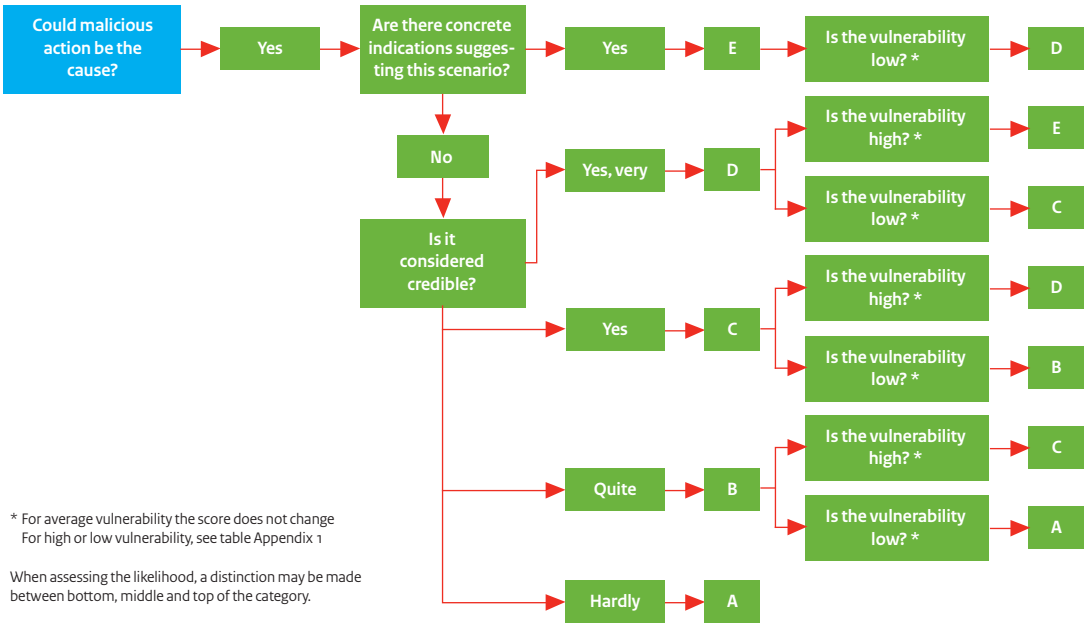
		Vulnerability HIGH	Vulnerability LOW
	Persons	No security	Personal security 24 hours per day Camera surveillance at home, intrusion security Planning of routes, accommodation, etc.
Infiltration		No screening, investigation of background Extensive use of contractors, temporary workers Poor personnel policy, poor working atmosphere No supervision/procedures with regard to sensitive information	Screening of personnel and temporary staff, employees of third parties Strict rules for hiring contractors, temporary personnel Open communication, good personnel policy Good awareness among personnel of anything suspicious

Determining uncertainty

We assume that the uncertainty with regard to likelihood is determined by the threat likelihood and not by the assessment of vulnerability. This means that for the likelihood of the threat scenario, inquiries will be made about the category used as the lower limit (O), upper limit (B) and anticipated value (V). The possible outcome may be that O, V and B are put into the same category.

Appendix C gives sample calculations for a limited number of scenarios.

Determination of likelihood (diagram 2, malicious)



* For average vulnerability the score does not change
For high or low vulnerability, see table Appendix 1

When assessing the likelihood, a distinction may be made between bottom, middle and top of the category.

6.3.4 Likelihood of a hazard scenario (or non-malicious action)

The assessment of likelihood for hazard scenarios (diagram 3):

- first determine to what extent quantitative data is available: incident data, failure data for systems, probability design data, statistical data about climatological conditions; if so, determine the likelihood on that basis;
- correct the basic likelihood if necessary for narrowing/widening of cause or condition described (correction factor 1);
- correct the likelihood if necessary for the described scale of the impact (correction factor 2);
- correct the likelihood if necessary for trends relating to altered conditions (correction factor 3);
- correct for an altered risk management level, which may result in higher or lower vulnerability (correction factor 4);

The determination of the likelihood of a hazard scenario always contains at least two elements:
- the likelihood that the defined hazard event will actually occur;
- the likelihood that the defined hazard event results in the impact described.

To determine both probabilities, the context in which the hazard event occurs must be taken into account. In general, the context relates to technical and management aspects, with government rules and compliance therewith, environmental factors, etc.

For example, the hazard scenario that corresponds to the cafe fire in Volendam:
- the hazard concerns a large fire in a cafe/leisure venue in the Netherlands;
- the impact of the hazard relates to the fact that the fire resulted in tens of fatalities and hundreds of more or less seriously injured/traumatised victims;

Note: the forecast impact should have been: major property damage, but only limited injury due to fire-retardant measures and the proper functioning of emergency exits.
Important elements of the context are the building regulations used in the Netherlands, the prescribed procedures for an outbreak of fire, the prescribed procedures to limit the consequences of fire and enforcement of compliance.
These are all described in the licence for the premises – if this is done correctly.

However, with regard to the context at the time of the cafe fire in Volendam:
- a considerable part of the catering establishment had no licence;
- there was too little regulatory control over the use of non-flammable materials and Christmas decorations;
- emergency exits did not meet the requirements, in combination with too many visitors being allowed in.

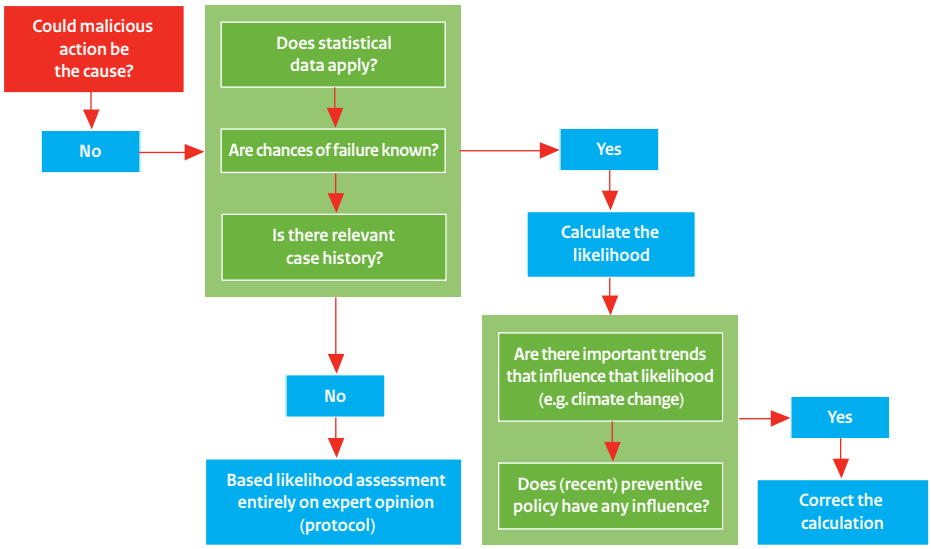
Since Volendam, the authorities have adopted a much stricter licensing policy. This does not directly influence the likelihood of fire, because the main causes are external (arson, lightning strike) or a technical cause. The likelihood of the fire causing a comparable result in 2009 would be much lower, due to a much stricter enforcement policy and more attention to fire safety facilities, number of visitors, emergency exits, etc.

Determining uncertainty

The likelihood is expressed as a forecast value (V). The lower limit and the upper limit must be determined by assessing the uncertainty with regard to each of the basic probabilities and correction factors determined. The opportunity or factor with the greatest uncertainty, i.e. the greatest deviation from the forecast value upward or downward, is taken as a measure for determining the lower limit (O) and the upper limit (B) of the likelihood.

Appendix C gives sample calculations for a limited number of scenarios.

Determining likelihood (diagram 3, not malicious)



When assessing the likelihood, a distinction may be made between bottom, middle and top of the category

7 Risk diagram and reporting of risk assessment

This chapter explains the presentation of the outcomes of the risk assessment in the risk diagram. Then it describes how the risk diagram can be read and used. Finally, it looks at analyses to obtain a picture of the robustness of the positioning of the scenarios in the risk diagram.

The reporting of the risk assessment shows in brief what the outcomes of the NRA are, and contains, among others, the following components:

- a summary of the input (the impact and likelihood scores of the scenarios) with explanation (see table 5-1);
- a risk diagram with explanation (see figure 7-1);
- a number of sensitivity analyses;
- a judgement about the robustness of the results.

7.1 The risk diagram

The standard risk diagram like the one shown in Figure 7-1 is based on:

- equal weightings for all ten impact criteria (preference profile 00)
- quantification of the ordinal labels X,A,B,C,D,E with the aid of the exponential partial value function with base three.

For each of the scenarios, the NRA returns a score for the aggregated impact and the likelihood. The scores are shown graphically in the logarithmically structured risk diagram. The impact is shown on the vertical axis. The maximum value of the axis corresponds to a (fictional) scenario that scores an E (disastrous) for all criteria (100%). All points are shown in the diagram based on their percentage of the maximum score. The likelihood is shown on the horizontal axis. The maximum value corresponds to a score with a likelihood assessed as very likely (50-100% likelihood in the next five years, or there is a concrete indication that the event will happen in the next 5 years).

Figure 7-1: Risk diagram with logarithmic axes

The aggregated impact scores (a number between 0 and 1) are converted using table 5-2 to category labels A score between 0.333 and 1.000 corresponds to an E-label, while a score between 0.111 - 0.333 corresponds to a D-label; A score between 0.037 and 0.111 corresponds to a C-label; A score between 0.037 and 0.012 corresponds to a B-label; and a score between 0 and 0.012 corresponds to an A-label. So the (rounded) score 0.333 corresponds to an average score D measured for all impact criteria, according to the above-mentioned exponential value function with base three; the simplest example of this is a scenario where all impact criteria score a D. Therefore, a score higher than 0.333 is shown in category E. the (rounded) score 0.111 corresponds to an average score C; Therefore, a score higher than 0.111 is shown in category D. and so on.

7.2 How to read the risk diagram?

How should the risk diagram be read? In other words: in what way can the risk diagram be used for prioritisation for the purposes of a capability analysis? This depends on a number of factors (viewpoints). The most important viewpoints concerning the information from the risk diagram are:

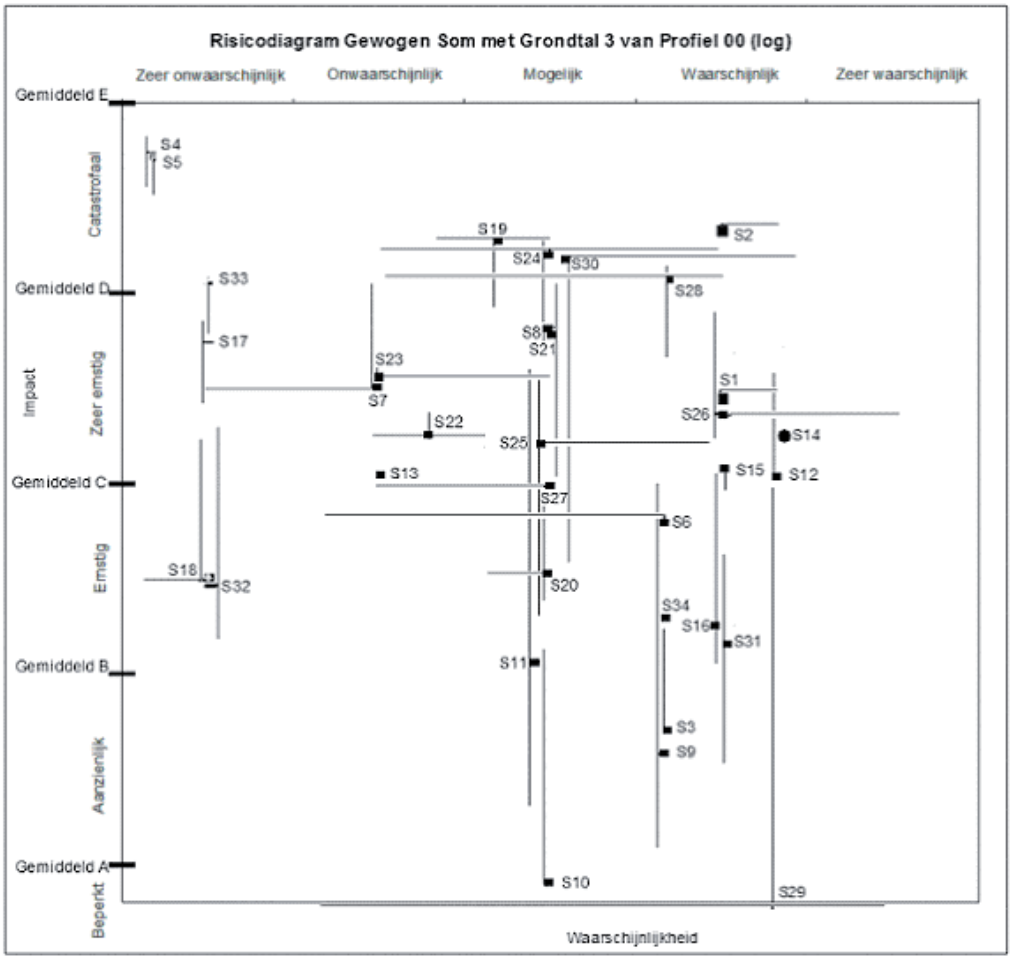
1. **Risk as a pure function of impact and likelihood;**
   Based on the classic risk concept, risk is the product of impact and likelihood (in which both are considered equally important). The ranking of the scenarios in relation to each other is shown visually by the shift from pale red to dark red. It goes without saying that in this case, priority is given to the scenarios characterised by a **high categorisation for impact and for likelihood.**
2. **The level of risk of administrative breakdown;**
   The selection of the NRA scenarios is not random: only scenarios that pose a threat to national safety and security are important for the NRA. A subset is formed by the 'real' disaster risks which form a high risk of administrative breakdown: for example a major flood or nuclear disaster. This type of scenario is characterised by a (very) low likelihood &and a **high impact.** From the viewpoint of risk of administrative breakdown, the risk is mainly posed by the impact.
3. **The possibility of risk reduction.**
   The question of which scenario should be given priority not only depends on the risk assessment, but also on the question of which scenarios offer benefits that can be obtained relatively simply: deployment of additional capabilities that would actually diminish the risk/ In many cases, this concerns risks with a **high likelihood.**

Ranking and prioritisation of risks for the purpose of capability analysis is not simple. The risk plays a role in this, but so does the possibility of improving the risk profile by deploying additional capabilities. Political motives also play an important role: topical social items and incidents.

7.3 Uncertainty analyses and sensitivity analyses.

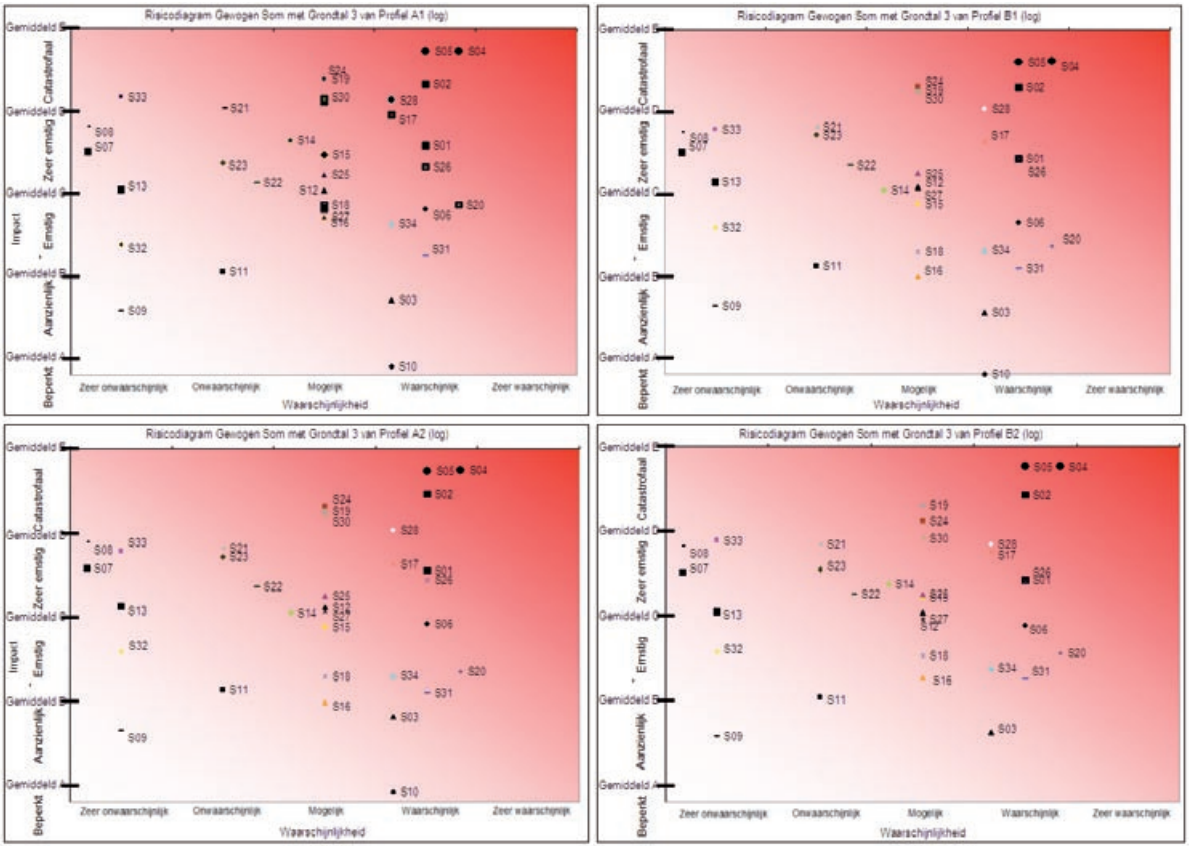
If the lower limits and upper limits of the impact scores differ greatly from the scores of the forecast values, it is sensible to show this in the graphics. Figure 7.2 shows the influence of the **lower limit and upper limit values** on the location of the scenarios of the NRA 2008 in the risk diagram.
A horizontal line around a scenario label shows that there is uncertainty in the determination of likelihood. The horizontal position of scenario in that case can vary from left to right on the probability axis; the wider the line the greater the uncertainty, but it is within the range that is covered horizontally by the line.
A vertical line around a scenario label shows that there is uncertainty in the determination of impact. In this case, the vertical position on the impact axis can vary from high to low. Here too, it is true that: the longer the line, the greater the uncertainty, but it is within the range on the impact axis that is covered by the line.

Figure 7-2: risk diagram with uncertainty bands



The basic analysis assumed equal relative weightings allocated to the criteria. In addition, calculations also use four other weighting profiles to take account of a certain diversity of values (see Appendix B). Comparison of the risk diagrams of the various profiles offers a visual insight into the influence of the slightly different world views.

Figure 7-3: Risk diagram weighted sum with base 3 for profiles A1, B1, A2 and B2



Besides the sensitivity analyses described above, additional sensitivity analyses are carried out on the category labels used for the impact scores (in other words, the various value functions) and therefore the variants used in the weighted sum method. All the sensitivity analyses carried out are intended to examine whether the position of the scenarios in the risk diagram changes significantly, in other words whether the positioning is robust or not, and whether it is necessary to pay greater or lesser attention to certain scenarios in the capability analysis.

8 Capability analysis and agenda setting

This chapter deals with the phase examining the possibilities of deploying additional capabilities to reduce the impact of a scenario, or reduce its likelihood. That is done in the capability analysis. After a brief explanation of the purpose of the capability analysis comes a practical guide to establishing the capability analysis process. Finally, the processing of the outcomes of the individual capacity analyses per scenario (group) into advice to the Cabinet about all scenarios analysed is examined.

8.1 Introduction

The third component of the National Safety and Security Strategy consists of a capability analysis. This analysis follows on from the first phase of the forward studies and horizon analysis, the selection of relevant scenario topics, the drawing up of scenarios, and the second phase, the analysis and assessment of the scenarios using the method of the national risk assessment, resulting in the risk diagram in which all scenarios are examined in relation to each other.
This is actually the phase that is all about the strategy: where are the weaknesses in our ability to reduce risks, and what can we do about it?

The whole National Safety and Security Strategy is aimed at improving our national safety and security. Devising the scenarios and performing the risk assessment gives us more understanding of what the position is. In order to curb a risk more effectively, it is possible that extra capabilities will be necessary. A capability may be a skill or knowledge, as well as things like measuring apparatus, or people to do things, or legislation to prevent dangerous situations.
In the capability analysis, we examine the scenario of the threat or the hazard, and the risk assessment, and then ask the following question: which capabilities do we need to reinforce in order to reduce the risk or be able to respond better?
These are explicitly two known dimensions of 'risk': reduction of the impact and reduction of the likelihood. The capability analysis is intended to create understanding of the options for reducing the risks and the extent to which taking additional measures to strengthen relevant capabilities would actually have an effect: if the position of a specific incident scenario in the risk diagram shifts significantly enough in the right/desired direction if the measures are implemented.

There follows a summary of the capability analysis process, and the steps involved:

8.2 Preparations for the capability analysis

A Form a working group with experts who have knowledge of possible capabilities relating to the given scenario(s).

Key areas:
I The membership of this working group may differ from the working group that wrote the scenario or performed the risk assessment.
II Ensure that all interests and viewpoints are represented in the working group. As many arguments as possible for or against reinforcement of a given capability must be considered.
III When constituting the working group, consider experts from ministries, decentralised authorities, knowledge institutes (including planning bureaus, universities, trade and industry).
IV See Appendix A for key areas requiring attention and tips about the use of expert opinion.

B Decide the organisation of the process that has to lead to the capability analysis.

Key areas:
I Consciously choose appropriate time planning to work on the analysis. Can the analysis be done during a two-day workshop, or is it better to meet fortnightly over a period of two months? How much can you ask of the experts? Does attention wane after a long process?

II Choose the modus operandi that produces maximum benefits.
III Decide whether representatives should speak as an individual expert or as the representative of an organisation. In the former case, personal pet subjects may arise, while in the latter, organisational interests may come into play in the background.
IV Agree whether the group has to reach a consensus, or whether minority views may be explicitly stated. The latter is preferable for the continuation of the process, in view of possible clashes of interest.

8.3 Stages to be followed

C Examine which areas may need to be reinforced (make an inventory) and draw up a first list of potential candidates.

Key areas:
I At the start of the process, explain to the experts in the working group the purpose of the capability analysis and what its role is alongside the scenario development and the risk assessment.
II Make a (schematic) inventory so as to put potential capabilities for reinforcement on a list of candidates;
  i For the scenario description, the experts are to make an assessment of important capabilities. Using the scenario, examine which capabilities appear relevant for reinforcement.
  ii Use the outcomes from the risk assessment. Examine for which of the ten impact criteria the scenarios score a D or an E, and determine what the origin of this high score is. Assess which capabilities could reduce the score of those criteria substantially if they were reinforced.
  iii Examine the scenarios. Do the same as in II.ii with high probability scores. In this way, high scores play a role in drawing attention to underlying (shortages of) capabilities. Assess which capabilities could reduce the score of those criteria substantially if they were reinforced.
  iv In doing this, make a distinction between capabilities:
    1 before the crisis (pro-action/prevention);
    2 during and after the crisis (preparation / response / post-crisis phase).
  v Also distinguish capabilities:
    i that are specific to the type of incident in a scenario;
    2 which are of generic interest to more types of incidents.
  vi A capability always belongs with a task. Capabilities are there to enable the performance of a task. Use the task list (Appendix) to examine whether tasks (and associated capabilities) appear important for the scenario, but have not yet been prominent.

D Make a priority list of approximately five capabilities to be reinforced for each of the four types of capability designated under C.II.iv.

Key areas:
I Make a strict selection of the most important tasks that could potentially be reinforced, from the list of candidates. A rule of thumb is a list of no more than five capabilities that really need improvement:
  i With the working group, assess whether there is a possibility of a shortage of capabilities. Here, this is a first estimate by the experts about which capacities are necessary (the target situation), and afterwards it should be determined what capacities are actually required (the actual situation). At this time, it is not yet necessary to provide detailed quantitative substantiating evidence.
  ii Examine which capabilities can lead to rapid improvement (quick wins);
  iii Examine which capabilities could lead to lasting improvement of security;
  iv Examine which capacities bring substantial results in relation to their cost (cost/benefit analysis).

Precisely in relation to this aspect, it is important to examine whether, and if so, the reinforcement of the capacity under consideration (or combination of capacities) leads to a significant shift in the scenario in the risk diagram. This can be done by modifying certain scores (effect of capability reinforcement measures that could be taken) and recalculating this in the diagram.

II Who is in charge of the capabilities that need to be reinforced: the government, a specific ministry, business, decentralised government? Indicate the extent to which this party actually wishes to commit to reinforcing this capability.

III Assess on the basis of political or social realities whether there are capabilities that it is politically urgent to reinforce.

E Record the prioritisation of capabilities to be reinforced, with justifications, in a single document.

Key areas:

I Indicate which capabilities were put on the list of potential candidates based on which arguments (scenario analysis, impact criteria analysis, task analysis).
Bear in mind that for the capabilities that need to be reinforced to be put on the agenda for the complete set of scenarios, it is important to have sight of the list of potential candidates for reinforcement. It is perfectly possible that capabilities that appear in different scenarios lead to a generic capability that needs to be reinforced.

II Indicate the top five capabilities. Based on which arguments (difference between target and actual situation, quick wins, lasting improvement, cost/benefit) were these capabilities chosen? Were there still dilemmas/discussion points about the selection of these five capabilities?

III Ultimately, a limited list of recommendations will have to made (for the capabilities to be reinforced) for the Cabinet. For the overall consideration of all capabilities that are put forward by the various working groups, it is important that each working group should indicate, for their chosen capabilities:
- i which scenario(s) are the basis of the capabilities chosen and what role (in terms of impact and likelihood) the scenario(s) has/have in the NRA;
- ii and to what extent the 'capability owner' is prepared to commit to reinforcing the capability;
- iii if it is politically urgent to reinforce the capability;
- iv what the improvement anticipated is (effects), in terms of impact reduction or likelihood reduction;
- v what the required effort is (including in terms of the order of magnitude of financing (4, 5 or 5 zeroes in Euros), time requirement (when can something be ready, manpower).

8.4 After the capability analysis

The various theme groups will put forward their various capability analyses. From the individual capability analyses, the findings report will have to advise the Cabinet on which capacities must be reinforced in the interests of national safety and security. Considering all the scenarios, proposals will be made based on the risk diagram, political attention, quick wins, cost/benefit analysis.

In the findings report, attention will be paid to specific capabilities, which means capabilities that are necessary for one risk type. It will also be indicated which capabilities require reinforcement and are useful for multiple risk types. The lists of capabilities that could potentially be reinforced for the various scenarios are important for finding these generic capabilities that potentially not only benefit one scenario but can also make an effective contribution to curbing various risk types.

The Cabinet will decide on the basis of the findings report which recommendations they adopt.

Appendix A
The use of expert opinions

The use of expert opinions. In the national safety and security programme new and known risks for the (near) future are mapped and analysed. Often insufficient information is available to adequately assess likelihood and impact of these risks and the future is uncertain. Therefore the use of expert opinions is necessary to gain results. This appendix highlights the areas requiring attention in the use of expert opinions.

Expert opinions are used throughout the National Safety and Security methodology:
- in identifying new risks and threats;
- in developing scenarios into storylines, likelihood and effects;
- in scoring the 10 impact criteria and the likelihood;
- in assessing the effect of policy measures.

An expert opinion is an important source of information. The backdrop to the choices made by experts is not always obvious. The ability to infer those experts' basic assumptions and a transparent process of scoring the impact and assessing the likelihood can improve the quality and reliability of the outcomes.

A.1 General areas requiring attention

The use of expert opinions is not just inevitable but also essential for the sufficient dependability, robustness and detail of the development of a scenario, the scoring of the impact and likelihood, and to produce an inventory of the necessary capacities.

In order to guarantee that experts are used properly, it makes sense to take account of the following key points.

Key points for the process:
- Decide who takes part in the scenario writing process, who scores the probability and the impact, and who takes part in the capability analysis. The membership of the group that scores the likelihood and the impact can be totally different from the group that writes the scenario or the group that performs the capability analysis.
- Ensure a proper balance between experts on content, and representatives drawn from policy-making circles;
- each expert takes part in a personal capacity;
- *in connection with the confidentiality of the available information, it is conceivable that for the threat scenarios, a select group of experts can be appointed (staff of the intelligence or national police services, etc.).*
- When composing the working groups (irrespective of whether they are for the development of scenarios, scoring or producing the inventory of capabilities), ensure that all specialist fields that are relevant to the scenario are represented;
- When composing the working groups, take into account the groups' results in the continuation of the work. At the stage of devising the scenario, ensure that there is sufficient dependable information that is relevant for the scoring of impact and likelihood. When devising the scenario, ensure that there is also sufficient information about relevant capabilities, so that the scenario offers points of departure for producing the inventory of capabilities that require reinforcement in the subsequent capability analysis.
- Determine how the experts' work can best be organised. Think about efficiency, use of their time and discussion between experts.
- Use experts efficiently: determine whether experts can provide continuous input into the process, or whether it will suffice to have a one-off contribution from an expert.
- Decide how expert input can be organised as reliably and robustly as possible: discussions between experts can improve the result. Situations are also conceivable where discussions actually suppresses divergent opinions or specific views and outlooks;

- bear in mind that the purpose of the process is not primarily to achieve consensus between the experts. Uncertainties and the associated differences of opinion are inevitable in the type of scenarios used in the national safety and security method. Well-argued differences in views are an enhancement of the usability of the results of analyses and scores.

Key areas for contribution of content by experts
- Make it explicit to the experts what the chain of events is, what the causal connection is and which line of reasoning will be followed. Agreement about the chain of events, the causal connection and the line of reasoning followed in the scenario is necessary for reliable scoring of the impact and likelihood and for the capability analysis;
- Experts often use many years of experience and know-how/knowledge from various sources when formulating their views;
- Ask experts to state explicitly the source of their know-how? (empirical data, model calculations), which assumptions they are using and what uncertainties affect their remarks;
- expert opinions are subject to empirical checking: available empirical data must not be rejected, replaced or removed.
- Naturally, empirical data must be checked against the latest circumstances or developments that influence (the likelihood of) the occurrence of future circumstances. With regard to threat scenarios, this is the reason that the explanation of diagram 3 (Chapter 6) mentions the correction factors. Determination of the correction factors will often need to be based on expert opinions.
- Experts have to adhere to the formal calculation rules of probability.
- Determine how the expert can best be helped in coming to an independent determination of his/her own interpretation and estimates.
- The more explicit the knowledge sources, assumptions and uncertainties are, the easier it will be to manage discussions between experts and substantiate and follow-up choices made. Record as many references, sources, assumptions and uncertainties.
- Make a distinction between uncertainties (due to lack of knowledge) and differences of views between experts.
- Determine how to achieve the greatest possible convergence between the various expert opinions, while maintaining individual views and to a 'best' outcome, and how the best can be reported, including the uncertainties and differences of views.

A.2 Protocol for the use of expert opinion in the risk assessment

This protocol can be used when the assessment of likelihood or impact cannot entirely be based on case histories or model calculations. This will be the case for most of the incident scenarios.

Possible procedure for assessing likelihood and scoring impact

Start by making an inventory of the available data. Distinguish between hazard incidents (non-malicious) and threat incidents (malicious).

Hazard incident:
- Make a joint inventory of available empirical data concerning incident, cause and effect.
- Make a joint inventory of available empirical data concerning the current context and the effect of risk management measures. Document available empirical data and/or include references in the scenario.
- *empirical data refers to design or model calculations, case histories, research results, trend analyses, amended legislation and demands, oversight of enforcement etc.*

Threat incident:
- Make a joint inventory of available data concerning potential terrorist groups, their aims, intentions and knowledge (concerning incident), available capabilities, as well as knowledge of

time and place. Document available empirical data and/or include references in the scenario description.

Now proceed to scoring the impact or assessing the likelihood. Opt for individual scoring by the experts followed by a joint discussion, or for joint scoring with individual opinions.

Making of an individual assessment followed by joint discussion:
If a score is reached based on individual assessments, go through the following stages:
Individual assessment

- Based on a joint understanding of the available empirical data, all experts give an individual scoring of the impact criteria and of the likelihood;
- The experts are asked to not only assess the most likely value (or category), but also give their opinions on the upper and lower limits;
- all estimates need to be well reasoned by
- for example, including the line of reasoning, the calculations, applied correction factors or citing the most decisive information and references used.

Making an inventory, assembly and reporting

- the chairman/secretary of the working group produces a joint report of the individual expert opinions, and sends them to the individual members;
- the individual members are given the opportunity to request explanation from individual experts.
  NB: The aim is – if necessary – to gain better understanding of the motivation of the individual expert.

Feedback and adjustment:

- Based on the insight obtained, experts are asked to review their initial assessment and give reasons for changes – if any. The update is individually made and documented.

Convergence and outcome, including uncertainty
The group chairman/secretary converts the results into:

- forecast value: the average of the individual expert assessments
- The lower limit: the absolute lower limit of all assessments
- The upper limit: the absolute upper limit of all assessments

Joint scoring:
If joint scoring is chosen, the following areas should be borne in mind:

- based on a joint understanding of the available empirical data, during the discussion the experts give an assessment of the scoring of an impact criterion and the likelihood;
- based on the uncertainty, as well as differences of opinion between the experts, the forecast value (or category) and the upper limit and lower limit are determined;
- reasons must be given for choices, and this must be substantiated and recorded.

After the scoring by the experts, the reporting and review come next. The full report on the expert opinion process is added to the scenario description. The NRA working group checks results for correct application of probability calculation laws.

Appendix B
Weightings and preference profiles

Important inputs for the MCA Method are (i) the scores of the risk scenarios for the ten criteria, and *(ii)* the relative weight of each of these criteria. Various policy makers (and citizens) would undoubtedly ascribe different relative weights to each of these 10 criteria, which would have consequences for the ranking of the scenarios.
Since the goal of the NRA is a robust ranking, this value diversity is included in the MCA analysis both explicitly – with the aid of 5 different preference profiles – and implicitly- by means of extensive sensitivity analyses for changes in the weightings. In practice, five different preference profiles are used instead of one single profile. The use of these preference profiles enables:

- a certain degree of value diversity to be taken into consideration explicitly, and to illustrate, analyse and communicate the influence of value diversity on the ranking in a comprehensible and transparent manner;
- the robustness of the ultimate ranking to be examined;
- extensive sensitivity analyses to be carried out from various starting points (the different profiles);
- circumventing an impossible task, namely the impossibility of incorporating the precise weightings of all policy managers (and citizens) perfectly into the analysis.

Ideally, these different preference profiles should largely reflect the main value orientations of Dutch policy makers (and the world views and attitudes to life of the citizens they represent). Although the preference profiles used here do aim to achieve this, they should be regarded as just as an initial attempt to do this: the profiles set out below are derived in an intuitive – and not scientifically rigorous – way from the preference profiles of Dutch policy makers (and citizens). The first four profiles, 'A1', 'B1', 'A2' and 'B2' are based on, and therefore to be compared with, the four perspectives/ lifestyles described in Cultural Theory:[5], the four world views of the IPCC[6], and the value orientations of the WIN model of TNS-NIPO[7]. The last preference profile, profile '00' is merely a profile with equal values for all criteria. These preference profiles will be outlined briefly – in a rather caricaturised way.

Profile A1 – the individualistic perspective – the global market: This profile represents the outlook of rather materialistic liberal entrepreneurs. These 'individualists' do not wish to be bound by a group or rules. They have firm belief in a meritocracy, the free market and technological progress. The free market economy is a vital interest like other interests that support the global free market. Success and merit are a personal responsibility, which is why individual liberties must be guaranteed. These individual liberties would be jeopardised in the event of disruption of everyday life. Furthermore, government interference is not appreciated. They find the quest for an individually stimulating and comfortable life to be more important than average. As long as harm to the democratic constitutional state, encroachment on the territory or harm to the integrity of the international position of the Netherlands does not affect that quest, they will consider these phenomena of lesser importance. In the event of a disaster, they nevertheless feel that fatalities, injuries and the chronically sick, as well as a lack of the basic necessities of life are important – especially when they and their ?nearest and dearest?close relations are affected. They find social indignation and fear less important, as they do harm to nature which is assumed to be defensible.

---

5 The four perspectives/lifestyles described in Cultural Theory are the *individualistic perspective,* the *egalitarian perspective,* the *fatalistic perspective* and the *hierarchical perspective* (Douglas, M., and Wildavsky, A. B. (1982). *Risk and culture: An essay on the selection of technical and environmental dangers.* University of California Press: Berkeley).

6 The four world views of the IPCC are the 'A1' world view 'the global market', the 'B1' world view 'global solidarity', the 'A2' world view 'the safe region', and the 'B2' world view 'the caring region' (IPCC (2000). Special Report on Emission Scenarios. Cambridge University Press: Cambridge. [Intergovernmental Panel on Climate Change]).

7 Four stylised versions of the archetypical scenario world views of the IPCC (2000) are compared in the Sustainability Study (RIVM 2004, p48) with the WIN value orientations of TNS-NIPO (liberals, committed, caring, conservative, hedonists, luxury seekers, businesspeople and balanced (RIVM (2004). *Kwaliteit en Toekomst. Verkenning van duurzaamheid.* Milieu- en Natuurplanbureau en Rijksinstituut voor Volksgezondheid en Milieu: Bilthoven. [RIVM Rapport 50001 3009], p48) (NIPO (2002). Het WIN-model, waardensegmenten in Nederland. Nederlands Instituut voor de Publieke Opinie: Amsterdam).

Profile B1 – the 'egalitarian' perspective – global solidarity: This profile represents the outlook of rather egalitarian citizens, who are in favour of solidarity, and keen on social and long term ecological stability. Equitable development of international and national social prosperity and welfare is what counts for these 'egalitarians'. They believe that nature is very important and vulnerable, and therefore needs to be protected. They also assume that inequality between people is unacceptable. That is why they find harm to the democratic constitutional state and social indignation and fear very serious matters. In the case of disasters, fatalities, injured, chronic illnesses and a lack of basic necessities of life – whoever is affected – this is considered very serious. Temporary disruption of everyday life is not considered serious. Such situations even lead to a desired side effect, namely to solidarity (for example with those whose daily life is always disrupted). The economy is of lesser importance: It is only a means, not an end in itself. 'Egalitarians trust the government to manage collective property and correct failures of market forces. They have a particularly international outlook: harm to the integrity of the international position of the Netherlands is perceived as more problematic than harm to the integrity of Dutch territory. 'Egalitarians are very strongly bound and determined by the group to which they belong, but are less inclined to accept rules, certainly if these interfere with their belief in the need to protect the weak, vulnerable nature, etc.

Profile A2 – the 'fatalistic' perspective – the safe region: This profile represents the outlook of rather fatalistic citizens. These fatalists feel strongly bound by rules, and excluded from a real tight-knit group member society, which leads to a feeling of powerlessness and a fatalistic attitude. These concerned citizens want to keep what they have, in terms of property and social values. Their preferred society is a closed, safe, liveable society, in other words, a safe region. they consider encroachment on the territorial integrity of the Netherlands as serious. The integrity of the international position is of lesser importance. Mistrustful of human nature, the emphasis here is on personal responsibility or that of certain interest groups, authorities (through expertise and experience) and certain institutions (politicians, security and judiciary). They are keen on social stability and, and this can be achieved through regulation, standards and hierarchy. They feel that socio-psychological impact (indignation and fear), disruption of everyday life and harm to the democratic constitutional state causes social instability and are therefore particularly serious, as are, in the event of disasters, fatalities, injured, chronically ill, lack of basic necessities of life. The direct economic costs of a disaster are also serious for these citizens (particularly if it hits their own pocket) since a comfortable and pleasurable life is an important goal for A2 people. Long-term harm to the environment and nature is of lesser importance for citizens and policy makers.

Profile B2 – the 'hierarchical' perspective – the caring region: This profile represents the outlook of rather traditional and hierarchically-minded citizens who are strongly bound by group and rules. This perspective/world view is that of the more traditional middle class, which want a society with a sense of community on a smaller scale, care for the immediate (social and ecological) environment, in which intangible values play a key role. These citizens feel equality is rather important. Consequences in terms of fatalities, injured, chronically ill, lack of basic necessities of life, long-term harm to the environment and nature, disruption to everyday life, and harm to the democratic constitutional state and the socio-psychological impact (indignation and fear) are regarded as very serious. Encroachment on Dutch territory is seen as rather less serious, unlike harm to the local area, which is indeed seen as serious. B2 people do not consider a comfortable life as very important, which is why economic costs and harm to the international position of the Netherlands in the case of disasters is not seen as serious.

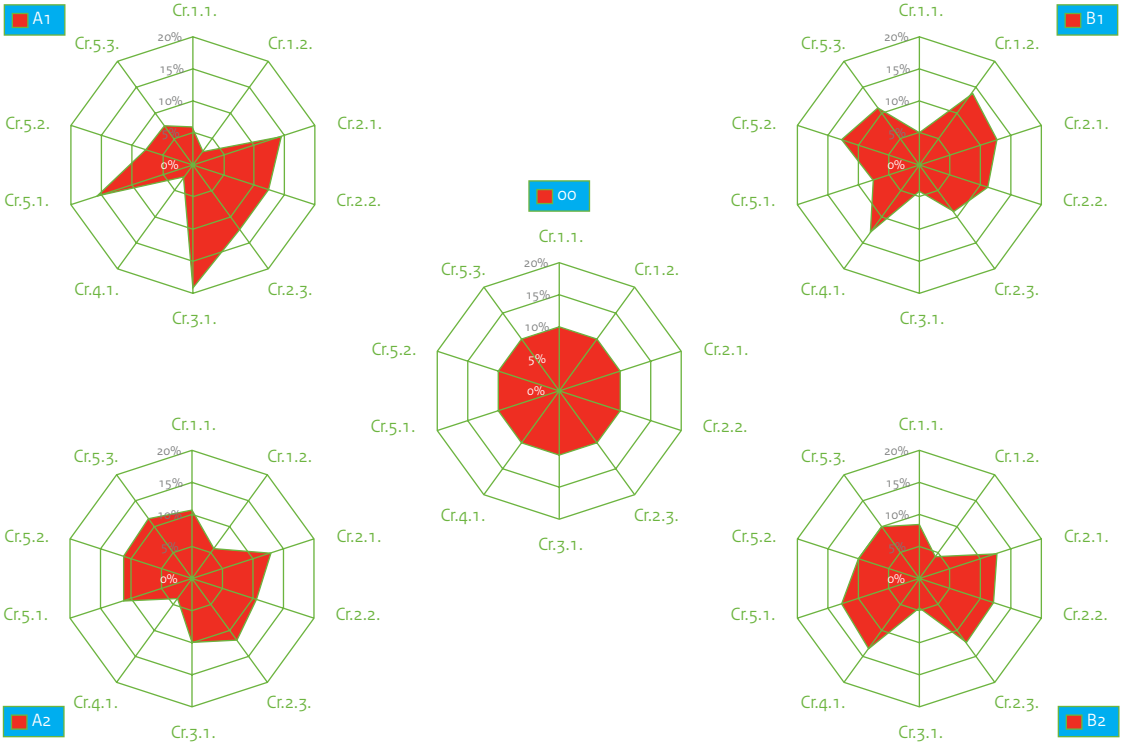
Profile 00 – the 'equal weightings' perspective: This profile ascribes an equal relative weight to each of the ten criteria. 10% of the total. Citizens and policy makers who identify with this profile argue that consequences of the same impact level (from A to E) on all criteria is of equal importance.

Table B-1 and Figure B-1 reflect the precise percentage interpretation for each of the five profiles that is used in the NRA. These slightly differing preference profiles enable a certain social value diversity to be taken into account and the robustness of the ranking of risk scenarios to be tested.

Table B-1: the weight distribution of the different profiles

Profile:	Cr.1.1	Cr.1.2	Cr.2.1	Cr.2.2	Cr.2.3	Cr.3.1	Cr.4.1	Cr.5.1	Cr.5.2	Cr.5.3	total weight
00	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	100%
A1	6%	3%	14%	12%	12%	19%	2%	16%	8%	8%	100%
B1	5%	14%	12%	11%	9%	4%	13%	8%	13%	11%	100%
A2	11%	6%	13%	11%	12%	10%	4%	11%	11%	11%	100%
B2	9%	5%	13%	12%	12%	4%	13%	12%	10%	10%	100%

Figure B-1: graphic presentation of the profiles



Appendix C
Examples of assessment of likelihood category

Major fire in a catering establishment with tens of fatalities.

Model incident scenario derived from cafe fire in Volendam.
Major fire in a catering location, resulting in tens of fatalities and possibly hundreds of injured. The location is completely destroyed.
Reference locations: cafes, discos, hotels, boarding houses, restaurants.

Determine likelihood on the basis of case histories: 2 examples in the last 30 years (Volendam and Hotel Poland). Possible correction factor for improvement of regulation and oversight of compliance (approx. factor 0.1 – 0.5; factor is determined by expectation that people can walk away unharmed).

$\mathcal{P}$ (catering fire) = 1/15 x (0.1 – 0.5) per year

= 5/15 x (0.1 – 0.5) % per 5-year period ≈ 10% per 5-year period = category D

An alternative line of reasoning is as follows:
$\mathcal{P}$ (catering fire) = P (G) x P (E|G)
= P (G1) x P (G2) x P (G3) x P (E|G)
= 50/5yr x 0.5 x 0.2 x 0.02
= 0.1 = 10% per 5-year period = category D

$\mathcal{P}$ (G1): number of catering fires per year (claims according to CBS, statistics 2005-2006)
$\mathcal{P}$ (G2): Likelihood that catering establishment is burnt out
$\mathcal{P}$ (G3): Likelihood that catering establishment is very busy
$\mathcal{P}$ (E|G): Likelihood that fire leads to a few tens of fatalities

NB: 1. The data chosen is fictional
2. The assumption is that the probabilities are mutually independent, but event G1 can be dependent on event G3.

Outbreak of pandemic form of influenza

A genetic mutation in of the H5N1 virus of influenza ('bird flu') leads to the virus being transmitted from human to human. The initial outbreaks are recorded in Malaysia, and within 4 to 8 weeks, the virus spreads to all continents. After 6 weeks, the virus reaches Western Europe, and the duration of the pandemic in the Netherlands is about 10 weeks. Almost 50% of the population fall sick; the chance of catching it is the same for all groups of the population. The mortality rate is 0.5% of those infected. The new virus is a completely new strain; it will take over six months for a new vaccine to be developed and available.

Determination of the likelihood from case histories: average of 2 pandemic outbreaks in a century. Experts are of the opinion that in 2007, the risk of a global outbreak is greater by at least a factor of 2, due to the intensification of travel/contacts.
The pandemic described should be rated as 'serious' within the potential range of seriousness (within the category: mild – average – serious – very serious), which is determined by the extent of genetic mutation and the risk of mortality. The likelihood that the pandemic outbreak belongs to this category is assessed at 10%.

$\mathcal{P}$ (pandemic scenario) = $\mathcal{P}$ **(pandemic) x F (pandemic) x** $\mathcal{P}$ **(Seriousness|pandemic)**
= 2/100 x 2 x 0.1 = 0.4% per year = 2% per 5-year period = category C

Flooding of coastal area

As a result of a severe storm and the associated long-lasting high water level, several breaches in dykes occur along the coast.
This concerns a long-lasting storm (45 hours) of hurricane force, with wind strength of 170 km/h being

reached 2 km up in the atmosphere. A week after the breaches in the dykes, the maximum area of land flooded would be 4330 km² and 2.3 million people would be affected
Progress: after 4 hours, an area of 1240 km² and over 700,000 people affected;
after 24 hours, an area of 3470 km² and over 1,800,000 people affected;
after 48 hours, an area of 3940 km² and over 2,000,000 people affected.
The storm scenario outlined is more serious than the storm scenario on which the safety standard for the design of the dykes is based. The safety standard is 1/10,000 per year for the coastal area.
The likelihood of the coastal area being flooded based on the scenario outlined is therefore less than 1/10.000 per year.

$\mathcal{P}$ (flood scenario) = < 1/10,000 per year
= < 5/10,000 per 5-year period
= < 0.05% per 5-year period = **category A**

Political assassination

On 15 March 2011 – four weeks before the elections to the Lower House of Parliament – Mrs. Fatima H. is murdered in broad daylight. The perpetrator is arrested a few days later, and appears to be connected with radical Islamist circles. No doubt about the motive: Fatima H. was considered as an 'unbeliever' and had previously been accused on several occasions of bringing the Koran into disrepute. Fatima H. had already been politically active for a number of years, and had drawn a lot of support for her views about emancipation of (Moslem) women and was, for many of them, a role model of an emancipated Moslem woman. Fatima H. was standing in the forthcoming elections to the Lower House. Fatima H. had round-the-clock security.

In view of the recent reference scenarios, this scenario was deemed very credible for the coming 5-year period. But there was no hard information concerning the person, place or time.

It was the task of the NCTb (national counter-terrorism) coordinator to arrange protection for Fatima H. This is done in a professional way.

$\mathcal{P}$ (political assassination) = category D with vulnerability score 'low' = **category C**

(adapt diagram for two examples (flooding and political assassination).

Likelihood is initially determined for a 5-year period.

Information source/ methodology	Likelihood of occurrence of incident (trigger)	Likelihood, scale of impact	Correction prevention	Correction repression	Likelihood
Flooding example	storm with extreme wind speeds	breach of dyke ring 14	dyke strengthening programme	evacuation	
	< 1/100,000	x 0.5	x 1.0	- (x 0.95)	1/200,000 = A
Sources:	- KNMI statistics - Historic analogy (+ adjustment) - Model calculations - Bayesian statistics - likelihood of failure, network analysis decision-trees - Scenario description and analysis				
Political assassination example	very credible No hard information	1 fatality	Low vulnerability	N/A	
	> 1/20	x 1	x 0.1	x 1	1/200 < W < 1/20 = C
Sources:	- Expert opinions - Trend analyses				

Likelihood (2008-2012):

Flooding 1/100,000 x 0.5 x 1.0 x 0.95 = ~ 1/200,000

NB: for hazards, in all cases a factor is used that can allow all values (less than, equal to or greater than 1).

Political assassination 1/20 x 0.1 = 1/200

NB:

1. For threats, the vulnerability is always calculated with a factor of 0.1 (low vulnerability), 1 (average vulnerability) or with a factor of 10 (high vulnerability).
2. Evaluation of vulnerability is carried out with the aid of vulnerability diagram later in this appendix.

For threats, the likelihood of impact is always set to 1 (converted into likelihood of occurrence of incident), and the repression correction factor is always set to 1.

Determination of likelihood for the period 2028-2032: Inclusion of forecast trends

Flooding example		
Likelihood of occurrence of incident (trigger)	storm with extreme wind speeds	< 1/100,000
Trend for likelihood, (from context)	climate change	++ or (x 1.5)
Likelihood, scale of impact	breach of dyke ring 14	x 0.5
Trend for scale of impact	economic and demographic growth	++ or (x 1.2)
Correction prevention	Dyke strengthening programme	x 1.0
Trend for prevention	Investment as share of GDP	- - (or 0.75)
Correction repression	evacuation	- (x 0.95)
Trend for repression	Ability to cope increases	- (or x 0.9)
Likelihood		1/50,000 = A

* the correction factors used are fictional

Likelihood of flooding within a future 5-year period (2028 – 2032)

1/100,000 x 1.5 x 0.5 x 1.2 x 1 x 0.75 x 0.95 x 0.9 = ~ 1/50,000

Appendix D
Task list for capability analysis – a checklist

Explanation about purpose of task list / - checklist

This checklist may help to produce a robust capability analysis. This (generic) task list includes all tasks that can play a role in a scenario in the context of national safety and security. This checklist can be used to determine whether all tasks that play a role for the scenario concerned have been brought into the picture. This is so that no tasks are left out and ultimately so that no capabilities are missed out that are necessary for a scenario.

This list is drawn up based on a large number of existing task lists from specific sectors, for specific scenarios and from home and abroad, and completed with input from a large group of experts.

Definitions

- A task is what actors/players in society (government, business, organisations, citizens) must be able to do in order to safeguard national safety and security (territorial, physical, economic and ecological security and social and political stability).
- Capabilities describe what is necessary (in terms of know-how, resources, people with skills, agreements, etc.) in order to perform that task and – where appropriate – which actor/player should have those capabilities.

Intended effects:

General:	safeguarding (the five vital interests of) national safety and security
Specifically:	A. as far as possible, avoiding a potential threat to national safety and security (proactivity)
	B. as far as possible, to limit (the source of) a potential threat before it happens (prevention)
	C. as far as possible, prepare to limit the impact of a threat (preparation)
	D. as far as possible, limit (the impact of) an (imminent) event (response) • as far as possible (in the case of an acute threat) remove or restrict the source of the threat / event • as far as possible limit the spread of the threat • as far as possible limit the impact on people from the threat
	E. as far as possible, repair the damage and the consequences (after-care) • return to normal functioning of society • compensate the loss sustained
Preconditions	F. and G. consider and implement measures that are intended to reach a), b), c), d) and e); does not make any direct contribution to security

The task list – the checklist

A. avoiding a potential threat to national safety and security (proactivity)

1 **removing** the source

2 rendering **impossible** situations that may lead to a threat

B. as far as possible, to limit (the source of) a potential threat before it happens (prevention)

3 limiting the threat by **spatial** layout

4 limiting the threat through the setup of the **infrastructure**

- i ensuring protection of data sources and systems (including international agreements on this subject)
- ii compartmentalisation with dykes
- iii layout of the road network

5 decisions about **market forces** within a sector

6 increasing the endurance and awareness of (vital) companies, organisations and citizens

- i **risk management**

C. as far as possible, prepare to limit the impact of a threat (preparation)

7 drawing up, implementing, exercising and overseeing response **plan** / public communication plans
criterion: ensure coordination beyond regional level
- i ensure **training** and exercises for personnel
- ii multi-disciplinary **exercises** with (vital) and societal organisations (including the media), local and regional administrations (internationally and nationally) and citizens
  - a exercises to train personnel
  - b exercise to test arrangements, systems, available capabilities
- iii create **buffer stocks** of vital goods and emergency supplies
- iv as far as possible, determine strategy for distribution of **scarce resources** (prioritise who gets what first)

8 drawing up, implementing, exercising and overseeing **continuity plans**

9 setting-up a clear **information structure** between government, business and citizens
criterion: clear, unambiguous, dependable, timely

10 ensure **risk communication**

11 set up response organisation / incident combating
- i ensure logistics support for emergency services
- ii preparation **of disaster response processes**
  - a management and coordination
  - b fire service processes (fire fighting and dealing with hazardous substances, rescues, measuring, decontamination)
  - c medical processes (medical assistance, mental health care, preventive health care, isolation and quarantine)
  - d police processes (maintaining public order, law enforcement (including guarding and securing), controlling traffic, cordoning off, guiding, identification of victims)
  - e local authority processes (victim and damage recording, mortuary)
  - f multi-disciplinary processes (information, warning, clearance, evacuation), relief operations, basic necessities, environment, making roads passable, collection of contaminated goods)
  - g miscellaneous: veterinary medicine, border controls, explosives clearance, secure clues for prosecution and learning lessons

12 setting-up of robust, **flexible,** versatile response organisation for the various actors
- i setting-up of stable communication infrastructure and communication arrangements and processes between actors
- ii provide fall-back scenarios
- iii build-in sufficient redundancy

D. as far as possible, limit (the impact of) an (imminent) event (response)

- i gather **information** and identify warning indicators (examples: forecasts of water levels, detect (non-) malicious disruptions of ICT infrastructure, monitoring of change and spread of viruses, intelligence analysis and production)
criterion: decide who gives what information / warning
- ii evaluate information and take decisions
- iii exchange and disseminate information between organisations
  - a example: exchange information about what measures companies and authorities (national and international) are taking
  - b example: dissemination of warning indicators / threat picture
- iv increasing citizens' **ability to cope** and **participate**

13 **escalate** to the level of control appropriate for the crisis

14 **alert and pass on alarms** to government administrations, ...??, companies and citizens

15 **decision-making and crisis coordination**
- i involving all relevant parties in decision-making (authorities, including international ones), vital companies, societal organisations, citizens)
- ii based on the available information, obtain understanding and overview of the situation
- iii imagine potential scenarios for the development of the crisis (including worst-case)
- iv take decisions (operational and administrative) at the appropriate level
- v if necessary, introduce emergency legislation/emergency powers
- vi coordinate / manage execution of decisions (incident location, between actors, between administrative levels)

vii take account of the consequences of the decisions taken (e.g. time required, road and transport capacity, social and political/administrative disruption)
viii prepare post-crisis situation

16 **incident fighting**
- i implement **disaster-fighting processes** (See 11.ii), if necessary with the support of the Defence Ministry
  - a guarantee the safety of help providers
  - b provide logistical support for incident fighting
- ii as far as possible (in the case of an acute threat) remove or restrict the source of the threat / event
- iii **as far as possible limit the spread** of the threat
- iv as far as possible limit the **impact** on people from the threat
  - a ensure certainty of supply
  - b distribute **scarce** resources optimally (strategy and implementation)
  - c use of physical emergency resources and technical and organisational emergency facilities

17 **public crisis communication** to inform citizens and enable them to act
- i draw up environment analysis with media picture
- ii decision-making on public communication: unambiguous and clear
  - a consider means to be used (website, disaster broadcast channel and figureheads (e.g. Mayor, expert))
- iii make sure possibilities for action are contained in any communications with citizens
- iv coordinate message with relevant actors/players (public and private, including internationally)

E. repair the damage and the consequences (after-care)

18 return to normal functioning of society
- i **repair** the damage (e.g. make affected area accessible)
- ii return of inhabitants
- iii economic recovery

19 **psychological and social after-care**

20 compensate the **loss sustained**

F. consider and implement measures intended to support A., B., C., D., and E. These do not in themselves make any direct contribution to security: *set up the policy process*

21 **preconditions**
- i maintain network of contacts with relevant services, organisations, firms and authorities (nationally and internationally)
- ii introduce the importance of national safety and security into relevant policy processes

22 identify threats / **risk-inventory**
- i carry out forward studies and produce scenarios
  - a gain insight into (the source of) threats to national safety and security (source)
  - b gain insight into the vulnerabilities of the five vital interests
    1. identification of vital sectors
    2. identification of vital services, processes and objects within the vital sectors
  - c gain insight into the vulnerabilities of vital sectors, including inter-sector dependencies (impact)

23 establishing the desired **security level**
- i requirements of certainty of supply
- ii security requirements for specific risks
- iii **tests** against standards (enforcement and oversight)

G. consider and implement measures intended to support A., B., C., D. and E. These do not in themselves make any direct contribution to security: *take actions*

24 decide which **actions** must be taken to achieve and maintain the desired security level
- i *see above tasks per specific intended effect according to the security chain*

criterion is interoperability of procedures, equipment and training

25 **prioritise** capabilities needed to implement tasks
- i based on the most objective possible (quantitative) methodology

26 **General constraints** for a national safety and security system
- i **task allocation,** responsibilities, powers between actors/players (government administrations, companies, societal organisations (national and international), citizens), whether laid down in (emergency) regulations or not
  - a make distinction for citizens between the ability to cope with a task and citizen participation tasks
  - b inform the various actors/players about tasks of others, and any limits to what will be done (managing expectations)
  - c subsidiarity is a criterion in this: assign responsibilities at the lowest possible level
- ii **encourage citizens to be active** (coping and citizen participation)
  - a inform citizens about their role
  - b create preconditions so that citizens can play their role
  - c monitor whether citizens are playing their role
- iii **activate vital infrastructure** (own continuity and vital role in society)
  - a inform vital infrastructure about its role
  - b create preconditions so that vital infrastructure can play its role
  - c monitor whether vital infrastructure is playing its role
- iv **activate companies and societal organisations** (own continuity and role in crisis control)
  - a inform them about their role and create preconditions so that firms and societal organisations can fulfil their role
  - b monitor whether companies and societal organisations are playing their role
- v ensure development, opening-up and **sharing of knowledge**

27 **evaluate** actions taken, learn lessons, implement points that have been learnt and monitor implementation
- i evaluate preventive measures
- ii evaluate preparation and exercises
- iii evaluate response after an event
- iv evaluate after-care

Sources used

1 Task list NSP 2006 (expert meeting)
2 Overview of tasks and capabilities Flooding Risk
3 Overview of tasks and capabilities Digital Paralysis
4 State Homeland Security – Program and Capability – Review Guidebook Volume I October 2005
5 Interim National Preparedness Goal DHS – Target Capabilities List
6 First Impression Report TMO – 'Waterproef' Exercise, 3-7 November 2008
7 Voorbereid on A grieppandemie! (Prepared for a flu pandemic) Handleiding continuiteitsmanagement voor de rijksoverheid, October 2008 (Continuity management manual for national government, October 2008)
8 Catalogus Civiel-Militaire Samenwerking (Civil-military cooperation catalogue), Defence Ministry and Ministry of Interior and Kingdom Relations, July 2007
9 CrisEZhandboek, Crisis Manual, Ministry of Economic Affairs
10 Taken bedrijfsleven (Tasks of business) (via Vitaal)
11 Response requirement based on National Planning Scenarios[8] in USA
12 Handboek operationele rampenbestrijding (Operational Disaster Fighting Manual). Deel (Part) B: operationele uitwerking (operational aspect[9]

8 February 2006
9 June 2003

Format
Tables for completion: impact criteria scenario assessment

This format can be used to record the scores of the 10 impact criteria. See sections 5.1 and 5.2 for a general explanation about the scoring system. See section 5.3 for an explanation about how to score the individual impact criteria.

You are asked to complete each score table for the 10 criteria with the scores/values V (forecast value), O (lower limit value) and B (upper limit value). If the criterion is not applicable because in principle, this type of impact cannot occur in the context of this scenario or comparable scenarios, tick the 'Not applicable' box.

Making an inventory of vital sectors affected

This table serves as a checklist for scoring the criteria, in particular C.3.1 (costs) an C5.1 (disruption of everyday life)

See section 5.3 for further explanation

☐ Electricity	☐ Maintenance of public order
☐ Natural gas	☐ Maintenance of public safety
☐ Oil & fuels	☐ Administration of justice and detention
☐ Telecommunications (fixed and mobile)	☐ Law enforcement
☐ Internet access	☐ Diplomatic communication
☐ Radio and satellite communication and navigation	☐ Information provision by government
☐ Postal and courier services	☐ Armed forces
☐ Broadcasting	☐ Main airport Schiphol
☐ Drinking water supplies	☐ Main port Rotterdam
☐ Food supplies/safety	☐ Main roads and main waterway network
☐ Emergency care/other hospital care	☐ Railways
☐ Drugs, sera and vaccines	☐ Transport, storage and production/treatment of chemical and nuclear materials
☐ Management of water quality	☐ Government financial payments
☐ Controlling quantity of water	☐ Payments traffic/payments structure

Territorial security

See section 5.3.1 for guidance about completing the tables below.

Criterion 1.1 Encroachment on the territorial integrity of the Netherlands

☐ Not applicable (see section 5.2 for explanation)

area → / time period ↓	local max. 100 km² (<0.25% of area)	regional 100 – 1,000 km² (0.25%-2.5% of area)	provincial 1,000 – 10,000 km² (2.5%-25% of area)	national > 10,000 km² (>25% of area)
2 to 6 days;				
1 to 4 weeks				
1 to 6 months				
1/2 year or longer				

	<250 pers/km²	250 – 750 pers/km²	> 750 pers/km²
Population density			

Criterion 1.2 Infringement of the international position of the Netherlands

☐ Not applicable (see section 5.2 for explanation)

extent ↓ / number indic. →	max. 1 indicator category	max. 2 indicator categories	max. 3 indicator categories
limited			
average			
considerable			

Physical safety

See section 5.3.2 for guidance about completing the table below.

Criterion 2.1 Fatalities

☐ Not applicable (see section 5.2 for explanation)

time ↓ / number →	< 10	10-100	100-1,000	1,000-10,000	> 10,000
Immediate death (within 1 year)					
Premature death (within 2-20 years)					

Criterion 2.2 Seriously injured and chronically ill

☐ Not applicable (see section 5.2 for explanation)

Number →	< 10	10-100	100-1,000	1,000-10,000	> 10,000

Criterion 2.3 Physical suffering (lack of basic necessities of life)

☐ Not applicable (see section 5.2 for explanation)

time period ↓ / number →	< 10,000 people	< 100,000 people	<1,000,000 people	>1,000,000 people
2 to 6 days;				
1 to 4 weeks				
1 month or longer				

Economic security

See section 5.3.3 for guidance about completing the table below.

Criterion 3.1 Costs

☐ Not applicable (see section 5.2 for explanation)

Costs in €	< 50 million	< 500 million	< 5 billion	< 50 billion	> 50 billion
1. damage to property					
2. health damage					
3. financial loss					
4. cost of combating the incident and repair					
Total economic loss					

Ecological security

See section 5.3.4 for guidance about completing the tables below.

Criterion 4.1 Long-term impact on the environment and on nature (flora and fauna).
A Impact on wildlife and scenery (flora and fauna)

☐ Not applicable (see section 5.2 for explanation)

Relative size → / Policy category ↓	<3%	3-10%	>10%
Nesting grounds of meadow birds			
National Ecological Network (EHS) areas			
Natura 2000 areas			
Waddenzee			
Is the duration of the harm longer than 10 years?			yes / no

Relative size is to be calculated from the area in hectares: for nesting grounds of meadow birds: 3% = 7500 ha (8,5 x 8,5 km), 10% = 25,000 ha (15 x 15 km); for National Ecological Network (EHS) sites: 3% = 10,400 ha (10 x 10 km), 10% = 43,710 ha (21 x 21 km); for Natura 2000 sites: 3% = 8,750 ha (9 x 9 km), 10% = 29,000 ha (17 x 17 km).

B Impact on the environment in the general sense (even outside wildlife and scenery areas)

☐ Not applicable (see section 5.2 for explanation)

Absolute area	local (max. 30 km^2)	regional (30 – 300 km^2)	provincial (300 – 3,000 km^2)	National (> 3,000 km^2)
Is the environment permanently damaged > 10 years)?				yes / no

Social and political stability

See section 5.3.5 for guidance about completing the tables below.

Criterion 5.1 Disruption to everyday life

☐ Not applicable (see section 5.2 for explanation)

number → / time period ↓	< 10,000 people	< 100,000 people	< 1,000,000 people	>1,000,000 people
1-2 days				
3 days to 1 week				
1 week to 1 month				
1 month or longer				

number of indicators applicable:

Criterion 5.2 Violation of the democratic system

☐ Not applicable (see section 5.2 for explanation)

number indic. → / time period ↓	Maximum 1 out of 6 indicators	Maximum 2 out of 6 indicators	≥3 out of 6 indicators
Days			
Weeks			
months			
1 or more years			

Number of indicators

Number of indicators >50% affected

Criterion 5.3 Social psychological impact (fear and anger)

☐ Not applicable (see section 5.2 for explanation)

	Indicator (see explanations)	irrelevant	relevant and therefore applicable			
		N/A	'none'	'limited'	'normal'	'considerable'
1 Perception						
1a	unfamiliarity					
1b	uncertainty					
1c	unnaturalness					
1d	disproportionate					
Totalled per intensity:						
Category 1 is significant (see explanation)						yes / no
2 Expectation pattern						
2a	blame					
2b	loss of trust in firms/authorities					
2c	loss of trust in emergency services					
Totalled per intensity:						
Category 2 is significant (see explanation)						yes / no
3 Possibility of action						
3a	lack of knowledge					
3b	no ability to cope					
Totalled per intensity:						
Category 3 is significant (see explanation)						yes / no
Total number of significant categories						1 / 2 / 3
Are there indicators that score 'limited', 'normal' or 'considerable'?						yes / no

number of significant categoriees→ final gradation ↓	0 significant categories	1 significant category	2 significant categories	3 significant categories
low		-	-	-
average				
high	-			

Are there perceptible expressions of fear and/or anger by fewer than 10,000 people lasting a maximum of 2 days? Yes / no

Are there perceptible expressions of fear and/or anger by more than 1,000,000 people (in 2 or more cities) for at least one week? Yes / no