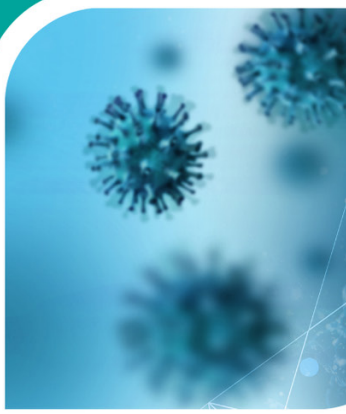
Belgian National Risk Assessment (BNRA)



National Crisis Center

BNRA

Better prepared. Better response.

Preface

The National Crisis Centre (NCCN) is very pleased to present the main conclusions of the Belgian National Risk Assessment (BNRA). In this report, you will find an overview of more than two years of work.

The BNRA is the result of intense cooperation between some of our internal departments and a large number of external experts from different fields and organisations. The NCCN would like to warmly thank these experts for their efforts. Collaborative working indeed forms the basis of this risk assessment. The NCCN remains committed to sustain its efforts to continue to further expand the panel of experts in the future, in order to maximise the sharing of knowledge regarding the numerous risks contained in this assessment.

The BNRA consists of 118 risks. Each of these risks was the subject of an in-depth study, eventually resulting in a correct definition, a clear description of the different scenarios (ranging from considerable to extreme) and a coherent assessment of the probability and potential impact of the risk. This gave rise to complex discussions with well experienced experts and to assiduous harmonisation work. The BNRA thus gathers an impressive amount of information.
This report provides an overview of this work.

As director-general a.i., I would like to express my pride regarding this in-depth analysis. The BNRA will form the basis of our understanding of risk management. Far from marking a completion, this analysis rather forms a starting point for many new developments and analyses that can lead to a better understanding of risks. This will enable us to introduce more targeted prevention and preparedness measures and manage crises more effectively!

Leen Depuydt

DG a.i.

Contents

Introduction

A European decision as a foundation

The Belgian National Risk Assessment finds its origin in Decision No 1313/2013/EU of the European Parliament and the Council on an EU Civil Protection Mechanism. Article 6 of this decision requires all Member States to submit a summary report consisting of two parts:

- A risk assessment, identifying the national risks likely to affect the country;
- An assessment of risk management capabilities, outlining the prevention and preparedness measures already implemented to address these risks.

All Member States are required to prepare a report for a three-year period. This BNRA is relevant for the period 2023-2026. By sharing risk assessments between Member States, we can exchange targeted information and best practices at European level. This allows for an effective and coherent approach to disaster prevention and preparedness within the EU mechanism.

This report is primarily aimed at Belgian organisations working in the field of risk management and national security.

One coordinator, one mission

The National Crisis Centre (NCCN) is the Belgian federal institution responsible for crisis management and coordination between the various key partners at the national level.

Its missions cover all stages of the risk cycle, the first stage being the identification and analysis of risks at national level (see Figure 1 below). The Belgian National Risk Assessment is an important part of this first stage and therefore falls directly under the responsibilities of the NCCN.

Figure 1 - Identification of the risk cycle as applied in Belgium, and its various stages.

The results of the BNRA provide important input for all subsequent stages of the risk cycle, such as the preparation and updating of emergency plans and procedures. The findings drawn from the BNRA contribute to more efficient emergency planning and a better understanding of crisis management. The iterative nature of the BNRA acts as a driver for continuously improving our understanding of the risks involved, enabling us to better anticipate and manage them.

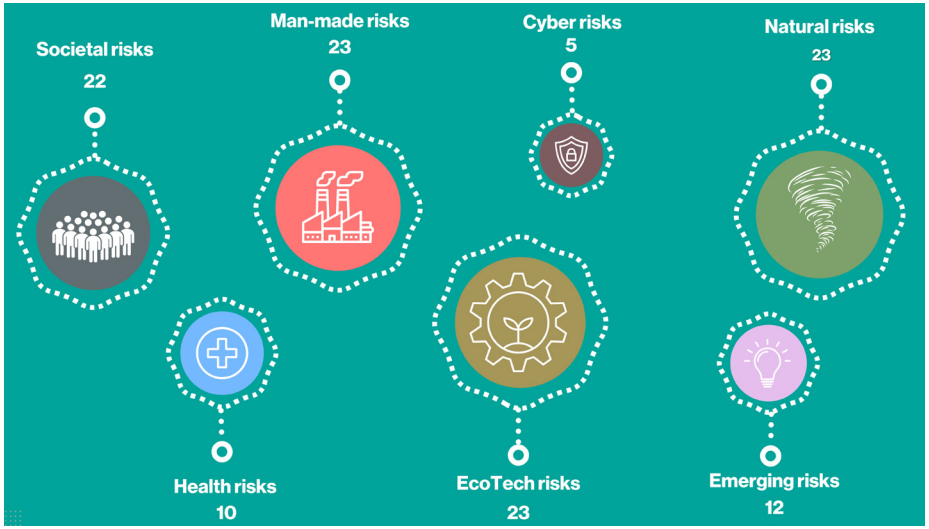
Methodology

The methodology developed by the NCCN for this BNRA and subsequent iterations is based on several existing national risk analysis methodologies, complemented by a handful of new elements.

A comprehensive risk catalogue

The risk catalogue forms the backbone of the BNRA. This catalogue contains a compilation of relevant risks that could significantly affect Belgium or that may have a major impact over the period 2023-2026. The selection of risks in this catalogue has previously been subject to an extensive benchmarking analysis of similar international risk assessments. In addition, any duplication or gaps between these selected risks have been carefully avoided.

The final risk catalogue for the BNRA contains 118 risks, divided into 7 categories, each of which was subject to an in-depth risk assessment.



For the sake of conciseness and relevance, this overview only includes a carefully considered selection of the risk catalogue (see page 12, section "Presentation of risk files").

Probability vs. impact

A risk is defined in relation to its probability and its impact. Probability refers to the likelihood of an event occurring. The consequences, or the effects of an event on society, constitute the impact of the risk.

The risks are then ranked according to the product of these two factors:

Risk= probability × impact

A detailed overview of the potential impact

The actual impact of an incident can occur in many different areas, such as the number of human fatalities, environmental degradation or financial losses. These are known as impact indicators.

The BNRA distinguishes ten different impact indicators divided into four impact categories: human impact, societal impact, environmental impact and financial impact. Each impact indicator is expressed in a specific unit (e.g. number of human lives lost vs km² vs €).

Human Impact	• Fatalities • Injured and sick people • People in need of assistance
Societal Impact	• Supply shortages and unmet human needs • Reduced public order and internal security • Damage to Belgium's reputation • Loss of confidence in the state and/or its values
Environmental Impact	• Damaged ecosystems
Financial Impact	• Damage to financial assets • Reduction in economic performance

In this report, you will always find the total impact score per category for each risk. This score is the combined total of all impact indicators within a given category.

A multi-scenario approach

For most of the hazards listed in the risk catalogue, it is possible to conceive a wide range of incidents (or, in some cases, incidents that have already occurred). In doing so, the impact can vary greatly from one scenario to another. Let's compare, for instance, a power cut that affects a single street for only a few hours to a country-wide power cut lasting several days.

Which of these scenarios is the most relevant for Belgium, or the most interesting in terms of prevention and preparedness measures? In the example of the power cut, this seems immediately obvious, but this is usually not the case. This is why the BNRA suggests three scenarios for each risk, with increasing levels of intensity. For each of these risk scenarios, a risk analysis is then carried out in order to identify the most relevant scenario for each risk.

Considerable scenario
- Relatively small impact
- Usually relatively high probability

Major scenario
- Relatively large impact
- Usually relatively low probability

Extreme scenario
- Very large impact
- Usually a very low probability

A focus on cascading effects

The BNRA does not examine each risk separately, but focuses on the causal links between risks and their cross-sectoral impacts. For example, a disruption of digital communications does not only affect the telecommunications sector, but can also have an impact on a wide range of other sectors, such as transportation and the medical sector.

Throughout the analyses, various experts have identified, described and quantified these relationships. This resulted in a network of interconnected risks. These links were then integrated into a mathematical model and automatically included in the final results of the risk analysis.

The present document does not elaborate on these cascades (although they are occasionally mentioned). However, these connections do form an integral part of the results being presented.

An extensive cooperation with domain experts

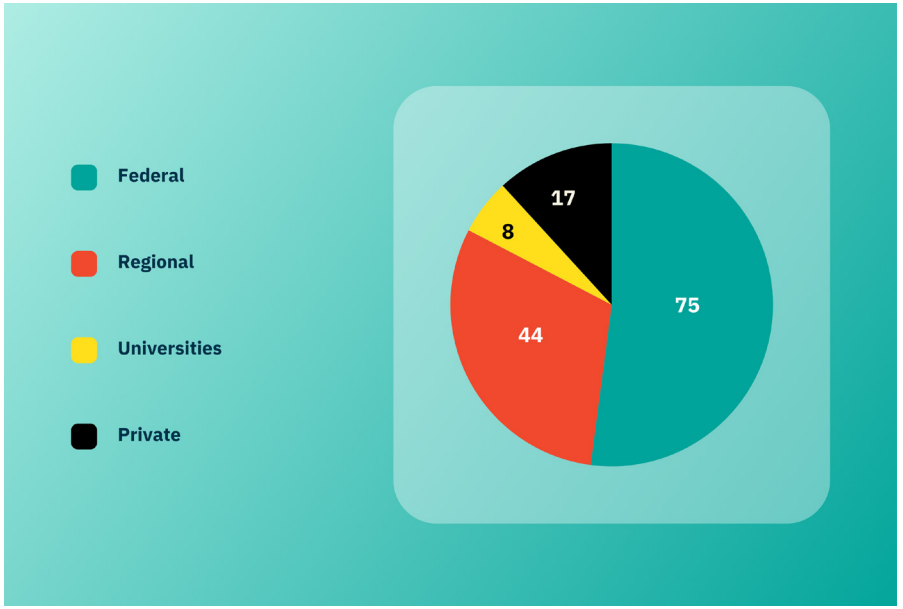
The development of our society's risk culture requires, first and foremost, a thorough understanding of each individual risk. To do so, the NCCN has selected a number of experts who have been asked, on a voluntary basis, to validate, assess and consolidate one or several risks.

Most of these experts originate from the public sector. In addition, academics and private operators were also actively involved at national level.

The methodology used in the BNRA calls for as many contributions as possible from the various panels of experts. The more contributions received, the more nuanced and precise the understanding of the risks.

All experts conducted the risk analyses according to their own level of knowledge. The accuracy of the analyses must therefore be approached with nuance. The analyses are a snapshot in time. It is therefore possible that they were influenced to a greater or lesser extent by events that occurred during the course of the assessment (March 2023 - March 2024). The findings also do not rule out the possibility of unforeseen extreme events occurring in the forthcoming period (also known as "black swans").

In total, more than 160 experts from about 140 different organisations were involved in the BNRA, providing input for one or several risks.



Addressing climate change and other emerging risks

While the estimates provided by the expert panels cover a period of three years into the future, the methodology also takes into account the fact that some risks cannot be adequately expressed within this limited timeframe. This is the reason why particular attention was paid to risks subject to climate change and new emerging risks.

In order to assess the impact of climate change, the BNRA also includes an estimate of the evolution of each risk up to 2050.

The experts have therefore assessed whether the probability of each of these risks could be expected to increase as a result of climate change and, if so, to what extent.

Furthermore, the BNRA has also examined eleven emerging risks. These risks were assessed on a purely qualitative basis. You will find more information on this in the chapter devoted to "Catalysing risks" (p. 51).

Risk matrix

Man-made risks

- M01 - Hybrid actor
- M06 - Attack against a CBRNe infrastructure
- M13 - Information operations
- M14 - Espionage
- M16 - Interference
- M17 - International armed conflict (IAC)

Cyber risks

- C04 - Cyberattack against a government institution
- C05 - Cyberattack against a vital infrastructure

Societal Risks

- S01 - Failure of electricity supply
- S02 - Failure of natural gas supply
- S03 - Failure of oil supply
- S06 - Failure of air transport
- S15 - Failure of digital infrastructure
- S19 - Failure of space based services

Economic and technological risks

- T05 - Nuclear plant incident (linked to "Release of radiation agents")
- T09 - Release of radiation agents (linked to "Nuclear plant incident")
- T16 - Dike failure
- T17 - Dam Failure

Health risks

- H01 - Infectious diseases
- H02 - Animal diseases excluding zoonoses
- H03 - Agricultural plant diseases & pests
- H04 - Levels of contaminants in food and feed

Natural risks

- N01 - Surface water flooding (see "Floods")
- N02 - Fluvial (river) flooding (see "Floods")
- N03 - Coastal flood (see "Floods")
- N13 - Drought
- N14 - Heatwave
- N17 - Wildfires
- N18 - Invasive species

Presentation of risk files

As mentioned earlier, this document contains information on only part of the risk catalogue. This selection consists of the most important risks per category (high probability and/or impact values), supplemented by some risks that have recently been in the public eye.

The risks in this report are listed in random order. Each risk file consists of two parts: a description and an analysis.

Description

In the first part of each file, the risk is defined as precisely as possible in a simplified form. To enhance readability, references of definitions are not included.

In addition, this report also describes the most relevant scenario. This is the scenario for which the score of probability x impact is the highest.

Analysis

The analysis part of each file focuses on probability, impact and possible cascading effects.

By way of example, the image on the right shows a graphical simplification of the main information obtained from the risk assessment for the 'most relevant scenario', namely: 1° the probability of the scenario occurring (which ranges from 'very small' to 'very large') and 2° a visual approximation of the impacts determined on the basis of the experts' input (from 'very small' to 'very large').

Part of the analysis is also dedicated to describing the 'cascading effects' of each risk. These are both the possible causes and the possible consequences that a risk can have.

Man-made risks

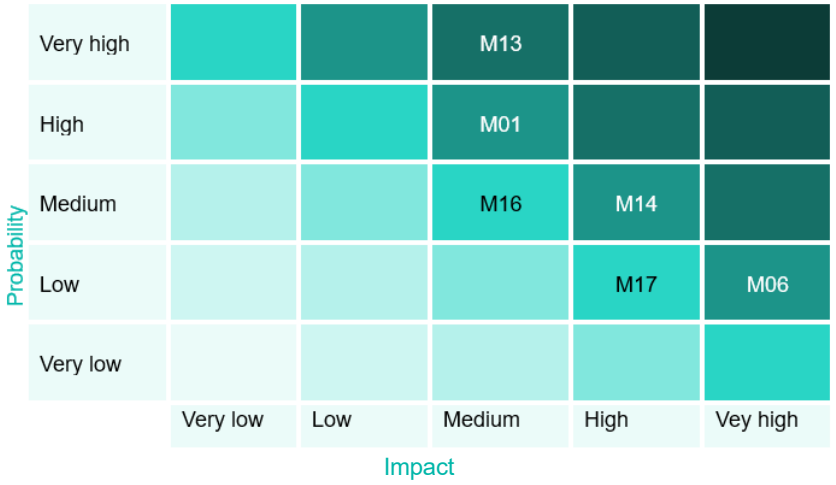
Man-made risks do not arise automatically, but are always carried out with malicious intent.
This section is therefore structured in two parts, namely an analysis of the different actors and an analysis of the different *modi operandi* they may use.

This section deals with hybrid actors. However, man-made risks can also be caused by terrorist groups, right-wing or left-wing extremist actors or criminal organisations. Each of these actors has its own preferred *modi operandi*. These can range from drug trafficking, espionage or interference, foreign direct investment to physical attacks.

In the present report, an attack on a CBRNe infrastructure is discussed because of the large-scale impact this risk could have if it were to occur.

In addition, the BNRA has also assessed other types of attack scenarios, such as attacks on a soft target, VIPs, vital infrastructures or groups of people or communities.

However, this assessment does not address all man-made risks. A selection of the most important risks has been made, along with a selection of certain very topical risks. The risks covered in this brochure are indeed closely linked to the current geopolitical context. It is therefore important to consider the results in the light of today's realities.



M01 - Hybrid actor
M13 - Information operations
M16 - Interference
M06 - Attack against a CBRNe infrastructure
M14 - Espionage
M17 - International armed conflict (IAC)

M01 - Hybrid actor

Description

The European Centre of Excellence for countering Hybrid Threats (Hybrid CoE) defines hybrid threats as follows:

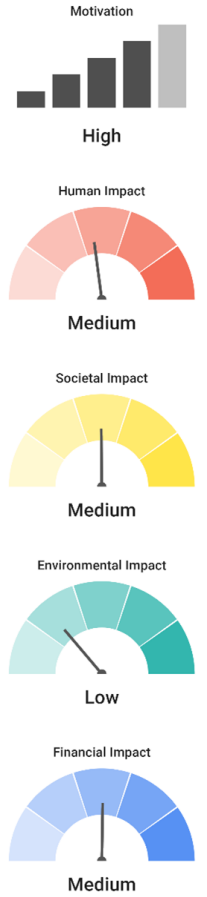
"The term hybrid threat refers to an action carried out by a state or non-state actor, aiming to undermine or harm a target by influencing decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronised with the aim of exploiting the vulnerabilities of democratic states and institutions. These activities can take place, for example, in the political, economic, military, civilian or information spheres. They are carried out using and in combination with a wide range of techniques and designed to remain below the threshold of detection and attribution."

The most relevant hybrid actor is an authoritarian regime opposed to European democratic values. The intentions are clearly malicious, the attack capabilities are high and there is a coherent strategy to engage in hybrid conflicts.

Analysis

In the current geopolitical context, it is not surprising that the above hybrid actors are highly motivated to carry out attacks against the West. An actor with considerable capabilities can use various tools and techniques to achieve its goal.

Continuously coordinated information operations aimed at polarising society, combined with cyberattacks on governmental, CBRNe and vital infrastructures undermine society's trust in their government. Espionage, interference and foreign direct investments are also used to achieve their own strategic goals or to destabilise the West.



M06 - Attack against a CBRNe infrastructure

Description

The most relevant scenario for an 'attack against a CBRNe infrastructure' is a deliberate physical attempt to destroy the infrastructure using all sorts of weapons to cause civilian casualties. CBRNe is the international abbreviation for chemical, biological, radiological, nuclear and explosive substances. CBRNe infrastructures are facilities that use or store CBRNe substances, such as Seveso and nuclear facilities.

Analysis

An attack on a CBRNe infrastructure will mainly be carried out by hybrid state actors seeking to destabilise our country. When such an attack is carried out by a state actor, this may lead to an international conflict.

While the probability of such an attack is low, the impact is certainly not. The destruction of a facility, for example, could result in the release of radioactive agents or other substances that could have a major human impact, causing many deaths and illnesses. Such an attack can also have a major financial impact, as facilities will have to be rebuilt and the immediately surrounding area sanitised. In addition, the affected facilities will be unable to provide services. Finally, such an attack will also instill fear in society and have an impact on the environment.

This type of event does not only affect Belgium. When such a site is close to the border, neighbouring countries can also be impacted.

M13 - Information operations

Description

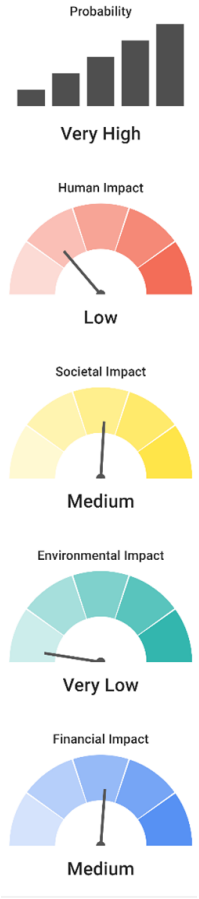
Information operations are actions aimed at influencing information and/or information systems to achieve a change in 1) the (potential) adversary's ability to act, 2) his understanding of the situation and 3) his ability to react. A change in any of these three factors is sufficient to disrupt the adversary's capabilities. Disinformation campaigns are a well-known example of this type of action, aimed, amongst others, at creating polarisation in society.

The most relevant scenario as far as information operations are concerned is that of an externally sponsored disinformation campaign via social media, lasting more than three months and specifically targeting Belgium. The campaign generated significant engagement: more than 100 000 likes, shares, tweets and/or retweets, with an actual reach of more than 10 000 people. The fake messages are spread through more than five channels (social, alternative and mainstream media) and are linked to an international incident.

Analysis

The societal impact of information operations cannot be underestimated. Foreign Information Manipulation and Interference (FIMI) aims at changing people's behaviour and creating polarisation. Depending on the context, this can cause immediate consequences and create panic. It can also lead to a larger part of the population refraining from critical thinking. If Belgium becomes the target of information operations, this could reduce citizens' trust in the government and seriously damage our country's reputation, both at home and abroad.

Information operations can also have a direct financial impact, depending on their nature. The objective of information operations is to stir up social divisions and influence individual cognitive behaviour, leading to different choices which, in turn, can influence the financial impact.



M14 - Espionage

DISCLAIMER

Espionage and interference are often mistakenly considered as going hand in hand. However, they should not be confused with each other. Espionage is an unauthorised way of obtaining information. Interference, on the other hand, involves the dissemination of misleading information to influence decision-making.

Description

Espionage is defined by the Intelligence and Security Services Act as: "*seeking or providing confidential information that is not publicly available, and maintaining confidential relationships that may facilitate such acts*". Malicious (state or non-state) actors may use various means (spies, cyberattacks, mechanical devices, etc.) to seek or obtain information that would otherwise be hidden or protected. The main motivations are most often the acquisition of commercial, technological or military know-how in order to gain an advantage over competitors.

In the most relevant espionage scenario, sensitive information likely to harm Belgium's military, diplomatic or economic interests is acquired. The actor involved disposes of considerable technological, financial and human resources so that the espionage operations can be carried out without being detected.

Analysis

The probability of such an act of espionage in the next three years is real. It is often caused through interference or by hybrid actors. Espionage can cause both direct and indirect damage. There may be a direct long-term impact on the Belgian economy. In addition, the societal impact of espionage can be significant, if it damages Belgium's reputation and affects our influence within multilateral fora such as the EU or NATO.

Moreover, this can fuel conspiracy theories, polarise society and erode trust in democracy. If the target of the espionage operation is an international organisation, the impact can also have cross-border consequences.

M16 - Interference

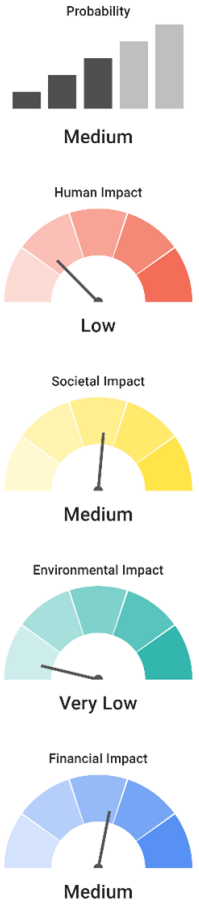
Description

Domestic or foreign interference includes intimidation, dissemination of misleading information and clandestine activities. These acts are carried out by or on behalf of an actor and go beyond normal diplomatic influence to shape decision-making processes. Influencing, on the other hand, is an overt and transparent attempt by foreign governments to influence the national public opinion on important issues to their advantage. The most relevant interference scenario focuses on the influence of individuals at the top of the decision-making process. This influence relates to issues linked to our national interests and can have permanent or long-term negative effects.

Analysis

Interference in Belgium can be the result of the work of various actors, including state actors through hybrid warfare or foreign direct investments[1]. Interference can result from espionage, by using stolen information to influence individuals, or it can even facilitate espionage. Some people who have been influenced may be more open to espionage. This can lead to disruptions in governmental operations. Interference of this magnitude can cause reputational damage to Belgium and lead to a loss of trust in the functioning of the government. Interference in Belgium's strategic interests and policies may also have (indirect) financial impact.

Belgium is at the heart of the international community, with EU and NATO institutions on its territory. Interference could therefore go beyond Belgian interests and target international policymakers or dossiers. This would not only affect Belgium but also the wider international community.



[1] The BNRA studied Foreign Direct Investment as a separate risk (M15), but did not identify it as one of the biggest risks. Therefore, it is not included in this document.

M17 - International armed conflict (IAC)

Description

An international armed conflict (IAC) is defined by the International Committee of the Red Cross as a situation in which states resort to armed force, even if the state of war is not recognised by any of them.

The most relevant scenario of an IAC takes place on NATO territory, but not within the borders of Belgium. Nevertheless, it is likely that such conflict will still require a significant deployment of Belgian military personnel and equipment in the area where the conflict is taking place.

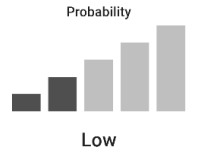
Analysis

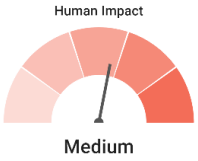
Experts consider the probability of this scenario as being rather low, but not non-existent, as geopolitical and economic tensions continue to increase. Belgium's membership of NATO also implies that Belgium could be involved in a conflict without being directly attacked.

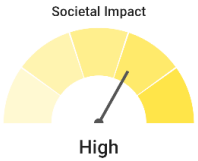
Malicious state actors are currently using various forms of hybrid attacks against Belgium and its allies. These attacks could trigger an IAC between NATO and its adversaries, especially if they increase in intensity or if the actor no longer remains below the detection threshold of detection.

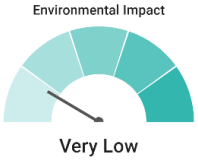
Such an IAC would have a major impact across several impact categories. Deployed military personnel are at risk, but supplies of food, raw materials and energy supplies (natural gas and oil) could also be compromised. On the financial front, public debt will increase and financial shocks are possible.

An influx of people from war zones in need of international protection is also very likely. Finally, there could be an increase in the number of attacks, particularly against vital infrastructures or CBRNe facilities.









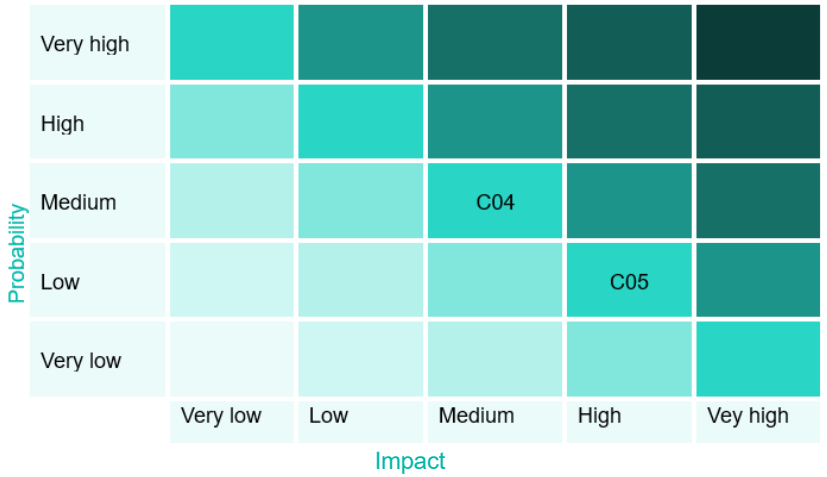
Cyber risks

In today's interconnected world, cyber risks have become pervasive and increasingly complex. From data breaches and ransomware attacks to state-sponsored espionage, the dangers in the cyber world are numerous and far-reaching.

The cyber risks in this analysis are always attacks with malicious intent. These attacks threaten the availability, integrity and confidentiality of information stored or processed in systems or transmitted over networks. Such an attack can take place by, amongst others, exploiting software and hardware vulnerabilities, software and hardware misconfigurations, or by using phishing or social engineering tactics.

Data breaches can lead to financial losses, reputational damage and legal liabilities. Ransomware attacks can cripple businesses and critical infrastructure and cause widespread disruptions.

Emerging technologies also always bring new challenges: as technology evolves, cyber risks also evolve.



C04 - Cyberattack against a government institution
C05 - Cyberattack against a vital infrastructure

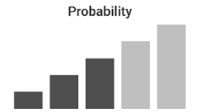
C04 - Cyberattack against a government institution

Description

A cyberattack carried out by a malicious actor on a government agency renders a central government or administration unable to perform its functions. The attack causes a security breach, resulting in the accidental or unlawful destruction, loss, modification, unauthorised disclosure or access to protected data transmitted, stored or processed. Government agencies related to defence, national security, public safety and law enforcement, as well as entities under the authority of the judiciary, parliament or central banks are excluded and covered by other risk files.

In the most relevant scenario of a cyberattack on a government agency, between 20 and 50% of computers are compromised by malware, leading to an IT service downtime of less than one day. The period from initial network breach by the actor to detection and removal is less than one month. As a result, 20-50% of partner organisations or citizens are affected by the virus, resulting in significant theft of classified data.

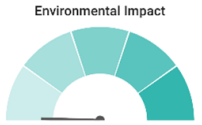
The stolen data could be used for espionage. Personal data or organisation charts may be used to identify persons of interest as targets. This could reduce public confidence in the government.



Medium

Very Low

Low



Very Low

Medium

Analysis

Depending on the intensity, duration and damage of the cyberattack, the financial impact can be significant. Cyberattacks can seriously disrupt and affect government and administrative services if they are successful. As these attacks become increasingly innovative and complex, the costs of protecting networks and infrastructure can be high. Depending on the severity of the attack and the content of the leaked sensitive information, Belgium's reputation may also be damaged.

C05 - Cyberattack against a vital infrastructure

Description

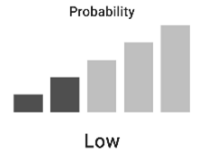
Cyberattacks can also target vital, digital and physical infrastructure, disrupting the operations and functioning of these infrastructures[1]. The most relevant scenario for this risk is a cyberattack against any vital infrastructure that provides physical, security or comfort needs to society and where the downtime of the IT -infrastructure exceeds one week.

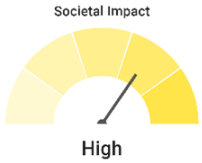
Analysis

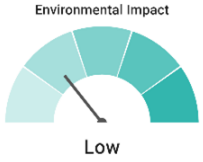
The probability of this scenario is low, but it could be carried out by malicious actors who want to destabilise the country or are looking for financial gain.

This scenario could have a significant financial impact. A successful cyberattack is usually accompanied by an expensive rebuilding of infrastructure and network security. If a cyber-attack leads to a disruption in gas supplies, for example, it can have direct and indirect costs, and both immediate and long-term consequences.

Cyber threats can also threaten the security of individuals and countries. The aim of a cyberattack is to cause damage, steal data or disrupt digital life in general. In the case of cyber espionage, the societal impact can be high, such as the loss of trust in the government and reputational damage for Belgium.





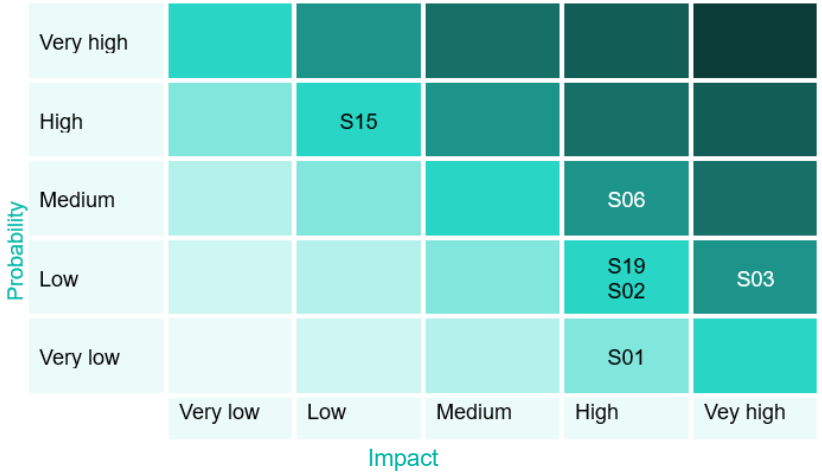


[1] According to the NIS2 Directive: electricity, heating and cooling, oil, natural gas, hydrogen, air, rail, water and road transport, financial services, financial markets, public health, drinking water, wastewater management, digital infrastructure, digital services, space services, postal and courier services, waste management, production and distribution of chemicals, production and distribution of food and industry.

Societal Risks

The current geopolitical context creates a dynamic threat landscape in which multiple types of risks and increased interdependence between infrastructures and sectors create a strong need for more resilient vital services.
After all, these services play an indispensable role in maintaining vital societal functions and economic activity. They are fundamental to the survival of our society. Access to drinking water, food, healthcare, government services and other institutions all contribute to individual needs for physical safety and comfort. A disruption of these vital services will therefore have an immediate and tangible impact on the resilience of Belgian society.

At present, the European Union has already drafted the CER and NIS2 directives, in which a large number of vital sectors have been identified.
This section describes and analyses the probability and potential impact of "a failure of" some of these catalogued services, which are essential to the security and needs of the population. In general, these risks can have a significant societal and financial impact.



S01 - Failure of electricity supply
S02 - Failure of natural gas supply
S03 - Failure of oil supply
S06 - Failure of air transport
S15 - Failure of digital infrastructure
S19 - Failure of space based services

S01 - Failure of electricity supply

Description

A disruption of the electricity supply can take several forms. A power outage usually refers to a partial or complete loss of electricity supply to an end user (e.g. the population, businesses, critical systems). An electricity crisis refers to a current or imminent situation where there is a significant electricity shortage on the supply side. Disruptions can occur in the form of brown-outs (voltage drop) or black-outs (voltage loss).

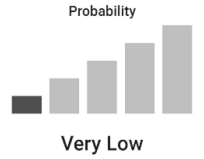
The most relevant scenario for a disruption of the electricity supply is a nationwide black-out lasting at least one day. A complete restart (black-start) is required and several critical sites on the electricity grid are damaged. Power imports from neighbouring countries are limited or even unavailable.

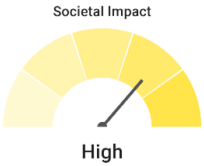
Analysis

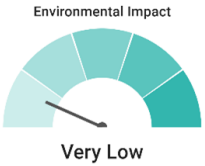
Analyses show that this risk is very low.
This is mainly due to the maturity of the sector, the numerous measures and legal obligations already in place and the general crisis preparedness for dealing with such disruptions. This risk is nonetheless addressed in this report because of the societal importance of electricity supply.

A disruption could result from physical or cyberattacks on certain critical parts of the energy infrastructure. Despite its low probability, this scenario has a significant impact. The societal impact is by far the most important category for this risk.

Almost the entire Belgian population and businesses would be without electricity for the duration of the black-out. The sectors with the largest expected impact include the food sector, the transport sector and the health sector.







S02 - Failure of natural gas supply

Description

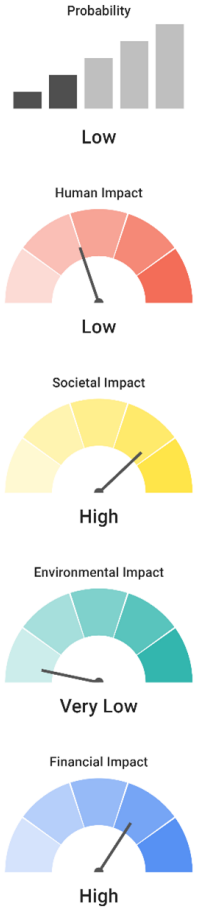
In the event of a national disruption of natural gas supply, the volume of natural gas injected into the Belgian grid (via imports, withdrawal from storage and local production) is lower than the volume of natural gas withdrawn from the Belgian grid (via consumption or transport to neighbouring countries). In the event of a real disruption of the supply of natural gas, the imbalance cannot be resolved by the regular market actions of market players. Instead, the measures of the federal emergency plan for natural gas supply (alarm or emergency) must be deployed.

The most relevant scenario is that of a nationwide disruption of natural gas supply. To address the shortage in natural gas, substantial emergency measures have to be taken, as defined in the FPS Economy's Federal Natural Gas Emergency Plan. This would obviously also have a cross-border impact, as such situation would require neighbouring EU countries to show solidarity.

Analysis

Cyberattacks and international armed conflicts are the most likely causes of such disruption.
They can be interrelated and even occur simultaneously. The societal impact of such a disruption depends on the duration and severity of the cyberattack and the location where the armed conflict takes place. The impact is likely to be severe as human needs can no longer be met due to the lack of heating. Some industrial sectors are expected to close down, which could cause unemployment and financial losses.

If the disruption of natural gas supply continues, it could lead to a significant reduction in economic performance and a loss of trust in the government from citizens and employers.



S03 - Failure of oil supply

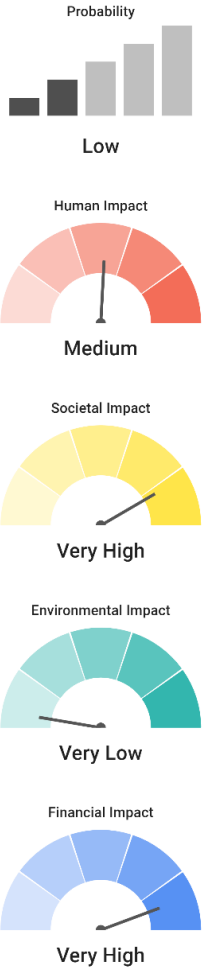
Description

A disruption of oil supply occurs when the demand for oil or petroleum products exceeds their availability. The cause may be limited availability or unusual consumption. However, most disruptions result from situations where the supply of oil or petroleum products is interrupted, impacting distribution to end-users. These disruptions can be the result of problems at international (e.g. geopolitical instability and/or conflicts) or local level.

The most relevant scenario with regards to the disruption of oil supply affects the whole country and neighbouring countries. The government takes measures to reduce long-term demand, by releasing national emergency stocks and triggering solidarity measures (EU, IEA).

Analysis

The causes for an oil supply disruption are very diverse, but the most likely one is an international armed conflict in an oil-producing region.
The financial impact should not be underestimated. A shortage of oil will seriously affect the petrochemical sector and the transport of goods and people. This could lead to a significant reduction in economic activity. The government must therefore take measures to reduce the demand of oil or petroleum and to restrict supply to priority consumers. This implies that some non-priority consumers could potentially be completely cut off or restricted to a maximum purchase programme for a certain period of time. This may have a negative societal impact.



S06 - Failure of air transport

Description

Air transport refers to any movement of goods and/or passengers in an aircraft (OECD). A failure occurs when air transport is interrupted, resulting in difficulties in transporting passengers or goods according to a pre-defined schedule.

The most relevant failure of air transport scenario involves the destruction or unavailability of a vital airport infrastructure. This destruction affects the provision of services at all regional and international Belgian airports for more than ten days and has an impact on the provision of services at airports beyond and close to our national borders. As a result, rerouting in the surrounding area is unavailable.

Analysis

The analysis shows that the disruption of digital infrastructure is the main cause of aviation disruptions. Communications between air traffic control towers and aircrafts on the ground or in the air are indeed crucial.

The societal impact of a failure of air transport should not be underestimated. The scenario assumes that goods can no longer be transported by air, which could lead to supply shortages and failures of the provision of essential services to the population.

In addition, a failure of air transport of this scale could also have a significant financial impact on airline companies.

Take-off and landing strips or aircrafts could become unusable and may have to be replaced. This risk also implies that Belgium's economic performance would suffer significantly.

S15 - Failure of digital infrastructure

Description

Digital infrastructure is a generic term encompassing all telecommunications and information technologies and operations. The most well-known are mobile phone networks (4G, 5G, etc.) and the internet. A disruption leads to difficulties or the impossibility of transmitting messages or data.

The scenario under consideration involves a nationwide interruption of telecommunication services of a single provider for less than one hour.

Analysis

This scenario is considered quite likely as multiple historical events of similar magnitude can be recalled.

The impact of such a failure is mainly of a societal and financial nature. Many people will not be able to use their regular online services or means of communication during the disruption, and possibly for longer.

With increasing connectivity and digitalisation, many service providers rely on digital infrastructure. However, increasing resilience and redundancy measures are being implemented. A failure of the digital infrastructure primarily affects the aviation sector, as it is heavily dependent on national infrastructure and communication providers. Air traffic could be interrupted for the duration of the disruption. This would lead to capacity problems and would have a huge financial and societal impact (e.g. passengers and freight would not reach their destinations on time, or even at all).

S19 - Failure of space based services

Description

Space based services refer to operational services that use space technologies placed in orbit around the Earth. These services include:

1. Positioning, Navigation and Timing (PNT) information received from Global Navigation Satellite Systems (GNSS);

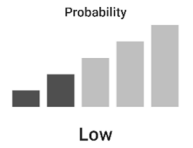
2. The provision of satellite imagery for the organisation of emergency services, including data for weather forecasts and alerts;

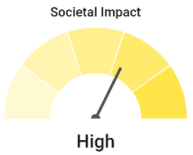
3. Communication services such as broadband Internet and data transfer services for civilian, military and commercial users.

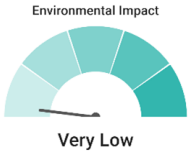
The most relevant scenario for this risk is an outage that simultaneously affects several types of services, lasting more than seven days and causing irreversible damage.

Analysis

Space technologies provide crucial support for military, commercial and civilian activities.
They contribute to weather forecasting, the effective functioning of banks and stock markets, power grids, all types of transport and emergency operations, not to mention nuclear and conventional deterrence and crisis prevention. Whether the cause of a disruption is natural (e.g. solar storm), technical (e.g. space debris collisions or cyberattacks) or geopolitical (e.g. foreign direct investments or international armed conflict), the impact of such disruption can be significant. If space services are interrupted for several days, affecting by nature various countries, the societal and financial impact would be significant, due to the disruption in the provision of the above mentioned services and the significant cost of repairing or replacing the space infrastructure.





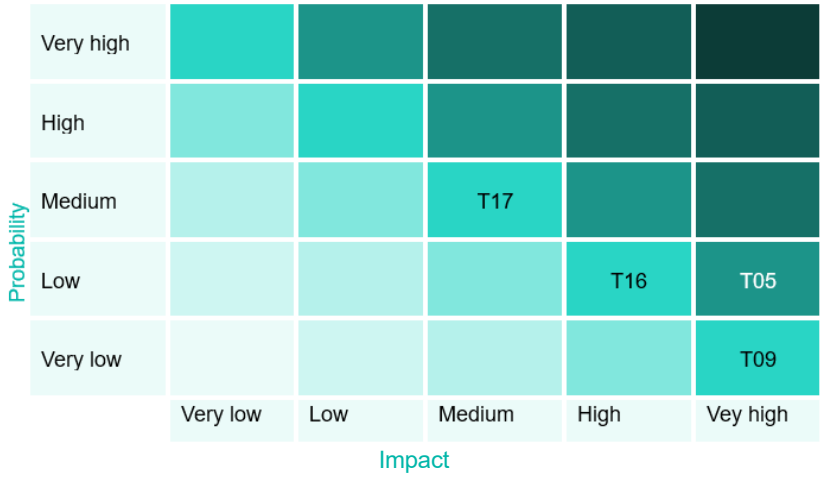


Economic and technological risks

Economic and technological risks are risks related to industrial incidents and incidents involving infrastructures (e.g. dike or dam breaches, bridge failures). This category focuses mainly on industrial and nuclear incidents, the release of hazardous substances (biological, chemical, nuclear or radioactive substances) and transport accidents (air, rail or road).

All these risks are and remain very important and permanent threats to society as a whole. However, their probability and harmful effects have often been reduced to a lower level of risk due to the many protective measures already in place, such as stronger safety policies, industrial controls and regulations, and surveillance systems.

As a result, some of these risks are now often considered acceptable. Nevertheless, prevention and protection measures remain essential for both current and future industrial safety.



T05 - Nuclear plant incident (linked to "Release of radiation agents")
T09 - Release of radiation agents (linked to "Nuclear plant incident")
T16 - Dike failure
T17 -Dam Failure

T05 and T09 - Nuclear plant incident with release of radiation agents

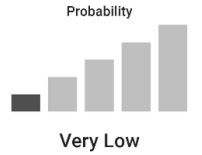
Description

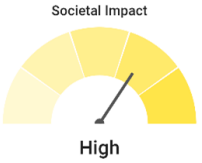
A nuclear power plant uses uranium and other fissile elements as nuclear fuel to produce steam for electricity generation. This process also generates residual fission products, which are radioactive. If an accident were to occur at a nuclear power plant, heat and pressure build up and the steam can be released along with radioactive agents.

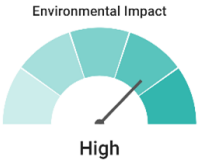
Depending on the extent of the incident and the exposure to the radioactive material, such an incident could pose a danger to human health. Radioactive material can also be hazardous to the health of animals, other life forms and the environment.

Analysis

The probability of an extreme incident occurring at a nuclear power plant seems rather unlikely, given the many protection and safety measures that are taken preventively. If radioactive agents are released in an incident, the human impact could be very high. Weather conditions may spread the radioactive agents and affect the population. Thus, persons undergoing high radiation doses could face serious health risks, such as injuries and life-threatening illnesses. Affected persons would have to be evacuated or housed in a safe area. Given that residual radiation levels may remain present in the affected area indefinitely, it may be uninhabitable for centuries. This will also have a major financial impact, e.g. the cost of decontamination of the affected area.







T16 - Dike failure

Description

A dike is a structure usually made of earth or concrete that protects land from water. It often runs parallel to the floodplains of a river or along low-lying coastlines. A dike failure occurs when part of a dike or its foundation collapses or shifts so that it can no longer retain water. This can release large amounts of water, causing risks to people or properties downstream. To take into account the reality in Belgium, locks and active dikes are also included in this risk file.

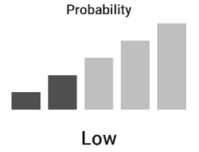
The most relevant scenario involves the breach or failure of a long and high dike, affecting a large densely populated area for several weeks.

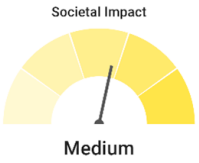
Analysis

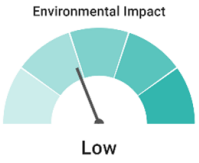
The main causes of dike failure are related to various phenomena or incidents that lead to the physical weakening of the dike, such as erosion, soil subsidence, landslide, dam failure and floods. Flooding is undeniably the main consequence in the affected areas.

A dike breach has a substantial financial impact, considering the enormous damage to surrounding homes, infrastructure and assets. Economic performance may be reduced for a considerable time due to inactivity of affected businesses and services. The human and societal impact can be significant as a large proportion of the affected population loses their homes and faces shortages of basic supplies.

In the future, climate change may lead to more dike breaches because of rising sea levels and increasingly strong river flows.







T17 - Dam failure

Description

There are two types of dams in Belgium:

- The large dams in the East of Belgium: their functions are the supply of electricity and the storage of drinking water ;
- River dams: these are built on the main navigable rivers and canals with rugged topography. They regulate the flows and levels of rivers and ensure inland waterways traffic. Weirs also fall under this group.

A dam breach occurs when part of a dam or its foundation collapses or shifts so that the dam can no longer hold back water. This releases large flows of water, posing risks to people, property and infrastructure downstream. Hydraulic infrastructures, such as dikes, weirs or dams further downstream, are particularly vulnerable.

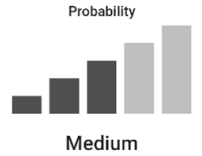
The most relevant scenario is that of a dam that overflows, releasing larger than normal water flows downstream for the next few hours or days.

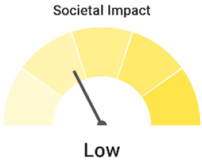
Analysis

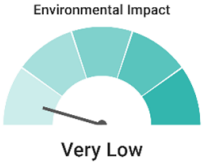
The main expected immediate effect is a major financial and social impact. Indeed, properties in the affected areas may suffer severe damage. A large part of the affected population may lose their homes and face shortages of basic services.

In the future, climate change may lead to more frequent overflow of dams due to increasingly frequent floods.

However, monitoring systems and emergency plans have recently been improved to ensure risk prevention as much as possible.







Health risks

This section describes risks that can affect human health and the quality of the environment. They are mainly caused by severe disturbances or changes in the environment (e.g. pollution of air, water or soil), contamination of food and the emergence of dangerous diseases affecting humans, animals and plants.

Like the COVID-19 pandemic, such crises have already occurred in recent years, both in Belgium and Europe. Health risks are common and mainly affect humans and the environment, which can have a substantial financial impact.

In addition, the societal impact can also be significant and lead to the disruption of essential services for the population, such as healthcare, and a serious loss of public confidence in the government.

Psychological risks, such as the mass rejection of modern medicine or processes of a socio-psychological nature, such as mass hysteria, are also discussed in this chapter, but in reality they hardly ever occur. Should they nevertheless occur, the potential effects would be less significant and mainly relate to human and societal levels.

H01 - Infectious diseases
H02 - Animal diseases excluding zoonoses
H03 - Agricultural plant diseases & pests
H04 - Levels of contaminants in food and feed

H01 - Infectious diseases

Description

Infectious diseases are illnesses caused by pathogens (such as a virus, bacterium, protozoan, macroparasite, prion, viroid and fungus) or their toxic products, which are transmitted from an infected individual, animal or infected object to a human host.

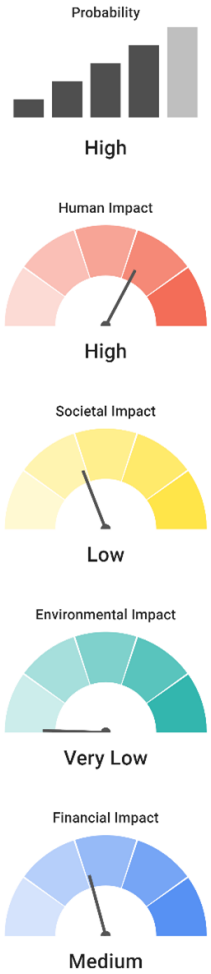
The most relevant scenario for this risk file is a situation where a disease is transmitted by air, resulting in a medium to high mortality rate. Even if a treatment is available, the pressure on hospital capacity remains high.

Analysis

Infectious diseases are responsible for a huge global disease burden that impacts public health services and economies worldwide, disproportionately affecting vulnerable populations.

Every two to five years, severe respiratory viruses are feared in winter in the form of seasonal influenza, COVID or a combination of several known respiratory viruses. Such conditions can pose a public health problem and increase pressure on healthcare systems.

The BNRA results show the same trend at Belgian level resulting in a very significant human impact, including many deaths and a higher number of sick patients. This could lead to staff shortages and, in the long term, to a reduction in Belgium's economic performance.



H02 - Animal diseases excluding zoonoses

Description

Non-zoonotic animal diseases are defined as infectious diseases that only affect animals. These animals can include both wild animals and livestock. Infectious diseases that can be transmissible to humans (zoonoses) are not included.

The most relevant scenario involves a highly transmissible or infectious disease with a high mortality rate, affecting all animals and with few or no drugs or regulatory measures available.

Analysis

An animal epidemic corresponding to an extreme scenario could potentially occur in the decades to come. Well-known examples are African swine fever, Newcastle disease virus in poultry and wildlife, and distemper in North Sea seals, which is transmissible to dogs. Invasive exotic species can also introduce animal diseases. The risk of the emergence of new species (such as mosquitoes and ticks) capable of spreading new diseases is significant, especially in the context of climate change.

The human impact is small, but real: the repercussions on livestock, which may require slaughter, can be profound for farmers. The societal impact of an extreme animal epidemic is considered quite low. Human needs (in case of temporary unavailability of meat due to affected livestock) and/or Belgium's reputation could be affected, for instance by introducing trade embargoes to limit the risk of the disease spreading.

The environmental impact of such an epidemic is estimated to be low. However, depending on the type of epidemic, a large proportion of wildlife could be affected. Moreover, the food pyramid of other species could be disrupted, causing indirect effects.

H03 - Agricultural plant diseases & pests

Description

This risk includes the following situations: bacterial contamination of plants, fungal infection, viral, mycoplasma and viroid plant disease epidemics and infestation by insects. Diseases and pests affecting crops are spread not only through environmental factors, but also through global trade, travel, traffic and transportation.

The most relevant scenario considers a highly contagious and easily transmissible disease or pest affecting food resources of major national or European importance. Several types of crops are affected. Possible treatment is available, but with limited distribution.

Analysis

The main causes, apart from direct outbreaks, are invasive species and hailstorms. In the latter case, crops that have endured hail are weakened, making them more vulnerable to pests and diseases.

If a disease affects a plant or crop that is of great importance for food supply and few treatments are available, it can have a significant social impact on the food supply. Indeed, such a disease affecting agricultural plants can lead to crop failure and, as a result, seriously compromises food production for humans and animals. This would not result in immediate famines or large-scale food shortages, but it can limit food choices. The societal impact is the consequence of such a situation for food production.

The possibility that one or more types of crops would be unavailable for a long period of time could affect human needs. Nevertheless, the national disease detection network would quickly detect such a disease.

H04 - Levels of contaminants in food and feed

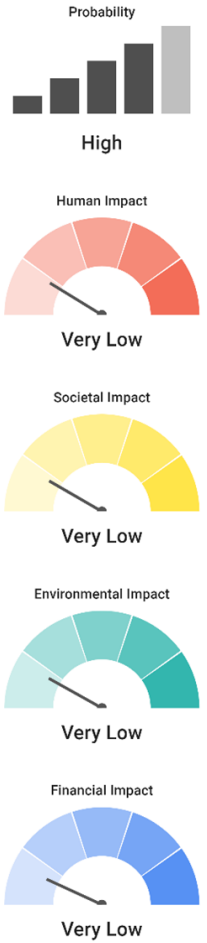
Description

A contaminant refers to any substance which is not intentionally added to (an ingredient of) food or feed (for food-producing or non-food-producing animals) but is nevertheless present as a result of production (including operations carried out for agriculture, animal husbandry and veterinary medicine), or as a result of environmental contamination. A contaminated liquid component is also taken into account.

The most relevant scenario implies a situation of limited consumption and therefore limited transmission. The product in question does not pose an immediate health risk, but symptoms may possibly appear after some time. The product could be recalled fairly quickly.

Analysis

The impact of this risk is rather limited, but the probability is high. The human impact mainly relates to indirect effects, such as spread of dangerous products or bacteria. In most cases, the government takes immediate action in the event of contamination of the food chain, which means that the impact on humans remains very limited. However, there could be a societal impact as a result of the product being withdrawn from the market, and a financial impact due to the economic losses that could be incurred by the producer.



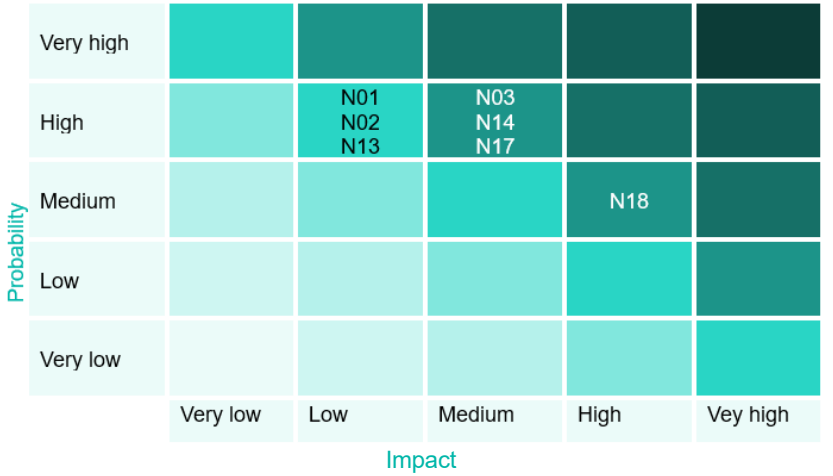
Natural risks

Natural risks include risks associated with all types of extreme weather conditions (e.g. floods, droughts, heat and cold waves, storms, tornadoes, hail, snow, ice and frost, lightning), various types of geophysical processes (e.g. soil subsidence and uplift, riverbank erosion) and extraterrestrial hazards (meteorites and solar radiation storms).

Most natural risks occur independently of human activity. An exception to this concerns the effects of the carbon footprint on climate change and the protective measures implemented to prevent natural risks from occurring and causing other significant risks.

In general, these risks are characterised by a significant environmental impact. Depending on the severity of the risks, societal and financial impacts can also be high. Human impact is generally limited, but there are exceptions, such as heatwaves and floods.

Special attention should be paid to the recent floods of 2021 which have strengthened expert warnings in their assessment of this risk. This is discussed further in the chapter.



N01, N02, N03 - Floods
N14 - Heatwave
N18 -Invasive species
N13 - Drought
N17 - Wildfires

Floods

Description

This section is a summary of three BNRA risk files (N01, N02 and N03), which discuss different types of flooding.

1° **Surface water (pluvial) flooding** refers to flooding caused by excess water not directly connected to a major river or navigable watercourse. Usually these are areas located in basins or particularly exposed to high water levels when rainfall is unusually intense and severe. Flooding occurs when the amount of rainfall exceeds the capacity of the soil or the drainage/sewerage system to absorb the water (e.g. due to dry soil preventing infiltration or saturation of the sewerage system).

2° **Fluvial (river) flooding** occurs when the water level of a watercourse (river, stream, canal) or body of water overflows into adjacent low-lying areas (the natural floodplains) that are not normally flooded, regardless of the cause.

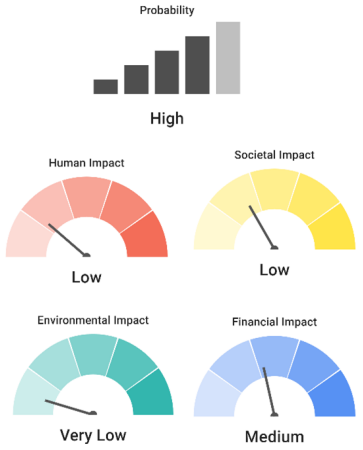
3° **Coastal flooding** is the inundation by the sea of land areas along the coast and the tidal zones of major rivers in estuaries. Coastal flooding usually results from storm surges and violent winds coinciding with high tides.

Analysis

Flooding is a phenomenon with a wide range of consequences. For any type of flood, there will be a very serious financial impact, with many direct and indirect economic losses. Coastal floods are even more devastating in this respect given the concentration of infrastructure along the coastline and the importance of maritime transport.

Floods have few identifiable causes. The amount of rainfall in a given area is, of course, the most common. With coastal flooding, it is also important to take account of the critical importance of protective structures, such as dikes and dams, and the consequences of their possible failure.

The most relevant scenarios that emerge from the BNRA tend to be small-scale and affect only a few areas. Nevertheless, recent events have shown that Belgium is not immune to far more catastrophic situations and large-scale flooding. Moreover, floods can have numerous consequences, including incidents with infrastructures (energy or CBRNe) and the release of hazardous substances, as well as the spread of invasive species. Therefore, damage to protective infrastructure, especially dikes, should not be overlooked.



N13 - Drought

Description

A drought is a period of abnormally dry weather that lasts long enough to cause, due to lack of precipitation, a severe hydrological imbalance between surface water and groundwater (which includes both deep and shallow aquifers).

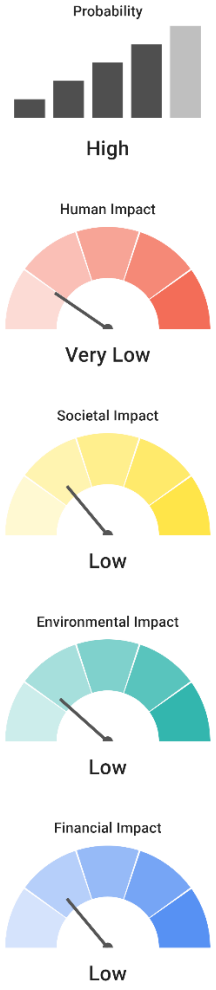
The most relevant drought scenario is a regional drought that does not affect more than three provinces, lasts up to six months and is characterised by the desiccation of soils and the drying up of small local rivers, but with no long-term effects observed.

Analysis

Droughts are not caused by other risks and their probability of occurrence is very high for the period 2023-2026. For the period 2050-2053, experts have not identified a clear trend regarding the effect of climate change on its probability of occurrence. The estimates therefore remain unchanged.

The proposed drought scenario has a relatively limited impact. Environmental impacts are almost exclusively caused by drought itself. Wetland ecosystems are likely to be the most affected.

Drought also creates indirect impacts. Populations may be impacted if drinking water supply is disrupted by water shortages. Soil dehydration due to drought can lead to soil movement, which in turn can lead to disrupted drainage systems and contribute to societal impacts. The financial impact results mainly from government deficits, as it is expected that insurance companies will no longer be able to bear the burden of drought alone.



N14 - Heatwave

Description

There is no universally accepted definition of a heatwave.

In Belgium, the Royal Meteorological Institute refers to a national climate heatwave when maximum temperatures in Uccle reach at least 25.0°C for at least five consecutive days and reach the 30.0°C threshold for at least three days.

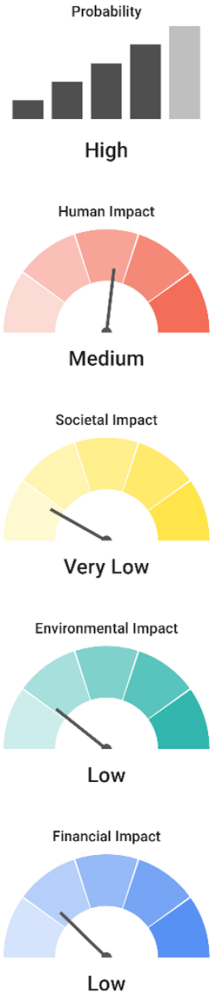
The most relevant heatwave scenario lasts less than 15 days and affects five to ten provinces. Maximum temperatures reach 30°C between five and ten days, with maximum temperatures going above 35°C for at least two days and average night-time temperatures remaining below 20°C.

Analysis

Heatwaves are not caused by other risks. Their probability of occurrence is very high for the period 2023-2026 and even slightly higher for 2050-2053 due to the effects of climate change.

If one considers the damage caused by heatwaves, it can be observed that they mainly have an impact on human health. The societal, environmental and financial impacts of heat waves exist but are quite limited.

One of the significant effects of a heatwave is chronic air pollution. This will affect the most vulnerable people and lead to numerous medical complications (e.g. chronic illnesses) or even hospital stays, possibly resulting in death.



N17 - Wildfires

Description

Wildfires are:

- Unplanned or uncontrolled fires that start in natural areas such as woodlands, grasslands, organic areas (peat, wetlands), agricultural land, moorland or dunes and which may affect industrial and residential areas as they spread;
- Unplanned or uncontrolled fires that begin to spread in the border zone between wildland and urban areas and which may affect natural, industrial and residential areas as they spread.

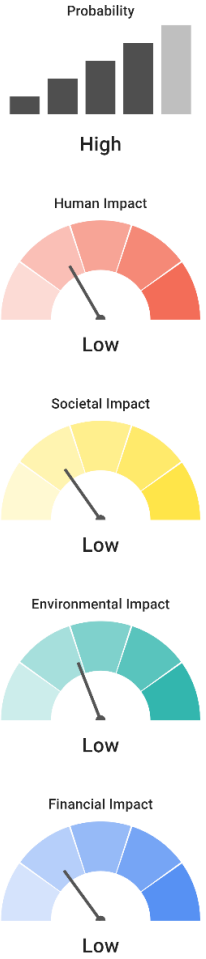
The most relevant scenario is a very severe wildfire that damages between 50 and 500ha in a natural area with limited use (≤ 1 000 visitors per day) and threatens one to two residential or recreational areas.

Analysis

Wildfires have a very high probability of occurrence. Other risks that cause wildfires (such as lightning, and various types of incident and accident hazards) contribute only in a very limited proportion to the overall probability of wildfires.

The various impact categories of wildfires are equally represented, with environmental impact being the most significant. It should be noted that the indirect effects resulting from forest fires are the main contributors to these impacts.

This is because wildfires create empty spaces that are subsequently colonised by invasive species, which in turn generate different forms of impact. If the wildfire occurs near our national border, there may also be a cross-border impact.



N18 - Invasive species

Description

An invasive alien species (abbreviated IAS or "invasive species") is a species that has been introduced or has spread outside its natural range by human activities, and has subsequently disseminated. Such a species poses a threat to biodiversity and/or ecosystem services, such as supply (materials, molecules...), cultural services (tourism...), regulation (climate, diseases, floods...) or the biological cycle (photosynthesis, nitrogen cycle...).

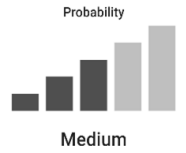
The most relevant scenario is that of a blacklisted invasive species, for which the exposure and impact parameters are very high.

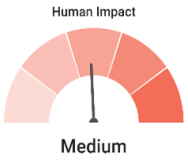
Analysis

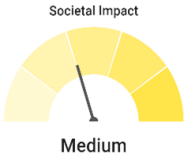
In addition to direct human activities, the main causes of this invasive species scenario are wildfires and fluvial floods.

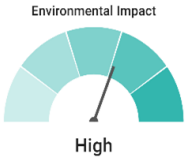
The environmental impacts are predominant, as invasive species threaten native species (plants or animals) and the functioning of ecosystems. Nevertheless, some species can also have an impact on human health, such as allergies to stings of Asian hornets (*Vespa velutina*) or ragweed pollen (*Ambrosia artemisiifolia*), chemical reactions to certain plants (burns) or the development of zoonotic diseases (e.g. raccoons - *Procyon lotor)* or infectious diseases, such as the tiger mosquito (*Aedes albopictus*) which spreads dengue fever.

The societal and financial impacts are not negligible either, as shown for example by the risks posed by Japanese knotweed (*Fallopia japonica*) to infrastructures (e.g. damage to foundations, sewers ...) or the burrows dug by animals in dikes.









Catalysing risks

Emerging risks

As mentioned in the introduction, the BNRA also takes into account eleven emerging risks. These risks do not yet pose a real danger to society, but may have an effect on all the other risks from the BNRA. This effect may be positive and provide opportunities for society, but it can also manifest itself in a negative way.

As these phenomena are still developing, it is uncertain what development path they will follow. It is therefore impossible to assess them in the same way as other risks. The effects of the emerging risk (if any) on the other risks should ideally be described quantitatively, but given the lack of historical data and knowledge to base these assumptions on, a qualitative approach is preferred.

Emerging health Risks

E12 – Antimicrobial resistance

+	−
This phenomenon creates a constant need for new research on antibiotics and antimicrobials. As a result, science will continuously push forward and improve.	When bacteria, viruses, fungi and parasites react less or not at all to drugs, antibiotics and other antimicrobials become less effective and infections become increasingly difficult to treat.

E09 – Biohacking

+	−
Biohacking can correct errors in the genome and manipulate genes in cells and organisms, for example to correct a disease or susceptibility to a disease.	Scientific research is still needed into the effects of gene modification. There is also the ethical issue regarding the limits of this practice. For example, biohacking can also be used to modify a person's physique or abilities.

Emerging technological risks

E02 – 5G

+	−
5G will provide near-everywhere connectivity, at very high speeds (ultra-fast data sharing) and low-latency (near real-time network responsiveness) not only for individual users, but also to a whole range of vital societal and economic services	5G may bring numerous new security challenges: • Local or global disruption; • Spying on traffic/data; • Modification or redirection of traffic/data; • Destruction or alteration of other digital infrastructures or information systems. Combined with increased reliance on 5G networks for economic and societal functions, these challenges could potentially have negative consequences.

E03 – Artificial intelligence

+	−
AI can provide all kinds of benefits for individuals and services. For example, it can help detect and combat a number of risks, such as cyberattacks, disinformation and exploitation of systems vulnerabilities.	AI can be used to carry out cyberattacks, spread disinformation, interfere in public affairs, exploit service vulnerabilities, and so on.

E06 - Blockchain technology en cryptocurrencies

+	−
Blockchain is a peer-to-peer distributed ledger system that eliminates the need for a centralised management entity such as a bank. Cryptocurrency is an application based on blockchain technology. Currencies are traded between investors, but there is no central authority managing them.	Some people, such as criminals, also use cryptocurrency to make it difficult or even almost impossible to trace their activities.

E07 - Internet of things (IOT)

IOT is a network of devices that communicate with each other via the internet or other communication networks. It offers many opportunities in industry, agriculture, but also for private use, for example in smart homes, smartwatches and cars.

More connected devices means more digital security issues, such as outdated software, lack of cyber security or device failures, more risks of misconfiguration and more entry points for attackers.

E08 - Quantum computing

Quantum computing allows us to tackle mathematical problems that even the most powerful classical supercomputers could never solve.

Many cybersecurity pillars revolve around encryption, and quantum computing can break this encryption. This could be a major risk to the digital security of our society. Our cybersecurity will have to adapt accordingly, and the challenge will be to develop and deploy post-quantum cryptography.

Emerging societal

E04 - Energy transition

The energy transition is a pathway leading to the transformation of the global energy sector from fossil fuels to carbon-free energy by the second half of this century. To limit global warming to 1.5°C, carbon neutrality must be achieved by the middle of the 21st century.

The consequences of a change in energy supply are multiple: shifts in energy prices, EU and international politics, ecological risks but also new technological risks, risks for energy supply and resource management (including potential conflicts) and financial instability.

E05 - Systemic interdependence

Interdependencies encourage cooperation and synergies between stakeholders. They offer numerous benefits that contribute to the efficiency, resilience and innovation of economic and societal systems through specialisation.

The disruption of one infrastructure can propagate across all infrastructure systems through its digital or physical connections, generating cascading disruptions that can escalate into a broad crisis.

E10 - Polarisation of society

Party politics, activism and dissent can lead to conflict and polarisation (in the form of distance between different viewpoints or beliefs). If these are given a constructive place and do not lead to hostility, that is part of democracy.

In cases of dislike or hostility between groups, tensions between them can become harmful and threatening, and coexistence is put under pressure. A highly divided community with inter-group hostilities and strong "us versus them" thinking is the ideal breeding ground for radicalisation. In extreme cases, this can even lead to violence.

E11 - Erosion of privacy

People have unconsciously relinquished their privacy, which makes life in society significantly easier, for instance in terms of national security, healthcare, transparency and online services. Personal data is also an important resource for researchers for scientific research.

The risk is directly linked to the degree of access to personal data that a malicious actor would have and the masses of data that he can exploit for other purposes. This leads to risk of misuse (including but not limited to identity theft and fraud, surveillance and tracking, manipulation and influence, discrimination and exclusion).

E01 – Climate change

Compared to other emerging risks, the phenomenon of climate change has already been intensively studied in recent decades, resulting in more scientific data available. Climate scientists are constantly striving to better predict, with fewer uncertainties, the future impacts of climate change. the existing scientific uncertainties, it was decided to also consider climate change as an emerging risk within the BNRA.

To mitigate the potential impacts of climate change, measures should be taken as soon as possible. To determine what measures are needed to make societies more resilient to the effects of climate change, we need to raise awareness and gain a better understanding of what to expect.

The BNRA attempts to gain these improved insights by estimating how climate change may induce changes for any other risks analysed. This estimation is not done for the current period (2023-2026), but for the period 2050-2053, which is assumed to be a relevant period as it overlaps with the timeframes of the strategic policy plans currently being developed.

Since climate change has been studied in more detail than most other emerging risks, experts have estimated its effects on other risks quantitatively rather than qualitatively.

The risk scenarios likely to be influenced by climate change remain unchanged. The same is true for the associated impacts. For example, heatwaves should have a similar impact in 2023 or in 2050 (without taking into account additional measures that might be adopted in the meantime).

Changes due to climate change are therefore only expressed by the probability (i.e. the direct probability of their occurrence, and therefore not as a result of other hazardous events) of risks sensitive to climate change. For example, the experts were asked how the probability of heatwaves would change between 2023 and 2050 as a result of climate change.

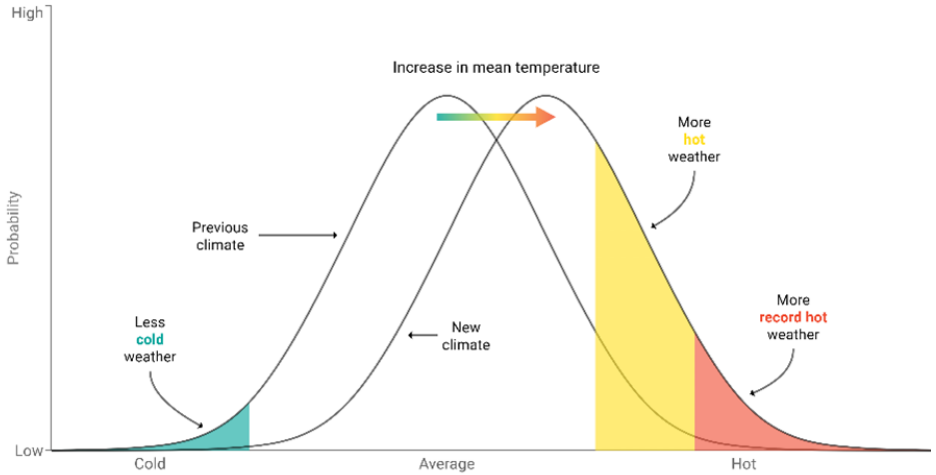


Figure 2: Impact of climate change on the probability (x-axis) of extreme events (y-axis) occurring (IPCC, 2007)

As shown in Figure 2, climate change is expected to create a new climate leading to an increase in the frequency of hot periods (the yellow area becomes larger).

To carry out these estimates in a coherent way, the experts involved in the BNRA have defined a common understanding of climate change.

This means that a single climate scenario has been used in the framework of their projection of future climate change.

The risks with the highest probability of increasing by 2050-2053 are listed in the table below:

N18 - Invasive species: Climate change will further increase the number of already established invasive species and contribute to their future spread. Moreover, it will promote the establishment of new species. As experts believe that invasive species cause **H02 - Animal diseases** and **N06 – Riverbank erosion**, the likelihood of these two risks may also increase by 2050.
T16 – Dike Failure: Dikes in Belgium are generally constructions that are several decades old. As these were never designed to withstand modifications induced by climate change (for example to take into account the effects of a rising sea level), we can expect a growing number of failures in the absence of adaptation measures. As experts believe that failing dikes cause **N03 - Coastal Flood**, the number of floods could also increase by 2050.
N04 - Coastal erosion and shoreline change: As the probability of storm surges increases in 2050 and sea levels continue to rise, coastal erosion and shoreline change will become more frequent.
S13 – Failure of drinking water supply: Experts believe that contamination of drinking water could increase by 2050. This increased water pollution could be due to burst pipes, poorly contained pollution or even technical problems within water treatment plants.
M17 - International armed conflict: With climate change, some areas will experience climate disasters, become uninhabitable (e.g. sea level rise) or experience crop failures resulting in food shortages (e.g. drought or floods). This could destabilise a region and disrupt communities, almost inevitably leading to international armed conflict. According to experts, international armed conflicts are one of the major causes of the **M23 - Inflow of people in need of international protection** risk, and the occurrence of this latter risk could also increase by 2050.

Concluding remarks

The Belgian National Risk **Assessment** (BNRA) is first and foremost an assessment process based on **probability and impact indicators**.
It is not intended to predict the unforeseeable. It is therefore important to specify that risks described as "black swans", or **unpredictable extreme events**, may not have been identified.

This report provides information on **29 of the 118 risks examined within the BNRA**. The proposed selection consists of the **most important risks (high probability and/or impact values)** by risk category (cyber, health, man-made, natural, societal, economic and technological), supplemented by some risks that have been brought to public attention due to relevant incidents in recent years.

A new innovative **risk assessment methodology** has been developed for this BNRA. It sets a new standard for future national risk assessments in Belgium. Future iterations will build on its merits and allow for further improvements.

Risks are presented in **a fixed format** consisting of a brief description followed by an analysis. These are grouped into risk categories and are **not ranked in any way**.

Each risk studied was assessed and consolidated by a group of domain experts. **More than 160 experts from nearly 140 organisations** were involved in conducting the analyses. The presence of a wide range of experts is essential to obtain meaningful results that are widely supported.

The experts are the heart of the BNRA and their many contributions are therefore indispensable.

The BNRA does not only consider risks as isolated events, but also took into account **cascading effects**, which help to understand the cause-and-effect relationships that exist between risks. However, it did not examine "composite risks" i.e. multiple independent risks occurring simultaneously.

A "**polycrisis**" is a concept that can describe today's complex risk landscape. It is an ambiguous and volatile reality in which crises and/or emergencies do not occur sequentially, but in which different evolutions in the risk and/or crises landscape in different domains develop simultaneously, are interconnected and even reinforce and influence each other. **Additional analysis of polycrises** is beyond the scope of this BNRA.

The results of the risk assessment are valid for the period 2023-2026. Thereafter, a new iteration will be carried out.

Key lessons from the BNRA

Risks in the **man-made** category generally have a high impact and most of them also have a relatively high probability. With the exception of one, the risks presented are not directly related to attacks, but rather linked to geopolitical tensions and influence strategies, whether hybrid threats, espionage or disinformation. In an increasingly connected world, the most serious **cyber risks** are generally linked to man-made activities (malicious and intentional), either with criminal intent or as part of a hybrid threat. The probability is often quite high, but the impact can vary depending on the scenario.

Societal risks can be divided into two broad categories:

- "HILP" risks (high impact, low probability): risks with a very high impact but a low or very low probability, such as energy supply disruptions;
- Risks with a higher probability and particularly high societal and financial impacts, such as disruptions in the aviation sector.

Economic and technological risks are generally "HILP" risks. Prevention and preparedness measures, as well as continuous monitoring, appear to significantly reduce the likelihood of occurrence, but it is clear that continuous efforts are still required.

The most relevant scenarios for **health risks** tend to be low-impact situations. However, for serious events such as infectious diseases, high societal and human impacts cannot be ruled out.

Natural risks have generally been assessed with a high probability, even though the impact varies greatly from one risk to another. Most of the scenarios described relate to specific, small-scale situations, with the exception of invasive species.

Finally, the analysis of **emerging risks** provides a glimpse of the future and potential development paths for existing risks. **Climate change**, in particular, will significantly increase the likelihood of many major or extreme natural risks by 2050. Consideration of their cascading effects shows that most risks are indirectly influenced by climate change in one way or another.

Risk catalogue

Cyber risks

- C01 - Software/hardware vulnerability
- C02 - Misconfiguration of software and hardware
- C03 - Cyberattack against a CBRNe infrastructure
- C04 - Cyberattack against a government institution
- C05 - Cyberattack against a vital infrastructure

Emerging risks

- E01 - Climate change
- E02 - 5G
- E03 - Artificial intelligence
- E04 - Energy transition
- E05 - Systemic interdependence
- E06 - Blockchain technology and cryptocurrency
- E07 - Internet of things (IOT)
- E08 - Quantum computing
- E09 - Biohacking
- E10 - Polarisation of society
- E11 - Erosion of privacy
- E12 - Antimicrobial resistance

Health risks

- H01 - Infectious diseases
- H02 - Animal diseases excluding zoonoses
- H03 - Agricultural plant diseases & pests
- H04 - Levels of contaminants in food and feed
- H05 - Chronic pollution of ambient air
- H06 - Chronic pollution of aquatic environment
- H07 - Chronic pollution of soil
- H08 - Substandard and falsified medical products
- H09 - Mass rejection of modern medicine
- H10 - Processes of a social psychological nature

Man-made risks

- M01 - Hybrid actor
- M02 - Left-wing extremist actor
- M03 - Right-wing extremist actor
- M04 - Organised crime actor
- M05 - Religious extremist actor
- M06 - Attack against a CBRNe infrastructure
- M07 - Attack against a government or international institution
- M08 - Attack against a group of people or community
- M09 - Attack against a soft target
- M10 - Attack against a VIP
- M11 - Attack against a vital infrastructure
- M12 - Attack on a transport of dangerous goods
- M13 - Information operations
- M14 - Espionage
- M15 - Foreign direct investments
- M16 - Interference
- M17 - International armed conflict (IAC)
- M18 - Drug trade
- M19 - Economic fraud
- M20 - Human trafficking and smuggling
- M21 - Civil unrest
- M22 - Strike
- M23 - Influx of people in need of international protection

Natural risks

- N01 - Surface water flooding
- N02 - Fluvial (riverine) flood
- N03 - Coastal flood
- N04 - Coastal erosion and shoreline change
- N05 - Subsidence and uplift
- N06 - Riverbank erosion
- N07 - Landslide or debris flow
- N08 - Cold wave
- N09 - Icing

- N10 - Snow
- N11 - Hail
- N12 - Lightning
- N13 - Drought
- N14 - Heatwave
- N15 - Wind
- N16 - Tornado
- N17 - Wildfires
- N18 - Invasive species
- N19 - Earthquake
- N20 - Tsunami
- N21 - Volcanic eruption abroad
- N22 - Solar radiation storm
- N23 - Meteorite impact

Societal Risks

- S01 - Failure of electricity supply
- S02 - Failure of natural gas supply
- S03 - Failure of oil supply
- S04 - Failure of hydrogen supply
- S05 - Failure of district heating
- S06 - Failure of air transport
- S07 - Failure of rail transport
- S08 - Failure of naval transport
- S09 - Failure of road transport
- S10 - Failure of financial services
- S11 - Failure of medical care supply
- S12 - Failure of medicine supply
- S13 - Failure of drinking water supply
- S14 - Failure of sewage disposal
- S15 - Failure of digital infrastructure
- S16 - Failure of digital service providers
- S17 - Failure of emergency organisations
- S18 - Failure of central public administration
- S19 - Failure of space based services
- S20 -Failure to supply postal and courier services
- S21 - Failure of food supply
- S22 - Failure of waste disposal

Economic and technological risks

- T01 - Incident in a CBRNe facility
- T02 - Incident in a Seveso installation
- T03 - Incident involving the transport of CBRNe substances
- T04 - Discharge of explosive agents
- T05 - Nuclear plant incident
- T06 - Release of biological agents
- T07 - Release of chemical agents
- T08 - Release of nuclear agents
- T09 - Release of radiation agents
- T10 - Air transportation accident
- T11 - Road traffic accident
- T12 - Rail accident
- T13 - Marine accident
- T14 - Inland waterways accident
- T15 - Bridge failure
- T16 - Dike failure
- T17 - Dam failure
- T18 - Building structural failure
- T19 - Fire of explosion in an urban or residential area
- T20 - Fire in or collapse of a tunnel
- T21 - Commodities shortage
- T22 - Financial shock
- T23 - Governmental deficit

Towards a more resilient Belgium

As we noticed in light of extreme events such as the floods of 2021, a lack of knowledge of the right reflexes can make emergency management even more complicated. The resilience of the population and the infrastructures to various risks is now a key word in society, but one that must continue to be learned and passed on.

This is not only a strict necessity in Belgium, but also a requirement of the European Union. The systemic interdependencies (cascades) now identified will continue to increase for the foreseeable future. The growing diversity of potential (cross-border) risks in a Europe with fewer internal borders has led to the CER Directive being drawn up and adopted by all Member States in 2022. This directive is dedicated to the resilience of critical entities and their respective sectors. As the implementation of the CER Directive only targets a few critical sectors, it will not achieve a uniform level of resilience across the whole of society. However, as new recommendations, new risk assessments and resilience measures strengthen these vital sectors, they will most likely have positive effects for other sectors not covered by the CER Directive.

One of the main objectives of this National Risk Assessment is therefore to make a modest contribution to the development of a risk culture in Belgium and to increase the resilience of our society as a whole. The results are valid for a period of three years, but mid-term reviews and new analyses may be carried out at federal level as at other levels (regions, provinces, sectoral) to update the current results or assess them in more detail and prepare the next iteration.

Safety and security are everyone's business. First and foremost, this requires sufficient knowledge of the potential risks facing Belgium.

National Crisis Center

September 2024

Hertogsstraat 53
1000 Brussel

www.crisiscenter.be

National Crisis Centre
CrisisCenter Belgium
Crisiscentrum / Centre de Crise