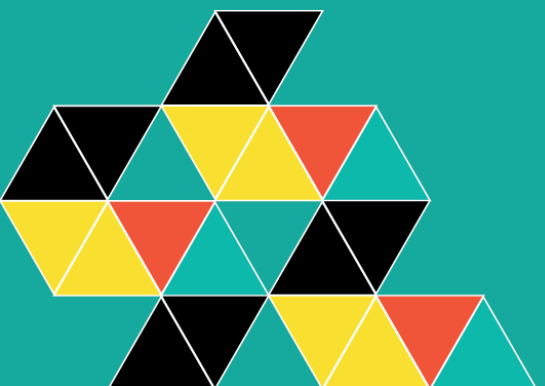
Belgian National Risk Assessment (BNRA)



Centre de crise National

BNRA

Anticiper pour mieux gérer.



Avant-propos



Le Centre de crise National (NCCN) est très heureux de présenter les conclusions principales de la *Belgian National Risk Assessment* (BNRA). Vous trouverez dans ce rapport un aperçu de plus de deux ans de travail.

La BNRA est le résultat d'une coopération intense entre certains de nos départements internes et un grand nombre d'experts externes issus de différents domaines et organisations. Le NCCN tient à remercier chaleureusement ces experts pour leurs efforts. Le travail collaboratif constitue la base de cette évaluation des risques. Le NCCN s'engage à prolonger ses efforts pour continuer d'étendre le panel d'experts dans le futur afin de maximiser le partage des connaissances quant aux nombreux risques contenus dans cette évaluation.

La BNRA comporte 118 risques. Chacun de ces risques a fait l'objet d'une étude approfondie qui a permis d'aboutir à une définition correcte, à une description claire des différents scénarios (du considérable à l'extrême) et à une évaluation cohérente de la probabilité et de l'impact potentiel du risque. Ceci a donné lieu à des discussions complexes avec des experts chevronnés et à un travail d'harmonisation assidu. La BNRA recueille ainsi une quantité impressionnante d'informations. Le présent rapport donne un aperçu de ce travail.

En tant que directrice générale a.i., je voudrais exprimer toute ma fierté pour cette analyse approfondie. Cette BNRA constituera le socle de notre compréhension en matière de gestion des risques. Loin de marquer un achèvement, cette analyse constitue plutôt un point de départ pour de nombreux développements et de nouvelles analyses qui peuvent conduire à une meilleure compréhension des risques. Ainsi, nous pourrons prendre des mesures de prévention et de préparation davantage ciblées et gérer les crises encore plus efficacement !

Leen Depuydt

DG a.i.

Table des Matières

Avant-propos 2

Introduction 3

- Au départ, une décision de l'UE 4
- Un coordinateur pour une mission 4

Méthodologie 5

- Un catalogue complet des risques 5
- Probabilité vs. impact 6
- Une analyse détaillée de l'impact potentiel 6
- Une approche multi-scénarios 7
- Un focus sur les effets cascade 7
- Une collaboration étendue avec des experts du secteur 8
- Regard sur le changement climatique et les autres risques émergents 9

Matrice des risques 9

Présentation des fiches de risque 11

Risques "man-made" 12

- M01 - Acteur hybride 14
- M06 - Attaque contre une infrastructure CBRNe 15
  M13 - Opérations d'information 16
- M14 - Espionnage 17
- M16 - Ingérence 18
- M17 - Conflit Armé International (CAI) 19

Risques Cyber 20

- C04 - Cyberattaque contre une institution gouvernementale 22
- C05 - Cyberattaque contre une infrastructure vitale 23

Risques sociétaux 24

- S01 - Défaillance de l'approvisionnement en électricité 26
- S02 - Défaillance de l'approvisionnement en gaz naturel 27
- S03 - Défaillance de l'approvisionnement en pétrole 28
- S06 - Défaillance du transport aérien 29
- S15 - Défaillance des infrastructures digitales 30
- S19 - Défaillance des services spatiaux 31

Risques économiques et technologiques 32

- T05 et T09 - Incident dans une centrale nucléaire avec libération d'agents radioactifs 34
- T16 - Défaillance d'une digue 35
- T17 - Défaillance d'un barrage 36

Risques sanitaires 37

- H01 - Maladies infectieuses 39
- H02 - Maladies animales non zoonotiques 40
- H03 - Maladies des plantes agricoles & pestes 41
- H04 - Contaminants dans la nourriture humaine et animale 42

Risques naturels 43

- Inondations 45
- N13 - Sécheresse 47
- N14 - Vague de chaleur / Canicule 48
- N17 - Feux de forêt 49
- N18 - Espèces invasives 50

Risques catalyseurs 51

- Risques émergents 52
- E01 - Changement climatique 56

Remarques finales 59

- Principaux enseignements de la BNRA 60

Catalogue des Risques 61

Vers une Belgique plus résiliente 63

Introduction

Au départ, une décision de l'UE

La *Belgian National Risk Assessment* trouve son origine dans la décision du Parlement européen et du Conseil de l'Union européenne n° 1313/2013/UE, établissant le mécanisme de protection civile de l'Union. L'article 6 de cette décision exige que tous les États membres soumettent un rapport de synthèse composé de deux parties:

- Une évaluation des risques, indiquant les risques nationaux susceptibles d'affecter leur pays;
- Une évaluation des capacités de gestion des risques, énumérant les mesures de prévention et de préparation déjà mises en oeuvre pour faire face à ces risques.

Tous les États membres doivent préparer un rapport pour une période de trois ans. Ce rapport, appelé BNRA est valable pour la période 2023-2026. En partageant les évaluations des risques entre États membres, nous pouvons échanger des informations ciblées et les meilleures pratiques au niveau européen. Ceci permet d'adopter une approche efficace et cohérente de la prévention et de la préparation aux catastrophes dans le cadre du mécanisme de l'UE.

Ce rapport s'adresse principalement aux organisations belges travaillant dans le domaine de la gestion des risques et de la sécurité nationale.

Un coordinateur pour une mission

Le Centre de crise National (NCCN) est l'institution fédérale belge responsable pour la gestion des crises et la coordination entre les différents partenaires clés au niveau national. Ses missions couvrent toutes les étapes du cycle du risque, la première étape étant l'identification et l'analyse des risques au niveau national (voir ci-dessous Figure 1). La *Belgian National Risk Assessment* est une partie importante de cette première étape et relève donc directement des responsabilités du NCCN.



Figure 1 – Identification du cycle du risque en usage en Belgique, et ses différentes étapes.

Les résultats de la BNRA constituent un apport important pour toutes les étapes suivantes du cycle du risque, telles que la préparation et la mise à jour des plans et procédures d'urgence. Les enseignements tirés de la BNRA contribuent ainsi à la mise en oeuvre d'une planification d'urgence plus efficace et à une meilleure maîtrise de la gestion des situations de crise. La nature itérative de la BNRA sert de moteur pour améliorer en permanence notre compréhension des risques afin de mieux les anticiper et les gérer.

Méthodologie

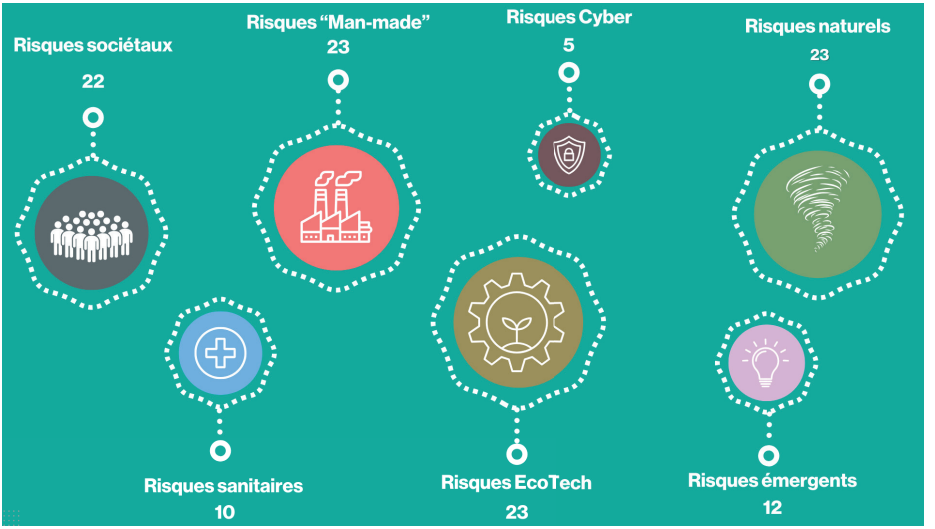
La méthodologie développée par le NCCN pour la BNRA et ses futures itérations est basée sur plusieurs méthodologies nationales d'évaluation des risques existantes, complétées par quelques nouveaux éléments.

La sélection des risques de ce catalogue a précédemment fait l'objet d'une analyse comparative approfondie des différentes évaluations de risques similaires au niveau international. En outre, les doublons ou les lacunes entre ces risques ont été soigneusement évités.

Un catalogue complet des risques

Le catalogue des risques constitue l'épine dorsale de la BNRA. Ce catalogue contient une compilation de risques pertinents pouvant affecter la Belgique de manière significative ou avoir un impact majeur, au cours de la période 2023-2026.

Le catalogue final des risques pour la BNRA couvre 118 risques répartis en 7 catégories, chacun ayant fait l'objet d'une analyse de risque approfondie.



Par souci de concision et de pertinence, cet aperçu n'inclut qu'une sélection raisonnée du catalogue des risques (voir page 11, la section Présentation des fiches de risque).

Probabilité vs. Impact

Un risque est défini en fonction de sa probabilité et de son impact. La probabilité représente la chance qu'un événement se produise. Les conséquences, ou les effets d'un événement sur la société, constituent l'impact du risque.

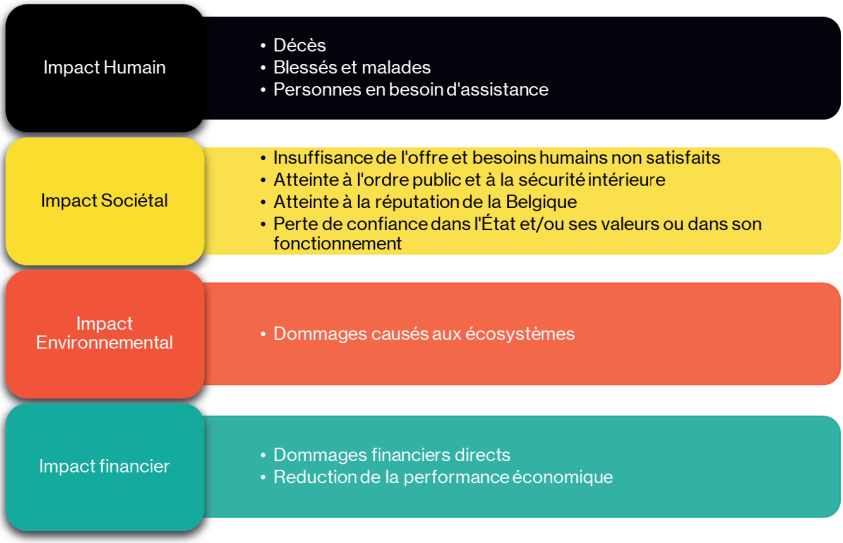
Les risques sont ensuite classés en fonction du produit de ces deux facteurs:

Risque=probabilité ×impact

Une analyse détaillée de l'impact potentiel

L'impact réel d'un incident peut se manifester dans de multiples domaines, par exemple le nombre de décès humains, la dégradation de l'environnement ou les pertes financières. C'est ce qu'on appelle les indicateurs d'impacts.

La BNRA distingue dix indicateurs d'impact distincts répartis en quatre catégories d'impact : impact humain, impact sociétal, impact environnemental et impact financier. Chaque indicateur d'impact est exprimé selon une unité spécifique (par exemple le nombre de vies humaines perdues vs. km² vs. €).

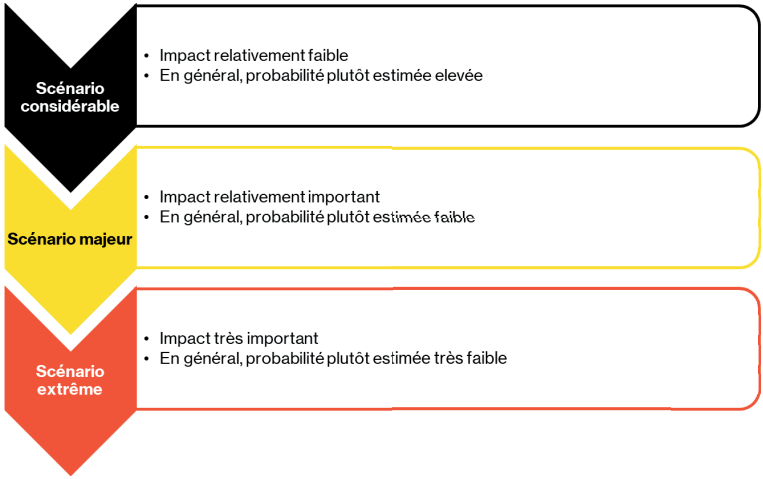


Dans ce rapport, vous trouverez toujours le score d'impact total par catégorie pour chaque risque. Ce score est la somme de tous les indicateurs d'impact au sein d'une catégorie.

Une approche multi-scénarios

Pour la plupart des risques figurant dans le catalogue des risques, il est possible d'imaginer un large éventail d'incidents (ou, dans certains cas, d'incidents qui ont même déjà eu lieu).
Ce faisant, l'impact peut varier considérablement d'un scénario à l'autre. Comparons par exemple une panne d'électricité qui touche une seule rue pour quelques heures seulement à une panne d'électricité d'échelle nationale durant plusieurs jours.

Lequel de ces scénarios est le plus pertinent pour la Belgique ou le plus intéressant pour envisager des mesures de prévention et de préparation ? Dans l'exemple de la panne d'électricité, cela semble immédiatement évident, mais ce n'est, en général, pas le cas. C'est la raison pour laquelle la BNRA propose pour chaque risque trois scénarios avec des niveaux d'intensité croissants. Pour chacun de ces scénarios, une analyse de risque est ensuite effectuée afin de déterminer le scénario le plus pertinent.



Un focus sur les effets cascade

La BNRA n'examine pas chaque risque de manière isolée, mais met l'accent sur les relations de cause à effet entre les risques et leurs impacts intersectoriels. Par exemple, une perturbation des communications numériques n'affecte pas seulement le secteur des télécommunications mais peut également affecter toute une série d'autres secteurs, tels que les transports et le secteur médical.

Au cours des analyses, différents experts ont identifié, décrit et quantifié ces relations. Il en est résulté un réseau de risques interconnectés. Ces liens ont ensuite été intégrés dans un modèle mathématique et automatiquement inclus dans les résultats finaux de l'évaluation des risques.

Le présent document ne développe pas ces cascades (bien qu'elles soient parfois mentionnées). Toutefois, ces connexions font partie intégrante des résultats présentés.

Une collaboration étendue avec des experts du secteur

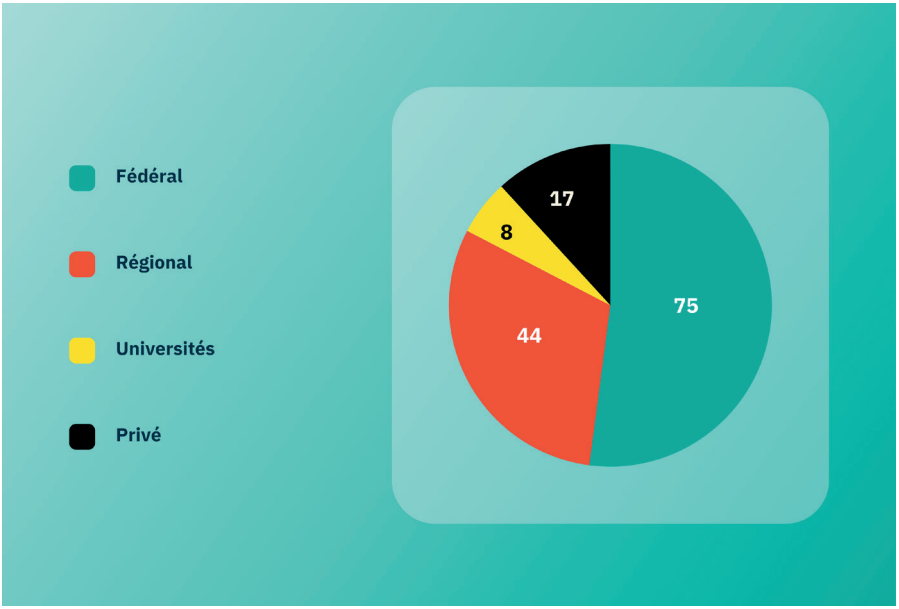
Le développement de la culture du risque dans notre société nécessite avant tout une compréhension précise de chaque risque. Pour ce faire, le NCCN a sélectionné pour chaque risque un certain nombre d'experts à qui il a été demandé, sur une base volontaire, de valider, d'évaluer et de consolider un ou plusieurs risques.

Ces experts sont principalement issus du secteur public. En outre, des universitaires et des opérateurs privés ont également participé activement à l'échelle nationale.

La méthodologie utilisée fait appel à un maximum de contributions de la part des différents groupes d'experts. Plus il y a de réponses, plus la compréhension des risques est nuancée et précise.

Tous les experts ont effectué les analyses de risques en fonction de leur propre niveau de connaissance. La précision des analyses doit donc être abordée avec nuance. Ces analyses sont un instantané dans le temps. Il est possible qu'elles aient été plus ou moins influencées par des événements survenus pendant l'évaluation (mars 2023 - mars 2024). Les résultats n'excluent pas non plus que des événements extrêmes imprévus se produisent au cours de la période à venir (également connus sous le nom de *black swans*, "cygnes noirs").

Au total, plus de 160 experts issus d'environ 140 organisations différentes ont été impliqués dans la BNRA, fournissant des contributions pour un ou plusieurs risques.



Regard sur le changement climatique et d'autres risques émergents

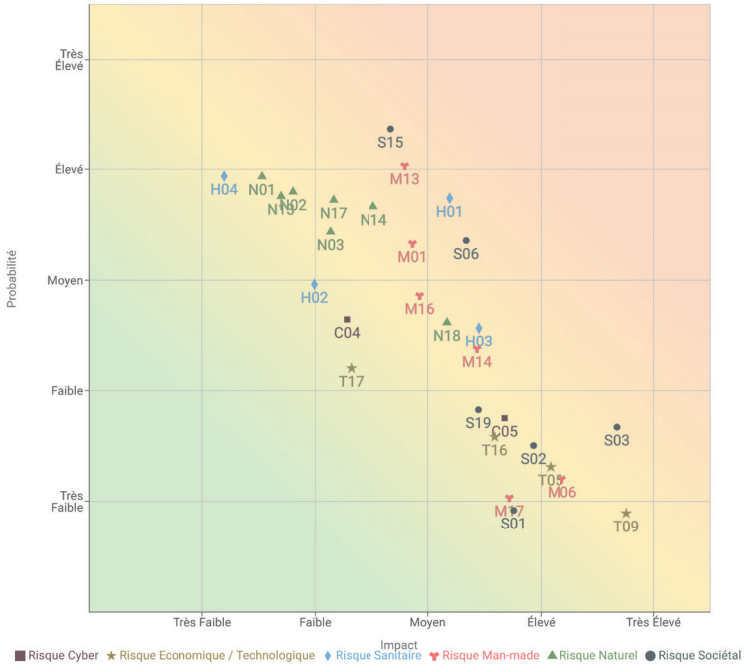
Bien que les estimations des groupes d'experts aient été réalisées pour une période de trois ans dans le futur, la méthodologie tient toutefois également compte du fait que certains risques ne peuvent pas être exprimés de manière adéquate dans ce délai limité. C'est pourquoi une attention particulière a été accordée aux risques liés au changement climatique et aux nouveaux risques émergents.

Afin d'évaluer l'impact du changement climatique, la BNRA inclut également une estimation de l'évolution de chaque risque jusqu'en 2050.

Les experts ont ainsi évalué si la probabilité de chacun de ces risques pourrait augmenter sous l'effet du changement climatique et, le cas échéant, dans quelle mesure.

En outre, la BNRA a également examiné onze autres risques émergents. L'évaluation de ces risques a été réalisée sur une base purement qualitative. Vous trouverez plus d'informations à ce sujet dans le chapitre consacré aux "Risques Catalyseurs" (p. 52).

Matrice des risques



Risques “man-made”

- M01 - Acteur hybride
- M06 - Attaque contre une infrastructure CBRNe
- M13 - Opérations d’information
- M14 - Espionnage
- M16 - Ingérence
- M17 - Conflit International Armé (CAI)

Risques Cyber

- Cyberattaque contre une institution gouvernementale
- Cyberattaque contre une infrastructure vitale

Risques sociétaux

- S01 - Défaillance de l’approvisionnement en électricité
- S02 - Défaillance de l’approvisionnement en gaz naturel
- S03 - Défaillance de l’approvisionnement en pétrole
- S06 - Défaillance du transport aérien
- S15 - Défaillance des infrastructures digitales
- S19 - Défaillance des services spatiaux

Risques économiques et technologiques

- T05 - Incident dans une centrale nucléaire (combiné avec “Libération d’agents radioactifs”)
- T09 - Libération d’agents radioactifs (combiné avec “Incident dans une centrale nucléaire”)
- T16 - Défaillance de digue
- T17 - Défaillance de barrage

Risques sanitaires

- H01 - Maladies infectieuses
- H02 - Maladies animales non zoonotiques
- H03 - Maladies des plantes agricoles & pestes
- H04 - Contaminants dans la nourriture humaine et animale

Risques naturels

- N01 - Inondation par les eaux de ruissellement (voir la fiche “Inondations”)
- N02 - Inondation fluviale (ou de rivière) (voir la fiche “Inondations”)
- N03 - Inondation côtière (voir la fiche “Inondations”)
- N13 - Sécheresse
- N14 - Vague de chaleur / Canicule
- N17 - Feux de forêt
- N18 - Espèces invasives

Présentation des fiches de risque

Comme indiqué précédemment, ce rapport ne contient des informations que sur un échantillon du catalogue des risques. Cette sélection se compose des risques les plus importants par catégorie (valeurs de probabilité et/ou d'impact élevées), complétés par certains risques qui ont été récemment portés à l'attention du public.

Les risques présentés dans ce rapport sont répertoriés dans un ordre aléatoire. Chaque fiche de risque se compose de deux parties : une description et une analyse.

Description

Dans la première partie de chaque fiche, le risque est défini aussi précisément que possible sous une forme simplifiée. Pour une meilleure lisibilité, les références des définitions ne sont pas incluses.

En outre, le présent rapport décrit également le scénario le plus pertinent. Il s'agit du scénario pour lequel le score combiné *probabilité x impact* est le plus élevé.

Analyse

La section d'analyse de chaque fiche se concentre sur la probabilité, l'impact et les éventuels effets en cascade.

À titre d'exemple, l'image de droite représente une simplification graphique des principales informations obtenues à partir de l'évaluation des risques pour le scénario le plus pertinent, à savoir : 1° la probabilité que le scénario se produise (qui varie de très faible à très élevé) et 2° une approximation visuelle des impacts déterminés sur base des contributions des experts (de très faible à très élevé).

Une partie de l'analyse peut également être consacrée à la description des "effets cascade" de chaque risque. Il s'agit à la fois des causes et des conséquences potentielles d'un risque.



Risques “man-made”

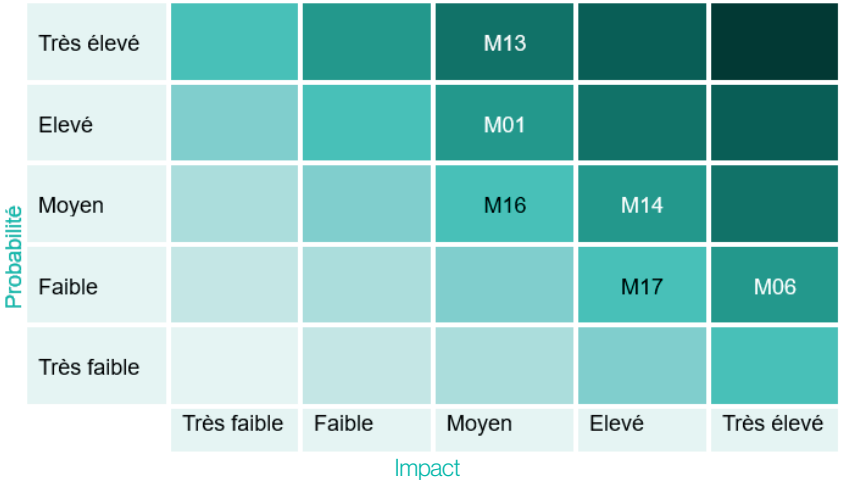
Les risques d'origine humaine ne surviennent pas automatiquement, mais sont toujours le fruit d'une intention malveillante. Cette section a donc été structurée en deux parties, à savoir une analyse des différents acteurs et une analyse des différents *modi operandi* qu'ils peuvent utiliser.

Ce chapitre traite des acteurs hybrides. Toutefois, les risques d'origine humaine peuvent également être réalisés par des groupes terroristes, des acteurs d'extrême droite ou d'extrême gauche, ou encore des organisations criminelles. Chacun de ces acteurs possède des *modi operandi* de prédilection, qui lui sont propres. Il peut s'agir de trafic de drogue, d'espionnage ou d'ingérence, d'investissements directs étrangers ou d'attaques physiques.

Dans ce rapport, une attaque à l'encontre d'une infrastructure CBRNe est évoquée en raison de l'impact à grande échelle que ce risque pourrait avoir s'il venait à se produire.

La BNRA a toutefois également étudié d'autres types de scénarios d'attaque, tels que des attaques contre des cibles vulnérables, des personnalités VIP, des infrastructures vitales ou certains groupes spécifiques de personnes ou des communautés.

Cependant, le présent rapport n'aborde pas l'ensemble des risques d'origine humaine. Une sélection des risques les plus significatifs a été réalisée, ainsi qu'une sélection de certains risques particulièrement actuels. Les risques évoqués dans cette brochure sont ainsi étroitement liés à la situation géopolitique actuelle. Il est donc important de considérer les résultats à la lumière des réalités d'aujourd'hui.



M01 - Acteur hybride
M06 - Attaque contre une infrastructure CBRNe
M13 - Opérations d'information
M14 - Espionnage
M16 - Ingérence
M17 - Conflit International Armé (CAI)

M01 - Acteur hybride

Description

Le Centre d'Excellence Européen pour la lutte contre les Menaces Hybrides (*Hybrid CoE*) définit les menaces hybrides comme suit :

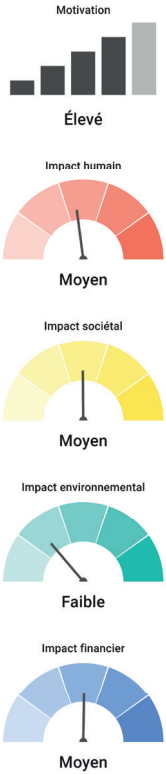
Le terme menace hybride fait référence à une action menée par un acteur étatique ou non-étatique dont l'objectif est de compromettre ou de nuire à une cible en influençant sa prise de décision au niveau local, régional, étatique ou institutionnel. Ces actions sont coordonnées et synchronisées, et ciblent directement les vulnérabilités des Etats et des institutions démocratiques. Des activités peuvent être déployées, par exemple, dans les domaines politique, économique, militaire, civil ou de l'information. Elles sont menées en utilisant et en combinant un large éventail de techniques et sont conçues pour rester en deçà du seuil de détection et d'attribution ».

L'acteur hybride le plus pertinent est un régime autoritaire opposé aux valeurs démocratiques européennes. Les intentions malveillantes sont claires, les capacités d'attaque élevées et la stratégie cohérente pour s'engager dans des conflits hybrides.

Analyse

Dans le contexte géopolitique actuel, il n'est pas surprenant que les acteurs hybrides susmentionnés soient très motivés pour mener des attaques contre l'Occident. Un acteur doté de capacités considérables peut utiliser divers outils et techniques pour atteindre son objectif.

Des opérations d'Information coordonnées menées en continu, visant à polariser la population, combinées à des cyberattaques sur des infrastructures gouvernementales, CBRNe et vitales, sapent la confiance de la société dans son gouvernement. L'espionnage, l'ingérence et les investissements directs étrangers sont également utilisés pour atteindre leurs propres objectifs stratégiques ou déstabiliser l'Occident.



M06 - Attaque contre une infrastructure CBRNe

Description

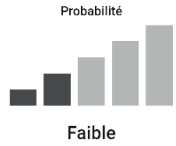
Le scénario le plus pertinent pour une "attaque contre une infrastructure CBRNe" est une tentative physique délibérée de détruire l'infrastructure avec toutes sortes d'armes pour faire des victimes civiles[1]. CBRNe est l'abréviation internationale faisant référence aux substances chimiques, biologiques, radiologiques, nucléaires et explosives. Les infrastructures CBRNe sont des installations qui font usage ou stockent des matières CBRNe, telles que les installations Seveso et les installations nucléaires.

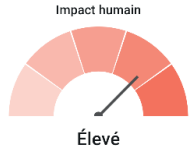
Analyse

Une attaque contre une infrastructure CBRNe sera principalement menée par des acteurs étatiques hybrides qui chercheront ainsi à déstabiliser notre pays. Lorsqu'une telle attaque est menée par un acteur étatique, ceci peut conduire à un conflit international.

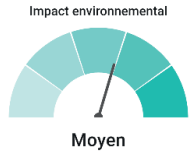
Si la probabilité d'une telle attaque est faible, il n'en va certainement pas de même de ses conséquences. La destruction d'une installation, par exemple, peut libérer des agents radiologiques ou d'autres substances qui peuvent avoir un impact humain majeur, entraînant de nombreux décès et malades. Une telle attaque peut également avoir un impact financier majeur, dans la mesure où les installations devront être reconstruites et l'environnement immédiat assaini. En outre, les services ne pourront pas être fournis par les installations touchées.

Enfin, une telle attaque suscitera également la peur dans la société et aura un impact sur l'environnement. Ce type d'événement n'affecte pas seulement la Belgique. Lorsqu'un tel site est proche de la frontière, les pays voisins peuvent également être touchés.











[1] Ce scénario est donc strictement limité aux installations fixes et physiques. Les incidents couvrant le transport de matières dangereuses CBRNe font l'objet d'une fiche spécifique "Attaque sur un transport de biens dangereux" (M12).

M13 - Opérations d'information

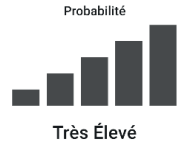
Description

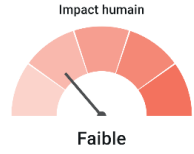
Les opérations d'information sont des actions visant à influencer l'information et/ou les systèmes d'information afin de parvenir à modifier 1) la capacité d'action, 2) la compréhension de la situation et 3) la capacité de réaction de l'adversaire (potentiel). Une modification de l'un de ces trois facteurs suffit à perturber les capacités de l'adversaire. Les campagnes de désinformation sont un exemple connu de ce type d'action visant notamment à créer une polarisation dans la société.

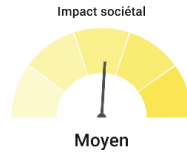
Le scénario le plus pertinent en matière d'opérations d'information correspond à une campagne de désinformation parrainée de l'extérieur via les médias sociaux, qui dure plus de trois mois et cible spécifiquement la Belgique. La campagne suscite un engagement important : plus de 100 000 likes, partages, tweets et/ou retweets, avec une portée réelle de plus de 10 000 personnes. Les faux messages sont diffusés par plus de cinq canaux (médias sociaux, alternatifs et grand public) et sont liés à un incident international.

Analyse

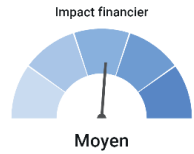
L'impact social des opérations d'information ne peut être sous-estimé. La manipulation étrangère de l'information et l'ingérence (FIMI) visent à modifier le comportement de la population et à créer une polarisation. Selon le contexte, elle peut avoir des conséquences immédiates et créer la panique. Elle peut aussi conduire à ce qu'une plus grande partie de la population s'abstienne de tout esprit critique. Si la Belgique devient la cible d'opérations d'information, cela pourrait réduire la confiance des citoyens dans le gouvernement et nuire gravement à la réputation de notre pays, tant au niveau national qu'à l'étranger. Les opérations d'information peuvent également avoir un impact financier direct, en fonction de leur nature. L'objectif des opérations d'information est de semer des divisions sociales et d'influencer le comportement cognitif individuel, ce qui conduit à des choix différents qui, à leur tour, peuvent influencer l'impact financier.











M14 - Espionnage

AVERTISSEMENT

L'espionnage et l'ingérence sont souvent considérés à tort comme allant de pair. Cependant, il convient de ne pas les confondre. L'espionnage est un moyen non autorisé d'obtenir des informations. L'ingérence, quant à elle, implique la diffusion d'informations erronées pour influencer la prise de décision.

Description

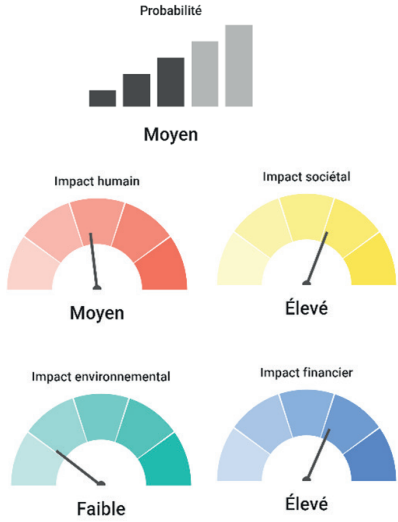
L'Espionnage est défini par la loi sur les services de renseignement et de sécurité comme : « le recueil ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter ». Des acteurs malveillants (étatiques ou non) peuvent utiliser divers moyens (espions, cyberattaques, dispositifs mécaniques, etc.) pour rechercher ou obtenir des informations qui, autrement, seraient dissimulées ou protégées. Les principales motivations sont, le plus souvent, l'acquisition d'un savoir-faire commercial, technologique ou militaire afin d'obtenir un avantage sur des concurrents.

Dans le scénario le plus pertinent de l'espionnage, des informations sensibles susceptibles de nuire aux intérêts militaires, diplomatiques ou économiques de la Belgique sont acquises. L'acteur responsable dispose de moyens technologiques, financiers et humains considérables afin que les opérations d'espionnage puissent être menées sans être détectées.

Analyse

La probabilité d'un tel espionnage au cours des trois prochaines années est réelle. Il est souvent causé par des interférences ou par des acteurs hybrides. L'espionnage peut causer des dommages directs et indirects. Il peut y avoir un impact direct à long terme sur l'économie belge.

En outre, l'impact social de l'espionnage peut être significatif, s'il nuit à la réputation de la Belgique et affecte notre influence au sein de forums multilatéraux tels que l'UE ou l'OTAN. En outre, ceci peut alimenter les théories du complot, polariser la société et éroder la confiance dans la démocratie. Si la cible de l'opération d'espionnage a des liens internationaux, l'impact peut aller au-delà des frontières.



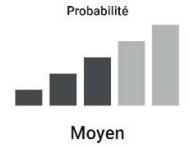
M16 - Ingérence

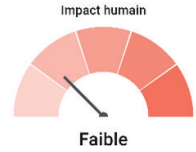
Description

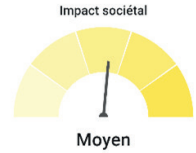
L'ingérence nationale ou étrangère comprend l'intimidation, la diffusion d'informations trompeuses et les activités clandestines.
Ces actes sont réalisés par ou au nom d'un acteur et vont au-delà de l'influence diplomatique normale pour orienter les processus de prise de décision. L'influence, pour sa part, est une tentative ouverte et transparente des gouvernements étrangers d'influencer à leur avantage le débat sur des questions importantes au sein de l'opinion publique nationale. Le scénario d'ingérence le plus pertinent se concentre sur l'influence d'individus au sommet du processus décisionnel. Cette influence porte sur des questions liées à nos intérêts nationaux et peut avoir des effets négatifs permanents ou à long terme.

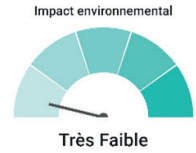
Analyse

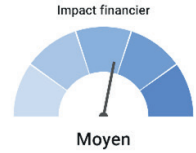
L'ingérence en Belgique peut être le fait d'une multitude d'acteurs, y compris des acteurs étatiques par le biais d'une guerre hybride ou d'investissements directs étrangers[1]. L'ingérence peut résulter de pratiques d'espionnage, par l'utilisation d'informations volées pour influencer les individus, ou même rendre possible l'espionnage. Certaines personnes ayant été influencées peuvent être plus ouvertes à des pratiques d'espionnage. Ceci peut entrainer des perturbations dans le fonctionnement du gouvernement. Une ingérence d'une telle ampleur peut porter atteinte à la réputation de la Belgique et entraîner une perte de confiance dans le fonctionnement du gouvernement. L'ingérence dans les intérêts stratégiques et les politiques de la Belgique peut également avoir un impact financier (indirect). La Belgique se situe au coeur de la communauté internationale avec les institutions de l'UE et de l'OTAN sur son territoire. L'ingérence pourrait donc dépasser les intérêts belges et viser des décideurs ou des dossiers internationaux. Ceci affecterait non seulement la Belgique, mais aussi la communauté internationale au sens large.











[1] La BNRA a étudié les Investissements Directs Etrangers (IDE) comme un risqué spécifique (M15) mais ne l'a pas identifié parmi les risques les plus élevés, il n'est donc pas inclus dans ce rapport.

M17 - Conflit Armé International (CAI)

Description

Un conflit armé international (CAI) est défini par le Comité International de la Croix Rouge comme une situation dans laquelle des États ont recours à la force armée, même si l'état de guerre n'est reconnu par aucun d'entre eux.

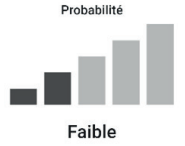
Le scénario le plus pertinent d'un CAI se déroule sur le territoire de l'OTAN, mais pas à l'intérieur des frontières de la Belgique. Néanmoins, il nécessitera vraisemblablement encore toujours un déploiement important de personnel et d'équipements militaires belges dans la zone où se déroule le conflit.

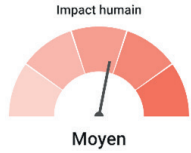
Analyse

Les experts estiment que la probabilité de ce scénario est plutôt faible, mais qu'elle n'est pas inexistante à mesure que les tensions géopolitiques et économiques augmentent. L'appartenance de la Belgique à l'OTAN implique également que la Belgique pourrait être impliquée dans un conflit sans être directement attaquée.

Des acteurs étatiques malveillants utilisent actuellement diverses formes d'attaques hybrides contre la Belgique et ses alliés. Ces attaques peuvent être le catalyseur d'un CAI entre l'OTAN et ses adversaires, surtout si elles augmentent en intensité ou si l'acteur ne reste plus en dessous du seuil de détection.

Un tel conflit armé aurait un impact important sur différentes catégories d'impact. Le personnel militaire déployé est en danger mais l'approvisionnement en nourriture, en matières premières et en vecteurs énergétiques (gaz naturel et pétrole) pourrait également être compromis. Sur le plan économique, la dette publique augmentera et des chocs financiers sont possibles. Un afflux de personnes provenant de zones de guerre et ayant besoin d'une protection internationale est également très probable. Enfin, les attentats peuvent se multiplier, notamment contre les infrastructures vitales ou les installations CBRNe.











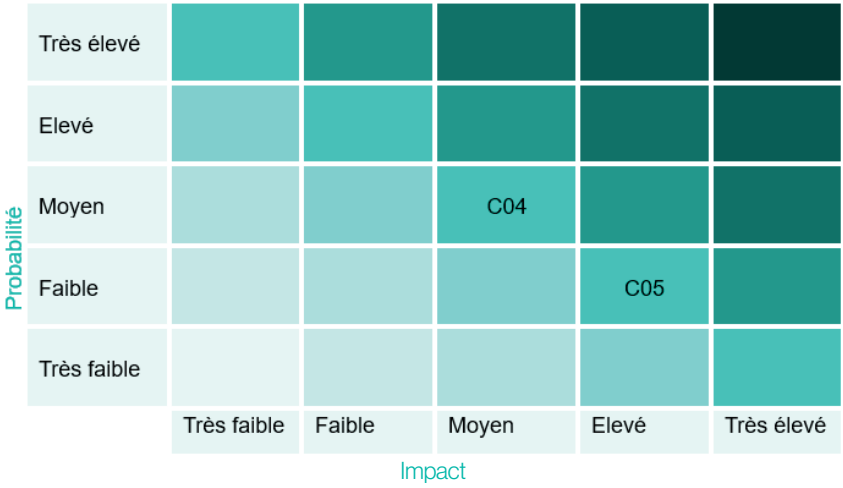
Risques Cyber

Dans le monde interconnecté d'aujourd'hui, les cyberrisques sont devenus omniprésents et de plus en plus sophistiqués. Qu'il s'agisse de violations de données, d'attaques par ransomware ou d'espionnage parrainé par un État, les dangers du cyberespace sont multiples et d'une grande portée.

Les cyberrisques repris dans cette analyse sont toujours des attaques avec des intentions malveillantes. Ces attaques peuvent compromettre la disponibilité, l'intégrité et la confidentialité des informations stockées ou traitées dans les systèmes ou transitant sur les réseaux. Une telle attaque peut avoir lieu en exploitant les vulnérabilités des logiciels et du matériel, les mauvaises configurations de logiciels et de matériel, ou en utilisant des tactiques d'hameçonnage ou d'ingénierie sociale.

Les violations de données peuvent entraîner des pertes financières, des atteintes à la réputation et des responsabilités juridiques. Les attaques par ransomware peuvent paralyser des entreprises et des infrastructures critiques et provoquer des perturbations généralisées.

Les technologies émergentes posent également toujours de nouveaux défis : les cyberrisques évoluent avec les technologies.



C04 - Cyberattaque contre une institution gouvernementale
C05 - Cyberattaque contre une infrastructure vitale

C04 - Cyberattaque contre une institution gouvernementale

Description

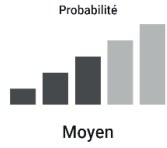
Une cyberattaque menée par un acteur malveillant contre un organisme gouvernemental rend un gouvernement central ou une administration incapable de remplir ses fonctions. L'attaque entraîne une violation de la sécurité qui se traduit par la destruction, la perte, la modification, la divulgation non autorisée ou l'accès à des données protégées transmises, stockées ou traitées, de manière accidentelle ou illicite. Les agences gouvernementales liées à la défense, à la sécurité nationale, à la sécurité publique et à l'application de la loi, ainsi que les entités relevant du pouvoir judiciaire, le parlement ou les banques sont exclues et font l'objet d'autres fiches de risque.

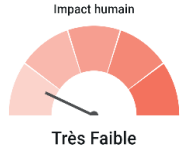
Dans le scénario le plus pertinent d'une cyberattaque contre une agence gouvernementale, entre 20 et 50 % des ordinateurs sont compromis par des logiciels malveillants, ce qui entraîne une indisponibilité des services informatiques de moins d'une journée. La période qui s'écoule entre l'intrusion dans le réseau et la détection et la suppression est inférieure à un mois. En conséquence, 20 à 50 % des organisations partenaires ou des citoyens sont touchés par le virus, ce qui entraîne un vol important de données classifiées.

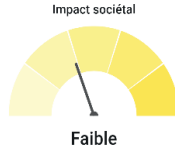
Analyse

En fonction de l'intensité, de la durée et des dommages de la cyberattaque, l'impact financier peut être important. Des cyberattaques peuvent également gravement perturber et affecter les services gouvernementaux et administratifs si elles aboutissent.

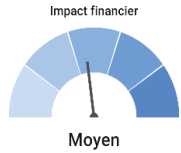
Comme ces attaques deviennent de plus en plus innovantes et complexes, les coûts de la protection des réseaux et des infrastructures peuvent être élevés. En fonction de la gravité de l'attaque et du contenu des informations sensibles divulguées, la réputation de la Belgique peut être entachée. Des données personnelles ou des organigrammes peuvent servir à identifier des personnes d'intérêt comme cibles. Ceci peut réduire la confiance des citoyens dans le gouvernement.











C05 - Cyberattaque contre une infrastructure vitale

Description

Les cyberattaques peuvent également viser les infrastructures vitales, numériques et physiques[1], et perturber les opérations et le fonctionnement de ces infrastructures. Le scénario le plus pertinent pour ce risque est une cyberattaque contre toute infrastructure vitale qui répond aux besoins physiques, de sécurité ou de confort de la société et où le temps d'indisponibilité de l'infrastructure informatique dépasse une semaine.

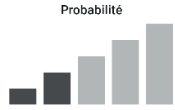
Analyse

La probabilité de ce scénario est faible, mais il pourrait être mené par des acteurs malveillants qui veulent déstabiliser le pays ou qui recherchent un gain financier.

Ce scénario peut avoir un impact financier important. Une cyberattaque réussie s'accompagne généralement d'une reconstruction coûteuse de l'infrastructure et de la sécurité du réseau. Si une cyberattaque entraîne une interruption de l'approvisionnement en gaz, par exemple, elle peut avoir des coûts directs et indirects, ainsi que des conséquences immédiates et à long terme.

Les cybermenaces peuvent également menacer la sécurité des personnes et des pays. Une cyberattaque vise à causer des dommages, à voler des données ou à perturber la vie numérique en général.

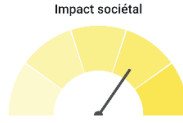
Dans le cas du cyberespionnage, l'impact social peut être important, comme la perte de confiance dans le gouvernement et l'atteinte à la réputation de la Belgique.



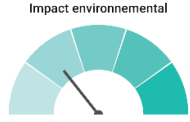
Faible



Moyen



Élevé



Faible



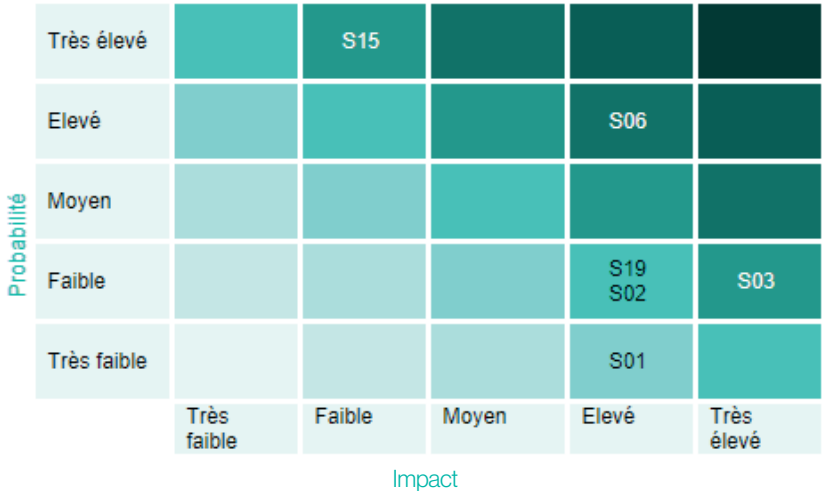
Élevé

[1] Secteurs couverts par la directive NIS2 : électricité, chauffage et climatisation, pétrole, gaz naturel, hydrogène, transport aérien, ferroviaire, fluvial et routier, services financiers, marchés financiers, santé publique, eau potable, eaux usées, infrastructure numérique, services numériques, services liés à l'espace, services postaux et de messagerie, gestion des déchets, production et distribution de produits chimiques, production et distribution de denrées alimentaires et industrie manufacturière.

Risques sociétaux

Le contexte géopolitique actuel crée un paysage de menaces dynamique dans lequel de multiples types de risques et une interdépendance accrue entre les infrastructures et les secteurs créent un fort besoin de services vitaux plus résilients. Après tout, ces services jouent un rôle indispensable dans le maintien des fonctions sociétales vitales et de l'activité économique. Ils sont fondamentaux pour la survie de notre société. L'accès à l'eau potable, à la nourriture, aux services de soins de santé, aux services gouvernementaux et à d'autres institutions, contribuent aux besoins de sécurité physique et de confort de tout un chacun. Une perturbation de ces services vitaux aura donc un impact immédiat et tangible sur la résilience de la société belge.

Aujourd'hui, l'Union européenne a déjà élaboré les directives CER et NIS2 dans lesquelles de multiples secteurs vitaux ont été identifiés.
Ce chapitre décrit et analyse la probabilité et l'impact potentiel d'une "défaillance" de certains de ces services catalogués, qui sont essentiels à la sécurité et aux besoins de la population.
De manière générale, ces risques peuvent avoir un impact sociétal et financier important.



S01 - Défaillance de l'approvisionnement en électricité
S02 - Défaillance de l'approvisionnement en gaz naturel
S03 - Défaillance de l'approvisionnement en pétrole
S06 - Défaillance du transport aérien
S15 - Défaillance des infrastructures digitales
S19 - Défaillance des services spatiaux

S01 - Défaillance de l'approvisionnement en électricité

Description

Une perturbation de l'approvisionnement en électricité peut prendre plusieurs formes. Une panne de courant fait généralement référence à une perte partielle ou totale de l'alimentation électrique d'un utilisateur final (par exemple, la population, les entreprises, les systèmes critiques). Une crise d'électricité désigne une situation actuelle ou imminente de pénurie importante du côté de l'offre. Les perturbations peuvent prendre la forme de *brown-outs* (chute de tension) ou de *black-outs* (perte de tension ou panne).

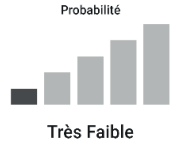
Le scénario le plus pertinent pour une perturbation de l'approvisionnement en électricité est une panne nationale d'une durée d'au moins un jour. Un redémarrage complet (*black start*) est nécessaire et plusieurs sites critiques du réseau électrique sont endommagés. L'importation depuis les pays voisins est limitée, voire indisponible.

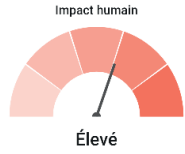
Analyse

Les analyses montrent que ce risque est très faible. Ceci s'explique surtout par la maturité du secteur, les nombreuses mesures et obligations légales déjà en place, ainsi qu'à la préparation générale aux crises pour de telles perturbations. Ce risque est néanmoins abordé dans le présent rapport en raison de l'importance sociétale de l'approvisionnement en électricité.

Une perturbation pourrait résulter d'attaques physiques ou informatiques sur certaines parties critiques de l'infrastructure énergétique.

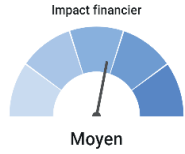
Malgré sa faible probabilité, ce scénario a un impact important. De toute évidence, l'impact sociétal est de loin la catégorie la plus importante pour ce risque. La quasi-totalité de la population et des entreprises belges serait alors privée d'électricité pendant toute la durée de la panne. Les secteurs pour lesquels l'impact attendu est le plus important sont le secteur alimentaire, le secteur des transports et le secteur de la santé.











S02 - Défaillance de l'approvisionnement en gaz naturel

Description

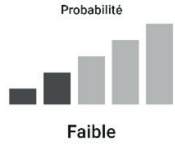
En cas de rupture d'approvisionnement en gaz naturel au niveau national, le volume de gaz naturel injecté dans le réseau belge (via l'importation, le déstockage et la production locale) est inférieur au volume de gaz naturel retiré du réseau belge (via la consommation ou le transport vers les pays voisins). En cas de perturbation réelle de l'approvisionnement en gaz naturel, le déséquilibre ne peut pas être résolu par les actions régulières des acteurs du marché. Au lieu de cela, les mesures du plan d'urgence fédéral pour l'approvisionnement en gaz naturel (alarme ou urgence) doivent être mises en oeuvre.

Le scénario le plus pertinent vise une perturbation à l'échelle nationale. Pour faire face au déficit gazier, des mesures d'urgence importantes doivent être prises, telles que définies par le plan d'urgence fédéral pour l'approvisionnement en gaz du SPF Économie. Cela aurait évidemment un impact transfrontalier, car les pays voisins de l'UE devront faire preuve de solidarité dans une telle situation.

Analyse

Les cyberattaques et les conflits armés internationaux sont les causes les plus probables d'une perturbation. Ils peuvent être liés entre eux et même se produire en même temps. L'impact sociétal d'une telle perturbation dépend de la durée et de la gravité de la cyberattaque ainsi que du lieu où se déroule le conflit armé. L'impact devrait être sévère car les besoins humains ne peuvent plus être satisfaits en raison du manque de chauffage.

Certains secteurs industriels devraient fermer, ce qui pourrait entraîner du chômage et des pertes financières. Si l'interruption de l'approvisionnement en gaz naturel se poursuit, elle pourrait entraîner une réduction importante des performances économiques et une perte de confiance des citoyens et des employeurs envers le gouvernement.











S03 - Défaillance de l'approvisionnement en pétrole

Description

Une rupture de l'approvisionnement en pétrole se produit lorsque la demande de pétrole ou de produits pétroliers dépasse leur disponibilité. La cause peut être une disponibilité limitée ou une consommation inhabituelle. Cependant, la plupart des perturbations résultent de situations dans lesquelles l'approvisionnement en pétrole ou en produits pétroliers est interrompu, ce qui a un impact sur la distribution aux utilisateurs finaux. Ces perturbations peuvent être la conséquence de problèmes au niveau international (instabilités géopolitiques et/ou conflits) ou local.

Le scénario le plus pertinent en matière de perturbation des approvisionnements en pétrole touche l'ensemble du pays et les pays voisins. Le gouvernement prend des mesures pour réduire la demande à long terme, en libérant les stocks nationaux de sécurité et en mettant en oeuvre des mesures de solidarité (UE, AIE).

Analyse

Les causes de défaillance de l'approvisionnement en pétrole sont très diverses, mais un conflit armé international dans une région productrice de pétrole en constitue la plus probable. L'impact financier ne doit pas être sous-estimé. Une pénurie de pétrole affectera gravement le secteur pétrochimique ainsi que le transport des marchandises et des personnes. Ceci pourrait conduire à une réduction significative de l'activité économique. Le gouvernement doit alors prendre des mesures pour réduire la demande de pétrole et limiter l'approvisionnement aux consommateurs prioritaires. Ceci signifie que certains consommateurs non prioritaires peuvent potentiellement être complètement déconnectés ou limités à un programme d'achat maximum pendant un certain temps. Un impact social négatif serait dès lors à prévoir.



S06 - Défaillance du transport aérien

Description

Le transport aérien désigne tout mouvement de marchandises et/ou de passagers à bord d'un avion (OCDE). Il y a défaillance lorsque le transport aérien est interrompu, entraînant des difficultés pour transporter des passagers ou des marchandises selon le calendrier préalablement défini.

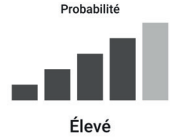
Le scénario le plus pertinent concernant une défaillance du transport aérien implique la destruction ou l'indisponibilité d'une infrastructure aéroportuaire critique. Cette destruction affecte la fourniture de services de tous les aéroports belges régionaux et internationaux pendant plus de dix jours et a un impact sur la fourniture de services des aéroports situés au-delà et à proximité de nos frontières nationales. Il en résulte l'indisponibilité des réacheminements à proximité.

Analyse

L'analyse montre que la perturbation de l'infrastructure numérique constitue la principale cause des perturbations dans l'aviation. En effet, la communication entre les tours de contrôle aérien et les avions au sol ou dans les airs est cruciale.

L'impact sociétal d'une défaillance du transport aérien ne doit pas être sous-estimé. Le scénario considère que les marchandises ne peuvent plus être acheminées par avion, ce qui peut engendrer des pénuries d'approvisionnement et des défaillances de services essentiels pour la population.

De plus, une défaillance du transport aérien de cette ampleur pourrait avoir un impact financier significatif sur les compagnies aériennes. Les pistes de décollage et d'atterrissage ou les avions pourraient devenir inutilisables et pourraient devoir être remplacés. Ce risque implique également que les performances économiques de la Belgique se détérioreraient sensiblement.











S15 - Défaillance des infrastructures digitales

Description

L'infrastructure digitale est un terme générique englobant toutes les technologies et opérations de télécommunication et d'information. Les plus connus sont les réseaux de téléphonie mobile (4G, 5G, ...) et Internet. Une défaillance entraîne des difficultés ou l'impossibilité de transmettre des messages ou des données. Le scénario le plus pertinent de défaillance de l'infrastructure numérique implique une interruption des services de télécommunication d'un seul fournisseur, à une échelle nationale et pendant moins d'une heure.

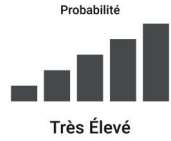
Analyse

Ce scénario est considéré comme très probable car plusieurs événements historiques d'ampleur similaire se sont déjà produits dans le passé.

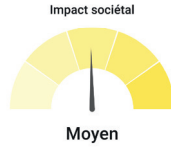
L'impact d'une telle défaillance est principalement de nature sociétale et financière. De nombreuses personnes ne pourront pas utiliser leurs services en ligne ou leurs moyens de communication habituels pendant la période de perturbation, voire plus longtemps.

En raison de la connectivité et de la numérisation croissantes, de nombreux fournisseurs de services dépendent de l'infrastructure numérique. Cependant, des mesures de résilience et de redondance croissantes sont mises en oeuvre. Une défaillance de l'infrastructure numérique affecte principalement le secteur de l'aviation, car celui-ci dépend fortement des infrastructures et des fournisseurs de communications nationaux.

Le trafic aérien pourrait être suspendu le temps de la perturbation. Ceci entraînerait des problèmes de capacité et aurait un impact financier et social considérable (par exemple, les passagers et le fret n'atteindraient pas leur destination à temps, voire pas du tout).











S19 - Défaillance des services spatiaux

Description

Les services spatiaux désignent les services opérationnels qui utilisent des technologies spatiales mises en orbite autour de la Terre. Ces services comprennent :

1. Les informations de positionnement, de navigation et de synchronisation (PNT) reçues depuis les systèmes mondiaux de navigation par satellite (GNSS);

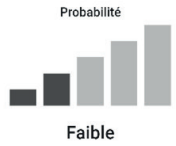
2. La fourniture d'images satellites pour l'organisation des services de secours, y compris des données pour les prévisions et alertes météorologiques;

3. Les services de communication tels que l'Internet à large bande et les services de transfert de données pour les utilisateurs civils, militaires et commerciaux.

Le scénario le plus pertinent pour ce risque est une panne qui affecte simultanément plusieurs types de services, dure plus de sept jours et provoque des dommages irréversibles.

Analyse

Les technologies spatiales apportent un soutien crucial aux activités militaires, commerciales et civiles. Elles contribuent à la prévision météorologique, au bon fonctionnement des banques et des marchés boursiers, des réseaux électriques, de tous types de transports et des opérations d'urgence, sans oublier la dissuasion nucléaire et conventionnelle et la prévention des crises. Que la cause d'une défaillance soit naturelle (par exemple, tempête solaire), technique (par exemple, collisions de débris spatiaux ou cyberattaques) ou géopolitique (Investissement direct étranger ou conflit armé), l'impact peut être important. Si les services spatiaux sont interrompus pendant plusieurs jours, affectant par nature divers pays, les conséquences sociétales et financières seraient significatives, en raison de la perturbation de la fourniture des services cités et du coût élevé de la réparation ou du remplacement de l'infrastructure spatiale.









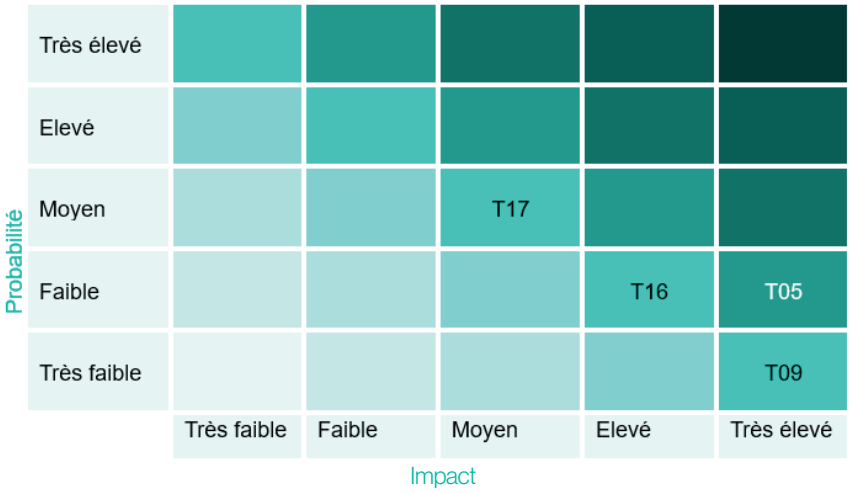


Risques économiques et technologiques

Les risques économiques et technologiques sont des risques liés à des accidents industriels et à des défaillances d'infrastructures (par exemple, ruptures de digue ou de barrage, faiblesses structurelles de ponts). Cette catégorie se concentre principalement sur des incidents industriels et nucléaires, les fuites de matières dangereuses (biologiques, chimiques, nucléaires ou radioactives) et les accidents des moyens de transport (aérien, ferroviaire ou routier).

L'ensemble de ces risques sont et restent des menaces permanentes et très importantes pour la société dans son ensemble. Toutefois, les probabilités et l'ampleur de leurs effets ont été réduites à des niveaux de risques plutôt faibles grâce aux multiples mesures de prévention et de protection déjà en place, telles que des politiques de sécurité plus strictes, des contrôles et réglementations industrielles et des systèmes de surveillance.

Par conséquent, ces risques sont à présent considérés comme acceptables. Néanmoins, il convient de rappeler que les mesures de protection et de prévention restent absolument essentielles pour garantir durablement la sécurité industrielle actuelle et future.



T05 - Incident dans une centrale nucléaire (combiné avec "Libération d'agents radioactifs")
T09 - Libération d'agents radioactifs (combiné avec "Incident dans une centrale nucléaire")
T16 - Défaillance de digue
T17 - Défaillance de barrage

T05 et T09 - Incident dans une centrale nucléaire avec libération d'agents radioactifs

Description

Une centrale nucléaire utilise de l'uranium et d'autres éléments fissiles comme combustible nucléaire pour produire de la vapeur à des fins de production d'électricité. Ce processus génère aussi des produits de fission résiduels, qui sont radioactifs. Si un accident devait survenir dans une centrale nucléaire, la chaleur et la pression pourraient s'accumuler et de la vapeur comportant des agents radioactifs pourrait s'échapper dans l'atmosphère.

Selon l'ampleur de l'accident et de l'exposition à la substance radioactive, un tel incident pourrait constituer un danger pour la santé humaine. Les matériaux radioactifs peuvent aussi être dangereux pour la santé des animaux, d'autres formes de vie et l'environnement.

Analyse

Un incident dans une centrale nucléaire est plutôt improbable, vu les multiples niveaux de protection et de sécurité pris à titre préventif. Néanmoins, en cas de libération d'agents radioactifs, l'impact humain pourrait être très élevé. Les conditions météorologiques peuvent propager les particules et affecter la population. Ainsi, les personnes qui reçoivent des doses de rayonnement élevées peuvent être confrontées à de graves risques pour leur santé, tels que des blessures et des maladies mortelles. Les personnes concernées devraient alors être évacuées ou hébergées dans une zone sûre.

Étant donné que les niveaux de rayonnement résiduels peuvent rester indéfiniment dans la zone affectée, celle-ci peut devenir inhabitable pendant des siècles. Ceci aura également un impact financier majeur, par exemple le coût de l'assainissement de la zone touchée.



T09 - Libération d'agents radioactifs

T16 - Défaillance d'une digue

Description

Une digue est une structure généralement constituée de terre ou de béton qui protège le terrain de l'eau. Une digue est souvent parallèle aux zones inondables d'une rivière ou le long de côtes basses. La défaillance de digue peut se définir comme tout effondrement ou mouvement d'une partie d'une digue ou de sa fondation au point qu'elle ne puisse plus retenir les eaux. Généralement, il en résulte une libération de grandes quantités d'eau qui peuvent devenir une menace pour les personnes et biens situés en aval. Pour tenir compte de la réalité belge, les écluses et les digues actives font également partie intégrante de cette fiche.

Le scénario le plus pertinent vise la rupture ou l'effondrement d'une haute et longue digue, affectant une large zone densément peuplée pendant quelques semaines.

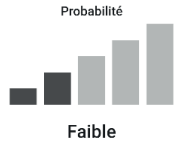
Analyse

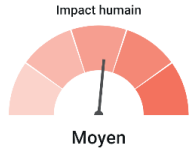
Les principales causes de défaillance de digue sont liées à divers phénomènes ou incidents qui conduisent à l'affaiblissement physique de la digue tels que l'érosion, l'affaissement, les glissement de terrain, les ruptures de barrages et les crues. Les inondations des zones touchées constituent indéniablement la principale conséquence de ce risque.

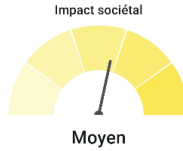
Une rupture de digue a un impact financier élevé, étant donné les énormes dégâts causés aux habitations, aux infrastructures et aux actifs environnants. Les performances économiques peuvent être réduites pendant une période significative en raison de l'inactivité des entreprises et des services concernés.

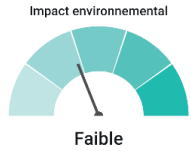
Les effets humains et sociétaux pourraient atteindre des niveaux considérables dans la mesure où une grande partie de la population locale perdrait son logement et serait confrontée à des pénuries de fournitures de base.

À l'avenir, le changement climatique pourrait entraîner davantage de ruptures de digues en raison de l'élévation du niveau de la mer et de débits fluviaux de plus en plus forts.











T17 - Défaillance d'un barrage

Description

En Belgique, il y a deux types de barrages:

- Les grands barrages de l'Est de la Belgique : leurs fonctions sont l'approvisionnement en électricité et le stockage de l'eau potable ;
- Les barrages fluviaux : ceux-ci sont construits sur les principales rivières et canaux navigables à topographie accidentée. Ils régulent les débits et niveaux des fleuves et assurent la circulation sur les voies navigables intérieures. Les déversoirs sont également inclus dans ce groupe.

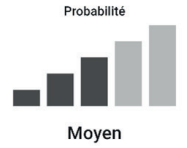
Une rupture de barrage se définit comme l'effondrement ou le mouvement d'une partie d'un barrage ou de ses fondations, de sorte qu'il ne peut plus retenir les eaux. Le principal résultat est le rejet de grandes masses d'eau, engendrant des risques pour les personnes, les biens et les infrastructures situés en aval. Les infrastructures hydrauliques, comme les digues, les déversoirs ou les barrages plus en aval, y sont particulièrement vulnérables.

Le scénario le plus pertinent est celui d'un barrage qui déborde, libérant en aval des débits d'eau plus importants que la normale dans les heures ou les jours suivants.

Analyse

L'effet direct attendu le plus important est un impact financier et social majeur. Les biens immobiliers situés dans les zones touchées peuvent subir de graves dommages. Une grande partie de la population touchée pourrait perdre son logement et souffrir de pénuries des services de base.

À l'avenir, le changement climatique pourrait entraîner des débordements de barrages plus nombreux en raison d'inondations de plus en plus fréquentes. Les systèmes de surveillance et les plans d'urgence ont toutefois été récemment améliorés pour garantir au maximum la prévention des risques.











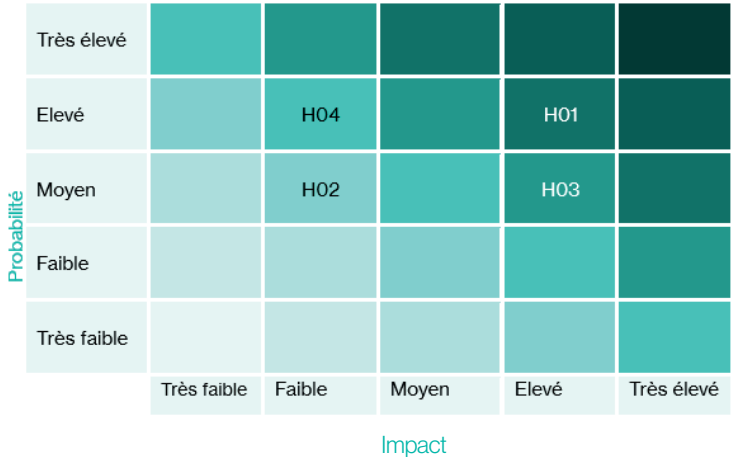
Risques sanitaires

Cette partie aborde les risques pouvant affecter la santé publique et la qualité de l'environnement. Ils trouvent principalement leurs origines dans les sévères perturbations ou changements que subissent les milieux de vie (notamment la pollution de l'air, de l'eau et des sols), la contamination des denrées alimentaires et l'émergence de dangereux fléaux affectant les êtres humains, les animaux et les plantes.

À l'instar de la pandémie de COVID-19, de telles crises se sont déjà produites au cours de ces dernières années, tant en Belgique qu'en Europe. Les risques sanitaires sont courants et touchent principalement les personnes et l'environnement, ce qui peut avoir un impact financier considérable.

En outre, l'impact social peut également être significatif, entraînant la défaillance de services essentiels à la population, notamment les soins de santé, et une grave perte de confiance de la population envers les autorités.

Cette section aborde également les risques psychologiques comme le rejet en masse de la médecine moderne ou les processus de nature socio-psychologique comme l'hystérie collective mais leur occurrence est en réalité quasiment nulle. S'ils venaient néanmoins à se produire, les effets potentiels resteraient à des niveaux assez faibles et induiraient principalement des impacts sur les plans humain et sociétal.



H01 - Maladies infectieuses
H02 - Maladies animales non zoonotiques
H03 - Maladies des plantes agricoles & pestes
H04 - Contaminants dans la nourriture humaine et animale

H01 - Maladies infectieuses

Description

Les maladies infectieuses sont des maladies provoquées par des agents pathogènes (comme par exemple, virus, bactérie, protozoaire, macroparasite, prion, viroïde et champignon) ou par leurs produits toxiques, et qui se transmettent à partir d'un individu, d'un animal ou d'un objet infecté à un hôte humain.

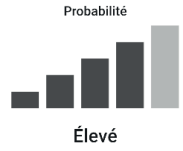
Le scenario le plus pertinent pour cette fiche de risque renvoie à une situation où une maladie se transmet par voie aérienne, avec un taux de mortalité moyen à élevé. Même si un traitement existe, la pression sur la capacité hospitalière reste forte.

Analyse

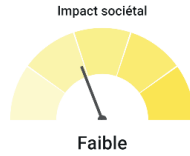
Les maladies infectieuses sont responsables d'une immense charge mondiale de morbidité qui a un impact sur les services de santé publique et les économies du monde entier, affectant de manière disproportionnée les populations vulnérables.

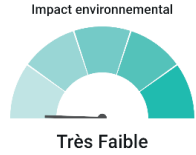
Tous les deux à cinq ans, des virus respiratoires graves sont redoutés chaque hiver sous la forme de grippe saisonnière, de COVID ou d'une combinaison de différents virus respiratoires connus. De telles conditions peuvent devenir un véritable problème de santé publique et accroître la pression sur les services de santé.

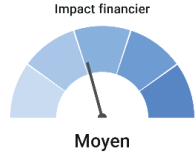
Les résultats de la BNRA montrent la même tendance au niveau belge avec des effets humains très importants comprenant de nombreux décès et un nombre plus élevé de malades. Ceci pourrait entraîner des pénuries de main-d'œuvre et, à long terme, une diminution des performances économiques de la Belgique.











H02 - Maladies animales non zoonotiques

Description

Les maladies animales non zoonotiques sont définies comme des maladies infectieuses qui ne touchent que les animaux. Ces animaux peuvent être sauvages ou domestiques (bétail). Les maladies infectieuses transmissibles à l'homme (zoonoses) ne sont pas incluses.

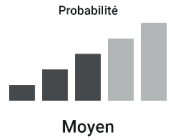
Le scénario le plus pertinent envisage une maladie hautement transmissible ou contagieuse au taux de mortalité élevé, affectant tous les animaux d'une espèce et avec peu ou pas de médicaments ou de mesures réglementaires disponibles.

Analyse

Une épidémie animale correspondant à un scénario extrême pourrait potentiellement se produire dans les décennies à venir. Quelques exemples notables sont la peste porcine africaine, la maladie de Newcastle chez la volaille et la faune sauvage et la maladie de Carré chez les phoques de la mer du Nord, transmissible aux chiens. Les espèces exotiques invasives peuvent également introduire des maladies animales. Le risque de voir émerger de nouvelles espèces (comme les moustiques, et les tiques) capables de propager de nouvelles maladies est important, surtout dans le contexte du changement climatique.

L'impact humain est faible, mais existant : les répercussions sur le bétail, pouvant nécessiter un abattage, peuvent être profondes pour les agriculteurs. L'impact sociétal d'une épidémie animale extrême est estimé comme étant plutôt faible. Les besoins humains (en cas d'indisponibilité temporaire de viande en raison du bétail atteint) et/ou la réputation de la Belgique pourraient être affectés, par exemple en introduisant des embargos commerciaux pour limiter le risque de propagation de la maladie.

L'impact environnemental d'une telle épidémie est estimé faible. Toutefois, la pyramide alimentaire d'autres espèces pourrait être perturbée, causant ainsi des effets indirects.



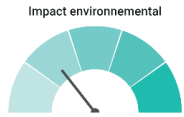
Moyen



Faible



Faible



Faible



Faible

H03 - Maladies des plantes agricoles & pestes

Description

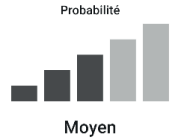
Ce risque inclut les situations suivantes : une contamination bactérienne des plants, une infection fongique, les épidémies de maladies virales, mycoplasmes et viroïdes affectant les plantes et une infestation d'insectes nuisibles. Les maladies et les nuisibles affectant les cultures ne sont pas seulement propagés par des facteurs environnementaux mais aussi par le commerce mondial, les voyages, la circulation et les transports. Le scénario le plus pertinent considère une maladie ou un nuisible hautement contagieux et facilement transmissible qui impacte les sources alimentaires de grande importance nationale ou européenne. Plusieurs types de cultures sont touchés. Un traitement est potentiellement disponible, mais sa distribution est limitée.

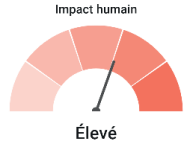
Analyse

Outre l'occurrence directe pour ce risque, les principaux risques causaux identifiés sont les espèces invasives et les tempêtes de grêle. Dans ce dernier cas, les cultures qui ont survécu à la grêle sont affaiblies et plus vulnérables aux maladies et aux nuisibles.

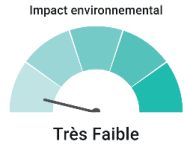
Si une maladie affecte une plante ou une culture très importante pour l'approvisionnement alimentaire et que peu de traitements sont disponibles, elle peut avoir un impact sociétal important sur l'approvisionnement alimentaire. En effet, une telle maladie des plantes agricoles peut entraîner une perte des récoltes et, par conséquent, compromet sérieusement la production alimentaire pour les êtres humains et les animaux.

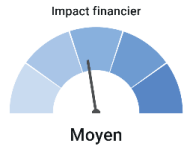
Si un tel scénario n'entraîne pas de famines immédiates ou de pénuries à grande échelle, il peut toutefois limiter les choix alimentaires. L'impact sociétal constitue la conséquence d'une telle situation pour la production alimentaire. Dans l'éventualité où un ou plusieurs types de cultures seraient indisponibles pendant une longue période de temps, ceci pourrait affecter les besoins humains. Néanmoins, une telle maladie devrait être vite identifiée grâce au réseau national de détection des maladies.











H04 - Contaminants dans la nourriture humaine et animale

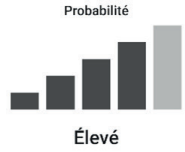
Description

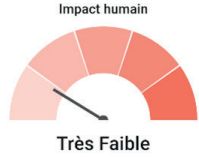
Un contaminant fait référence à toute substance qui n'est pas ajoutée intentionnellement (à une denrée) alimentaire ou à un aliment pour animaux (animaux producteurs ou non de denrées alimentaires), ou l'un de leurs ingrédients, mais qui est néanmoins présente dans cette denrée ou cet aliment à la suite de la production (y compris les opérations effectuées pour l'agriculture, l'élevage et la médecine vétérinaire) ou à la suite d'une contamination de l'environnement. Cette fiche de risque inclut également la possibilité qu'un composant liquide soit contaminé.

Le scénario le plus pertinent implique une situation de consommation limitée et donc de transmission limitée. Le produit en question ne présente pas de risque immédiat pour la santé, mais des symptômes peuvent apparaître après un certain temps. Le produit pourrait être rappelé assez rapidement.

Analyse

L'impact de ce risque est plutôt limité, mais la probabilité est élevée. L'essentiel de l'impact humain proviendrait des effets indirects, comme la propagation de produits dangereux ou de bactéries. Dans la plupart des cas, les autorités prennent des mesures immédiates en cas de contamination de la chaîne alimentaire, ce qui signifie que l'impact sur l'homme reste très limité. Cela pourrait néanmoins entraîner un éventuel impact sociétal suite au retrait du produit du marché et un impact financier dû aux pertes économiques que cela pourrait engendrer pour le producteur.











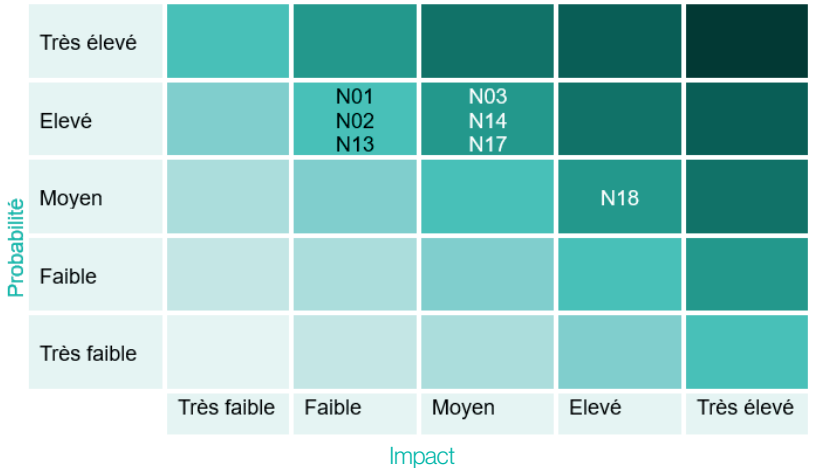
Risques naturels

Les risques naturels comprennent les risques liés à tous les types de conditions météorologiques extrêmes (par exemple inondations, sécheresses, vagues de chaleur et de froid, tempêtes, tornades, grêle, neige, givre et verglas, foudre), aux différents types de processus géophysiques (par exemple affaissement et soulèvement des sols, érosion des berges de rivière) ainsi qu'aux risques extraterrestres (météorites et tempêtes de rayonnement solaire).

La plupart des risques naturels surviennent indépendamment de toute action humaine. Une exception à cette règle concerne les effets de l'empreinte carbone sur le changement climatique et des mesures de protection mises en œuvre pour empêcher les risques naturels de se produire et d'entraîner d'autres risques significatifs.

En général, ces risques se caractérisent par un impact environnemental important. En fonction de la gravité des risques, les impacts sociétaux et financiers peuvent également être élevés. Les incidences sur l'homme sont en général limitées mais il existe des exceptions, comme les vagues de chaleur et les inondations.

Il convient de prendre tout particulièrement en compte les récentes inondations de 2021, qui ont particulièrement influencé les experts dans leur évaluation de ce risque. Ceci sera discuté plus loin dans ce chapitre.



N01, N02, N03 - Inondations
N13 - Sécheresse
N14 - Vague de chaleur / Canicule
N17 - Feux de forêt
N18 - Espèces invasives

Inondations

Description

Cette fiche constitue une synthèse des trois fiches de risques (N01, N02 et N03) de la BNRA, qui traitent des différents types d'inondations.

1° **L'inondation par les eaux de ruissellement (pluviale)** désigne une inondation causée par un excès d'eau qui n'est pas directement lié à une grande rivière ou à un cours d'eau navigable. Il s'agit typiquement de zones situées dans des bassins ou particulièrement exposées à des niveaux d'eau élevés lorsque les précipitations sont exceptionnellement intenses et violentes. Ces inondations se produisent lorsque le volume des précipitations dépasse la capacité du sol ou du réseau de drainage/égouttage à absorber l'eau (par exemple, en raison d'un sol sec empêchant l'infiltration ou de la saturation du réseau d'égouttage).

2° Une **inondation fluviale** se produit lorsque le niveau d'eau d'un cours d'eau (rivière, fleuve, canal) ou d'un plan d'eau déborde sur les zones basses adjacentes (les plaines inondables naturelles) qui sont habituellement hors d'atteinte de l'eau, quelle qu'en soit la cause.

3° **L'inondation côtière** est l'inondation par la mer des zones terrestres situées le long des côtes et des zones de marée des grands fleuves au niveau des estuaires. Les inondations côtières sont le plus souvent le résultat d'ondes de tempête et de vents violents coïncidant avec des marées hautes.

Analyse

Les inondations sont un phénomène qui a des conséquences très diverses.

Ainsi, quels que soit leurs types, les impacts des inondations sont très graves d'un point de vue financier, avec de nombreuses pertes économiques directes et indirectes. À cet égard, les inondations côtières sont encore plus dévastatrices en raison de la concentration des infrastructures le long du littoral et de l'importance du transport maritime.



N03 - Inondation côtière

Peu de causes spécifiques aux inondations peuvent être identifiées. La quantité de précipitations dans une zone donnée est, bien sûr, la plus courante. Dans le cas des inondations côtières, il faut également tenir compte de l'importance capitale des ouvrages de protection contre les inondations, tels les digues et barrages, et des conséquences de leur possible défaillance.

Les scénarios les plus pertinents qui ressortent de la BNRA tendent à se produire à petite échelle, avec seulement quelques zones touchées. Néanmoins, les événements récents ont montré que la Belgique n'est pas à l'abri de situations bien plus catastrophiques et d'inondations de grande ampleur.

Il convient également de souligner que les inondations peuvent être à l'origine de nombreux incidents en cascade, y compris des incidents impliquant des infrastructures (énergétiques ou CBRNe) et la libération de substances dangereuses, et qu'elles sont l'une des principales causes de la propagation d'espèces envahissantes. C'est pourquoi il ne faut pas négliger les dommages causés aux infrastructures de protection, en particulier les digues.

N13 - Sécheresse

Description

Une sécheresse est une période de temps anormalement sec qui dure suffisamment longtemps pour provoquer, en raison du manque de précipitations, un grave déséquilibre hydrologique entre les eaux de surface et les eaux souterraines (qui comprennent à la fois les aquifères profonds et les aquifères peu profonds).

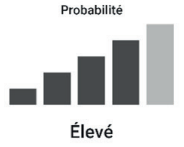
Le scénario de sécheresse le plus pertinent est celui d'une sécheresse régionale ne touchant pas plus de trois provinces, qui dure jusqu'à six mois et se caractérise par la dessiccation des sols et l'assèchement de petites rivières locales, mais sans effets à long terme observés après l'événement.

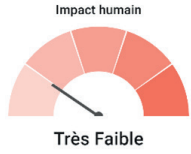
Analyse

Les sécheresses ne sont pas causées par d'autres risques et leur probabilité d'occurrence est très élevée pour la période 2023-2026. Pour la période 2050-2053, les experts n'ont pas établi de tendance claire concernant l'effet du changement climatique sur la probabilité d'occurrence. Les estimations demeurent donc inchangées.

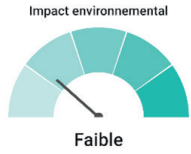
Le scénario de sécheresse proposé a un impact relativement limité. Les effets sur l'environnement sont presque exclusivement dus à la sécheresse elle-même. Les écosystèmes des zones humides sont susceptibles d'être les plus touchés.

La sécheresse a également des effets indirects. Les populations peuvent être affectées si l'approvisionnement en eau potable est perturbé par des pénuries d'eau. La déshydratation des sols due à la sécheresse peut entraîner des mouvements de sol, ce qui peut à son tour perturber les systèmes de drainage et contribuer aux impacts sociétaux. L'impact financier est principalement constitué de déficits publics, car on s'attend à ce que les compagnies d'assurance ne soient plus en mesure de supporter seules le fardeau de la sécheresse.











N14 - Vague de chaleur / Canicule

Description

Il n'existe pas de définition universelle acceptée d'une vague de chaleur.

En Belgique, l'Institut Royal Météorologique parle de vague de chaleur climatique nationale lorsque les températures maximales à Uccle atteignent au moins 25°C pendant au moins cinq jours consécutifs, avec le seuil de 30°C atteint pendant au moins trois jours.

Le scénario de canicule le plus pertinent dure moins de 15 jours et touche cinq à dix provinces. Les températures maximales atteignent 30°C entre cinq et dix jours dont au moins deux jours avec des températures maximales supérieures à 35°C et les températures nocturnes moyennes restent inférieures à 20°C.

Analyse

Les vagues de chaleur ne sont pas causées par d'autres risques. Leur probabilité d'occurrence est très élevée pour la période 2023-2026. Cette probabilité d'occurrence est estimée légèrement plus élevée pour 2050-2053 en raison des effets du changement climatique.

Si l'on considère les dommages des vagues de chaleur, on constate qu'elles causent principalement des impacts sur la santé humaine. Les dommages sociétaux, environnementaux et financiers générés par les canicules existent mais sont plutôt limités.

L'un des effets significatifs d'une vague de chaleur est la pollution chronique de l'air. Celle-ci affectera les personnes les plus vulnérables et entraînera de nombreuses complications médicales (par exemple, des maladies chroniques), voire des séjours à l'hôpital, pouvant aller jusqu'au décès.



N17 - Feux de forêt

Description

Les incendies naturels désignent :

- Les incendies non planifiés ou non contrôlés qui se déclarent dans des zones naturelles telles que les forêts, les prairies, les terrains organiques (tourbières, zones humides), les terres cultivées, les landes ou les dunes et qui peuvent affecter les paysages industriels et résidentiels en se propageant;

- Les incendies non planifiés ou non contrôlés qui commencent à se propager dans la zone frontalière entre les zones urbaines et les zones sauvages et qui peuvent en se propageant affecter les zones naturelles, industrielles et résidentielles.

Le scénario le plus pertinent est celui d'un feu de forêt très violent qui endommage entre 50 et 500ha dans une zone naturelle peu fréquentée (≤ 1000 visiteurs par jour) et menace une à deux zones résidentielles ou sites de loisirs.

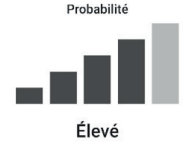
Analyse

Les incendies de forêt ont une probabilité d'occurrence très élevée. Les autres risques causaux potentiels (comme la foudre ou les différents types d'incidents et d'accidents) ne contribuent que pour une part très limitée à la probabilité globale d'occurrence des incendies.

Si l'on considère les impacts des incendies de forêt, on constate que tous les types d'impact sont représentés de manière égale, l'impact environnemental étant le plus important.

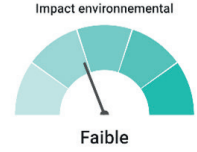
Il convient de noter que les effets indirects résultant des incendies de forêt sont les principaux responsables de ces impacts. En effet, les incendies de forêt créent des espaces vacants qui sont ensuite colonisés par des espèces envahissantes, lesquelles génèrent à leur tour différentes formes d'impact.

Si l'incendie se produit près de notre frontière nationale, il peut également y avoir un impact transfrontalier.











N18 - Espèces invasives

Description

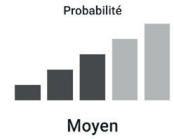
Une espèce exotique envahissante (abrégée EEE, également appelée “espèce invasive”) est une espèce qui a été introduite ou qui s’est répandue en dehors de son aire de répartition naturelle par les activités humaines, et qui s’est ensuite propagée. Une telle espèce peut dès lors constituer une menace pour la biodiversité et/ou les services écosystémiques, tels que l’approvisionnement (matériaux, molécules…), les services culturels (tourisme…), la régulation (climat, maladies, inondations…) ou le cycle biologique (photosynthèse, cycle de l’azote…).

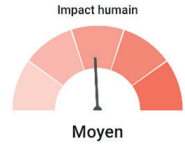
Le scénario le plus pertinent est celui d’une espèce envahissante figurant sur la liste noire, pour laquelle les paramètres d’exposition et d’impact sont très élevés.

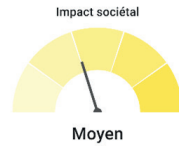
Analyse

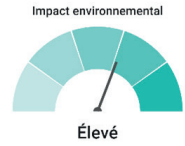
Outre les activités humaines directes, les principales causes de ce scénario d’espèces envahissantes sont les incendies de forêt et les inondations fluviales. Les impacts environnementaux sont prédominants en raison de la menace que les espèces envahissantes font peser sur les espèces indigènes (plantes ou animaux) et sur le fonctionnement des écosystèmes. Toutefois, certaines espèces peuvent également avoir un impact sur la santé, comme les allergies aux piqûres de frelons asiatiques (*Vespa velutina*) ou au pollen d’ambroisie (*Ambrosia artemisiifolia*), les réactions chimiques à certaines plantes (brûlures) ou le développement de zoonoses (par exemple, le raton-laveur – *Procyon lotor*) ou de maladies infectieuses, comme le moustique tigre (*Aedes albopictus*) qui propage notamment la dengue.

Les impacts sociétaux et financiers ne sont pas négligeables, comme le montrent par exemple les risques que la renouée du Japon (*Fallopia japonica*) fait peser sur les infrastructures (par exemple, dommages aux fondations, aux égouts…), ou les terriers creusés par les animaux dans les digues.











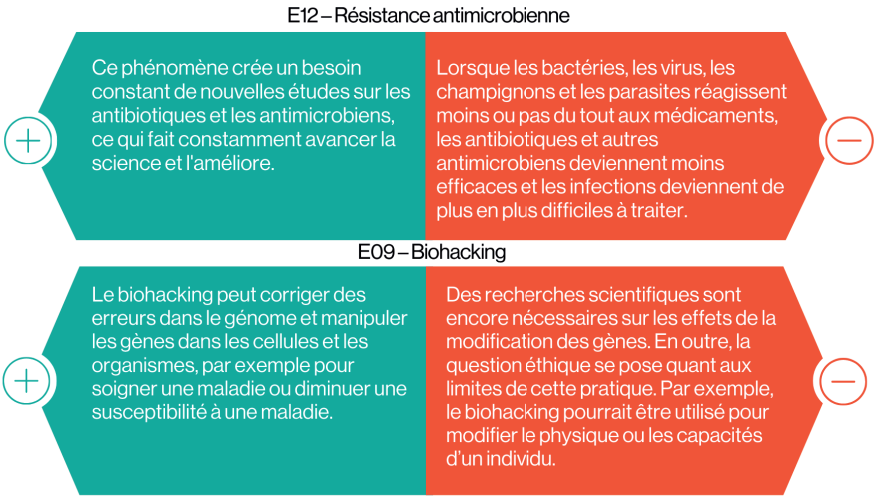
Risques catalyseurs

Risques émergents

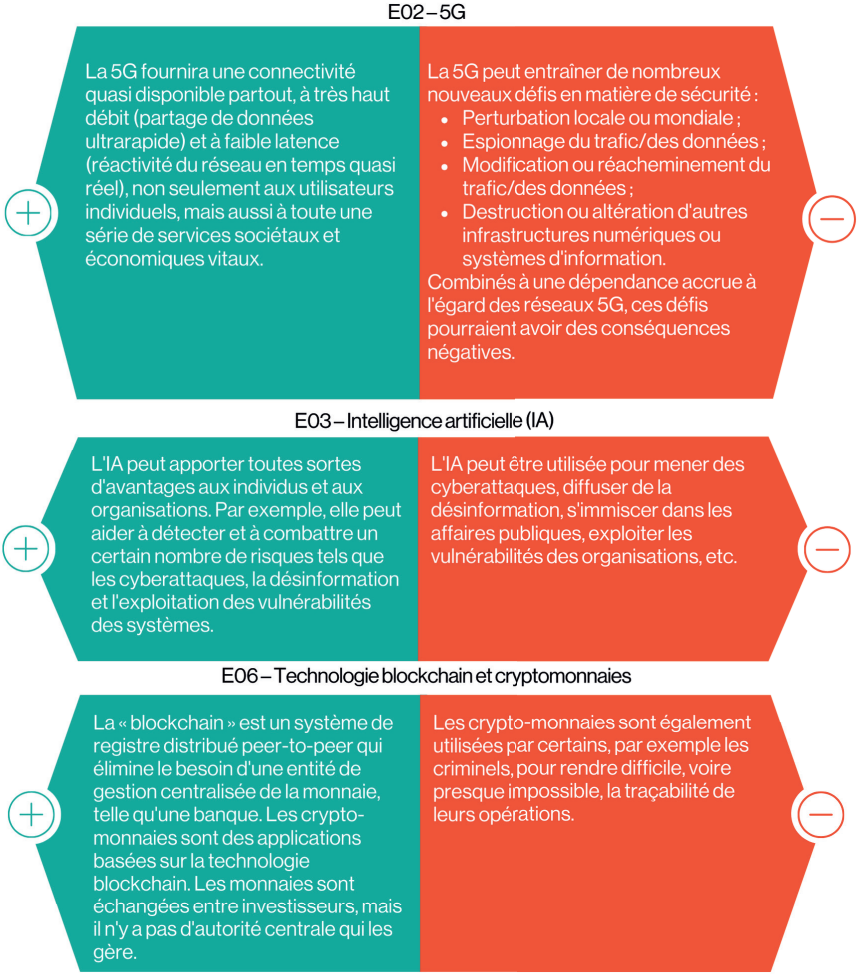
Comme indiqué dans l'introduction, la BNRA prend également en compte onze risques émergents. Ces risques ne représentent pas encore un danger réel pour la société, mais peuvent avoir un effet sur tous les autres risques de la BNRA. Cet effet peut être positif et offrir des opportunités à la société mais il peut aussi se manifester de manière négative.

Étant donné que ces risques sont encore en train de gagner en maturité et que l'on ne sait pas quelle voie de développement ils suivront, il est impossible de les évaluer comme les autres risques.
Les effets du risque émergent (s'il y en a) sur les autres risques devraient idéalement être décrits de manière quantitative mais compte tenu du manque de données historiques et de connaissances sur lesquelles fonder ces hypothèses, une approche qualitative est privilégiée.

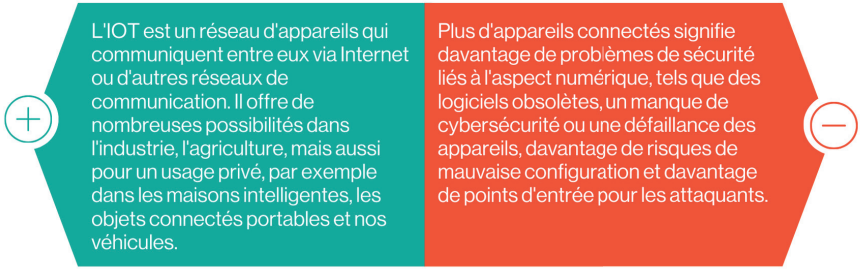
Risques émergents liés à la santé



Risques émergents technologiques



E07 – Internet des objets (IoT)



E08 – Informatique quantique



Risques émergents sociétaux

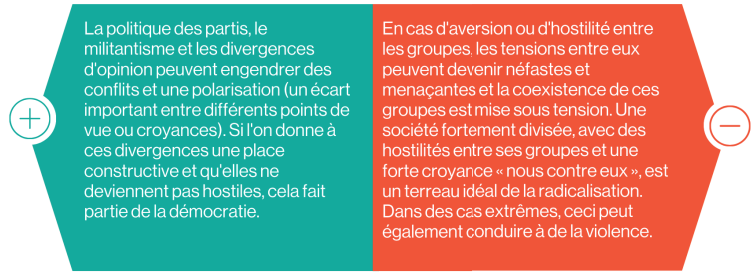
E04 – Transition énergétique



E05 – Interdépendance systémique



E10 – Polarisation de la société



E11 – Erosion de l'intimité et de la vie privée



E01 - Changement climatique

Comparé à d'autres risques émergents, le phénomène du changement climatique a déjà fait l'objet d'études intensives au cours des dernières décennies, ce qui a permis de disposer d'un plus grand nombre de données scientifiques. Les climatologues s'efforcent continuellement de mieux prédire, avec moins d'incertitudes, les répercussions futures du changement climatique. En raison des incertitudes scientifiques existantes, il a été décidé que le changement climatique devait également être considéré comme un risque émergent au sein de la BNRA.

En vue d'atténuer les potentiels effets du changement climatique, des mesures doivent être prises le plus rapidement possible. Pour déterminer les mesures nécessaires à l'amélioration de la résilience des sociétés face aux effets du changement climatique, il faut les sensibiliser à mieux comprendre ce à quoi il faudra faire face.

Pour ce faire, la BNRA tente d'estimer de quelle manière le changement climatique pourrait induire des changements pour les autres risques analysés, non pas pour la période actuelle (2023-2026) mais pour la période 2050-2053, laquelle est supposée être une période pertinente en ce qu'elle coïncide avec les objectifs des plans stratégiques actuellement en cours d'élaboration.

Le changement climatique ayant été étudié plus en détail que la plupart des autres risques émergents, ses effets sur les autres risques ont été estimés par les experts de manière quantitative plutôt que qualitative.

Les scénarios de risque susceptibles d'être influencés par le changement climatique restent les mêmes et les impacts associés ne changent donc pas non plus. Par exemple, des vagues de chaleur se produisant en 2023 ou en 2050 devraient avoir des impacts similaires (sans tenir compte des mesures supplémentaires qui pourraient être adoptées entre-temps).

Les changements dus au changement climatique ne sont donc exprimés que par la probabilité (c'est-à-dire la probabilité directe de leur survenance, et donc pas en raison d'autres événements dangereux) des risques sensibles au changement climatique. Par exemple, les experts ont été interrogés sur l'évolution de la probabilité des vagues de chaleur entre 2023 et 2050 en raison du changement climatique.

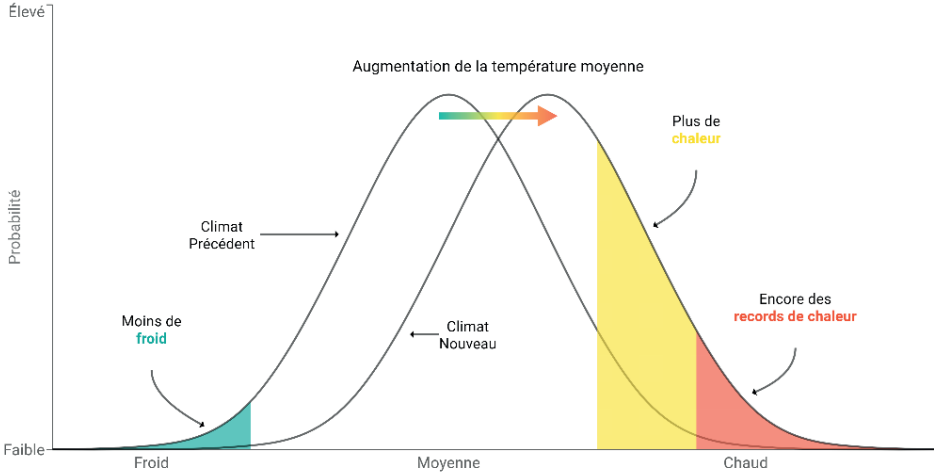


Figure 2 : Impact du changement climatique sur la probabilité d'occurrence (axe y) d'événements extrêmes (axe x) (GIEC, 2007)

Comme le montre la Figure 2, le changement climatique devrait créer un nouveau climat entraînant une augmentation de la fréquence des périodes chaudes (augmentation de la surface jaune).

Pour pouvoir réaliser ces estimations de manière cohérente, une compréhension commune du concept de changement climatique a été trouvée au sein de la communauté d'experts impliqués dans la BNRA. Il a ainsi été convenu d'utiliser un scénario unique dans le cadre de leur projection du changement climatique futur.

Les risques dont la probabilité augmente le plus d'ici 2050-2053 sont mentionnés dans le tableau ci-dessous :

N18 - Espèces Invasives :
Le changement climatique augmentera davantage la présence d'espèces invasives déjà établies et contribuera à leur expansion future. De plus, il favorisera l'arrivée de nouvelles espèces.

Les experts estimant que le risque « Espèces Invasives » est à l'origine des risques **H02 - Maladies Animales et N06 - Érosion des bancs de rivière**, l'occurrence de ceux-ci pourra également augmenter d'ici 2050.

T16 - Défaillance d'une digue :
En Belgique, les digues sont généralement des constructions datant de plusieurs décennies. Comme celles-ci n'ont pas été conçues pour résister aux modifications induites par le changement climatique (par exemple pour prendre en compte les effets de l'élévation du niveau de la mer), on peut s'attendre à ce qu'il y ait un nombre croissant de défaillances en l'absence de mesures d'adaptation.

Les experts estimant que le risque « Défaillance de digue » est une cause majeure du risque **N03 - Inondation Côtière**, l'occurrence de ce risque pourrait s'accroître également d'ici 2050.

N04 - Érosion côtière et modification du littoral :
Comme la probabilité d'ondes de tempête augmente d'ici 2050 et que le niveau de la mer continue à s'élever, le phénomène d'érosion côtière et de modifications du littoral deviendra plus fréquent.

S13 - Défaillance de l'approvisionnement en eau potable :
Les experts estiment que le risque de contamination de l'eau potable pourrait augmenter d'ici 2050. Une telle contamination accrue de l'eau peut résulter de ruptures de canalisations, d'une pollution mal contenue ou même de problèmes techniques au sein des stations de traitement.

M17 - Conflit armé international :
Avec le changement climatique, certaines régions seront confrontées à des catastrophes climatiques, deviendront inhabitables (par exemple, avec l'élévation du niveau de la mer) ou connaîtront de mauvaises récoltes entraînant des pénuries (suite par exemple à des sécheresses ou inondations). Ceci pourrait déstabiliser une région et perturber des sociétés, conduisant de manière quasi inévitable vers un conflit armé international.

Les experts estimant que le risque « Conflit armé international » est l'une des causes majeures du risque **M23 - Afflux de personnes nécessitant une protection internationale**, l'occurrence de ce dernier risque pourrait augmenter également d'ici 2050.

Remarques finales

La *Belgian National Risk Assessment* (BNRA) est avant tout un **processus d'évaluation** basé sur des **indicateurs** de **probabilité** et d'**impacts**. Il n'a pas vocation à prédire l'imprévisible. Il est donc essentiel de préciser que des risques qualifiés de *black swan*s ("cygnes noirs"), soit des **événements extrêmes imprévisibles**, peuvent ne pas avoir été identifiés

Ce rapport contient des informations sur **29 des 118 risques étudiés au sein de la BNRA**. La sélection présentée se compose des **risques les plus importants (valeurs de probabilité et/ou d'impact élevées**) par catégorie de risque (cyber, santé, man-made, naturel, sociétal, économique et technologique), complétés par certains risques qui ont été portés à l'attention du public en raison d'incidents pertinents survenus au cours des dernières années.

Une nouvelle **méthodologie innovante d'évaluation** des risques a été développée pour cette BNRA. Elle établit une nouvelle norme pour les futures évaluations nationales des risques en Belgique. Les itérations futures s'appuieront sur ses principes et permettront d'apporter de nouvelles améliorations.

Les risques sont présentés selon **un format fixe** qui consiste en une brève description, suivie d'une analyse. Ils sont regroupés en catégories de risques et ne font l'objet **d'aucun classement**.

Chaque risque étudié a été évalué et consolidé par un groupe d'experts du domaine concerné. **Plus de 160 experts issus de près de 140 organisations** ont été impliqués dans la réalisation de ces analyses. La présence d'un large éventail d'experts est essentielle pour obtenir des résultats significatifs et soutenus largement. **Les experts sont au cœur de la BNRA et leurs nombreuses contributions sont donc indispensables**.

La BNRA n'appréhende pas seulement les risques comme des événements isolés, mais prend également en compte les **effets en cascade**, qui permettent de comprendre les relations de cause à effet qui existent entre ces risques. Toutefois, il n'a pas étudié les « risques composites », c'est-à-dire des risques multiples et indépendants qui se produiraient simultanément.

La "**polycrise**" est un concept qui peut décrire le paysage complexe des risques d'aujourd'hui. Il s'agit d'une réalité ambiguë et volatile dans laquelle les crises et/ou les urgences ne se produisent pas de manière séquentielle, mais dans laquelle différentes évolutions du paysage des risques et/ou des crises dans différents domaines se développent simultanément, sont interdépendantes, voire se renforcent et s'influencent mutuellement. Une **analyse complémentaire des polycrises** dépasse le cadre de cette BNRA.

Les résultats de l'évaluation des risques sont valables pour la **période 2023-2026**. Par la suite, une nouvelle itération sera effectuée.

Principaux enseignements de la BNRA

Les risques de la **catégorie "man-made"** ont généralement un impact élevé et la plupart d'entre eux ont également une probabilité relativement élevée. À l'exception de l'un d'eux, les risques présentés ne sont pas directement liés à des attaques, mais plutôt à des tensions géopolitiques et à des stratégies d'influence, qu'il s'agisse de menaces hybrides, d'espionnage ou de désinformation. Dans un monde de plus en plus connecté, les **cyberrisques** les plus graves sont généralement liés à des actions d'origine humaine (malveillantes et intentionnelles), soit avec une intention criminelle, soit dans le cadre d'une menace hybride. Les probabilités sont souvent assez élevées, mais l'impact peut varier en fonction du scénario.

Les **risques sociétaux** peuvent être divisés en deux grandes catégories:

- Les risques "HILP" (*high impact, low probability*), c'est-à-dire les risques ayant un impact très élevé mais une probabilité faible ou très faible, comme les ruptures d'approvisionnement en énergie ;

- Les risques ayant une probabilité plus élevée et des impacts sociétaux et financiers particulièrement importants, comme les perturbations dans le secteur de l'aviation.

Les **risques économiques et technologiques** sont généralement des risques "HILP". Les mesures de prévention et de préparation ainsi que la surveillance continue semblent avoir considérablement réduit les probabilités d'occurrence, mais des efforts persistants restent de toute évidence nécessaires.

Les scénarios les plus pertinents en matière de **risques sanitaires** tendent à correspondre à des situations à faible impact. Toutefois, dans le cas d'événements graves, tels que les maladies infectieuses, on ne peut exclure des impacts sociétaux et humains importants.

Les **risques naturels** ont généralement été évalués avec des probabilités d'occurrence élevées, même si les impacts varient fortement d'un risque à l'autre. La plupart des scénarios décrits se rapportent à des situations bien définies et à petite échelle, à l'exception des espèces invasives.

Enfin, l'analyse des **risques émergents** donne un aperçu de l'avenir et des pistes d'évolution potentielles pour les risques existants. Le **changement climatique**, en particulier, augmentera considérablement la probabilité de nombreux risques naturels majeurs ou extrêmes d'ici à 2050. La prise en compte de leurs effets en cascade montre que la plupart des autres risques sont indirectement influencés par le changement climatique d'une manière ou d'une autre.

Catalogue des Risques

Risques Cyber

- C01 - Vulnérabilité matérielle ou logicielle
- C02 - Mauvaise configuration du logiciel ou du matériel
- C03 - Cyberattaque contre une infrastructure CBRNe
- C04 - Cyberattaque contre une institution gouvernementale
- C05 - Cyberattaque contre une infrastructure vitale

Risques émergents

- E01 - Changement climatique
- E02 - 5G
- E03 - Intelligence artificielle
- E04 - Transition énergétique
- E05 - Interdépendance systémique
- E06 - Technologie blockchain et cryptomonnaies
- E07 - Internet des objets (IoT)
- E08 - Informatique quantique
- E09 - Biohacking
- E10 - Polarisation de la société
- E11 - Erosion de l'intimité et de la vie privée
- E12 - Résistance antimicrobienne

Risques sanitaires

- H01 - Maladies infectieuses
- H02 - Maladies animales non zoonotiques
- H03 - Maladies des plantes agricoles & pestes
- H04 - Contaminants dans la nourriture humaine et animale
- H05 - Pollution chronique de l'air ambiant
- H06 - Pollution chronique de l'environnement aquatique
- H07 - Pollution chronique du sol
- H08 - Produits médicaux de qualité insuffisante et falsifiés
- H09 - Rejet en masse de la médecine moderne
- H10 - Processus de nature socio-psychologique

Risques "man-made"

- M01 - Acteur hybride
- M02 - Acteur d'extrême-gauche
- M03 - Acteur d'extrême-droite
- M04 - Acteur du crime organisé
- M05 - Acteur extrémiste religieux
- M06 - Attaque contre une infrastructure CBRNe
- M07 - Attaque contre une institution gouvernementale ou internationale
- M08 - Attaque contre un groupe de personnes ou une communauté
- M09 - Attaque contre une cible facile
- M10 - Attaque contre un VIP
- M11 - Attaque contre une infrastructure vitale
- M12 - Attaque sur un transport de biens dangereux
- M13 - Opérations d'information
- M14 - Espionnage
- M15 - Investissements directs étrangers (IDE)
- M16 - Ingérence
- M17 - Conflit Armé International (CAI)
- M18 - Trafic de drogue
- M19 - Fraude économique
- M20 - Traite des êtres humains et contrebande
- M21 - Troubles sociaux
- M22 - Grève
- M23 - Afflux de personnes nécessitant une protection internationale

Risques naturels

- N01 - Inondation par les eaux de ruissellement
- N02 - Inondation fluviale (ou de rivière)
- N03 - Inondation côtière
- N04 - Erosion côtière et modification du trait de côte
- N05 - Subsidence et soulèvement des sols
- N06 - Erosion des berges de cours d'eau
- N07 - Glissement de terrain ou coulée de débris

- N08 - Vague de froid
- N09 - Givre
- N10 - Neige
- N11 - Grêle
- N12 - Foudre
- N13 - Sécheresse
- N14 - Vague de chaleur / Canicule
- N15 - Tempête
- N16 - Tornade
- N17 - Feux de forêt
- N18 - Espèces invasives
- N19 - Tremblement de terre
- N20 - Tsunami
- N21 - Éruption volcanique à l'étranger
- N22 - Tempête de rayonnement solaire
- N23 - Impact de météorite

Risques sociétaux

- S01 - Défaillance de l'approvisionnement en électricité
- S02 - Défaillance de l'approvisionnement en gaz naturel
- S03 - Défaillance de l'approvisionnement en pétrole
- S04 - Défaillance de l'approvisionnement en hydrogène
- S05 - Défaillance des réseaux de chaleur
- S06 - Défaillance du transport aérien
- S07 - Défaillance du transport ferroviaire
- S08 - Défaillance du transport naval
- S09 - Défaillance du transport routier
- S10 - Défaillance des services financiers
- S11 - Défaillance de l'offre de soins médicaux
- S12 - Défaillance de l'approvisionnement en matériel médical
- S13 - Défaillance de l'approvisionnement en eau potable
- S14 - Défaillance de la gestion des eaux usées
- S15 - Défaillance des infrastructures digitales
- S16 - Défaillance des fournisseurs de services digitaux
- S17 - Défaillance des services d'urgence
- S18 - Défaillance de l'administration publique centrale et du gouvernement
- S19 - Défaillance des services spatiaux
- S20 -Défaillance des services postaux
- S21 - Défaillance de l'approvisionnement en denrées alimentaires
- S22 - Défaillance de la gestion des déchets

Risques économiques et technologiques

- T01 - Incident dans une installation CBRNe
- T02 - Incident dans une installation Seveso
- T03 - Incident impliquant le transport de substances CBRNe
- T04 - Décharge d'agents explosifs
- T05 - Incident dans une centrale nucléaire
- T06 - Libération d'agents biologiques
- T07 - Libération d'agents chimiques
- T08 - Libération d'agents nucléaires
- T09 - Libération d'agents radioactifs
- T10 - Accident aérien
- T11 - Accident routier
- T12 - Accident ferroviaire
- T13 - Accident maritime
- T14 - Accident sur les voies navigables intérieures
- T15 - Défaillance d'un pont
- T16 - Défaillance d'une digue
- T17 - Défaillance d'un barrage
- T18 - Défaillance structurelle d'un bâtiment
- T19 - Incendie ou explosion dans une zone urbaine ou résidentielle
- T20 - Feu ou effondrement dans un tunnel
- T21 - Pénurie de matières premières
- T22 - Choc financier
- T23 - Déficit gouvernemental

Vers une Belgique plus résiliente

Comme nous l'avons vu à la lumière d'événements extrêmes tels que les inondations de 2021, la méconnaissance des bons réflexes face au risque peut rendre la gestion des situations d'urgence encore plus difficile. La résilience de la population et des infrastructures face aux différents risques est devenue le mot d'ordre dans notre société, mais il faut continuer à l'intégrer et la développer.

C'est non seulement une stricte nécessité pour notre pays, mais c'est aussi une exigence de l'Union européenne. Les interdépendances systémiques (en cascade) désormais établies continueront à se développer à l'avenir. La diversité croissante des risques (transfrontaliers) potentiels dans une Europe avec moins de frontières intérieures a conduit à l'élaboration et à l'adoption par tous les États membres de la directive CER de 2022. Cette directive est consacrée à la résilience des entités critiques et de leurs secteurs respectifs. Comme la mise en œuvre de la directive CER ne vise qu'un certain nombre de secteurs vitaux, elle ne permettra pas d'atteindre un niveau uniforme de résilience dans l'ensemble de la société. Toutefois, à mesure que de nouvelles recommandations, de nouvelles analyses de risques et des mesures de résilience renforceront ces secteurs vitaux, elles induiront très probablement des effets positifs pour d'autres secteurs qui ne sont pas visés par la directive CER.

L'un des principaux objectifs de la présente évaluation nationale des risques est donc de contribuer modestement au développement d'une culture du risque en Belgique et d'accroître la résilience de notre société dans son ensemble.

Ses résultats sont valables pour une période de trois ans, mais des évaluations à mi-parcours et de nouvelles analyses peuvent être effectuées au niveau fédéral ainsi qu'à d'autres niveaux (régions, provinces, secteurs) pour mettre à jour les résultats actuels ou les évaluer plus en détail et préparer la prochaine itération.

La sûreté et la sécurité sont l'affaire de tous. Cela implique avant tout une connaissance suffisante des risques potentiels auxquels la Belgique est confrontée.

Centre de crise National

Septembre 2024

Hertogsstraat 53
1000 Brussel

www.crisiscentrum.be

National Crisis Centre
CrisisCenter Belgium
Crisiscentrum / Centre de Crise