Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Kennisnotitie

Inventarisatie van externe dreigingen voor bedrijven die werken met gevaarlijke stoffen

RIVM

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

T 088 689 89 89

Auteurs:
T.J. Kerckhoffs
C.L.G. Stähler
G.H. Heideman
Centrum:
Veiligheid
Contact:
Henrieke Heideman
henrieke.heideman@rivm.nl
Kenmerk:
KN-2026-0040
DOI:
10.21945/RIVM-KN-2026-0040
Datum:
17 april 2026

1. Inleiding

Seveso-inrichtingen en ARIE-bedrijven werken met grote hoeveelheden gevaarlijke stoffen. Denk hierbij bijvoorbeeld aan chemische fabrieken, opslagbedrijven voor gevaarlijke stoffen en raffinaderijen, maar bijvoorbeeld ook bedrijven in de voedingsmiddelindustrie (grote koelinstallaties) of garages met grote opslagen voor oplosmiddelen en lakken. Naast de industriële veiligheidsrisico's (bijvoorbeeld werken met zware machines), lopen de werknemers bij deze bedrijven door de aanwezigheid van gevaarlijke stoffen het risico aan een brand, explosie of gifwolk blootgesteld te worden. Tegelijkertijd worden zij net als de rest van de maatschappij geconfronteerd met veranderende externe dreigingen. Zo zal als gevolg van klimaatverandering vaker sprake zijn van meer ernstige uitingen van extreem weer, zoals extreme neerslag en hitte (KNMI, 2023). Verder moeten deze bedrijven hun (digitale) processen beschermen tegen ongewenste invloed van buitenaf in een periode waarin het dreigingslandschap rond digitale veiligheid steeds complexer wordt (NCTV, 2025a). Ook is er in Europa steeds vaker sprake van hybride dreigingen in de vorm van bijvoorbeeld fysieke sabotage(pogingen) (Baumann & Pynnöniemi, 2025).

Alhoewel dreigingen als extreem weer en cyberaanvallen niet per se nieuw zijn, worden deze en andere typen dreigingen wel steeds frequenter, complexer of krijgen bedrijven te maken met (relatief) nieuwe uitingen hiervan. Deze dreigingen kunnen de bedrijfscontinuïteit mogelijk in het geding brengen en potentieel zelfs leiden tot een zwaar ongeval[1] waarbij gevaarlijke stoffen vrijkomen met negatieve gevolgen voor zowel medewerkers als voor de omgeving. Er zijn relatief veel richtlijnen en een mate van ervaring rond het voorkomen van een zwaar ongeval als gevolg van problemen binnen de processen die zich in een bedrijf zelf afspelen. Dit geldt in mindere mate voor het beheersen van de gevolgen van (nieuwe) externe dreigingen. Het is dus belangrijk om verder kennis op te doen over hoe bedrijven zich weerbaar kunnen maken tegen deze externe dreigingen.

2. Doel van het onderzoek en leeswijzer

Er zijn veel verschillende soorten dreigingen die de maatschappij kunnen raken (ANV, 2022). Niet al deze dreigingen zijn echter even relevant voor Seveso-inrichtingen en ARIE-bedrijven (hierna: bedrijven). In opdracht van de Nederlandse Arbeidsinspectie (NLA) heeft het RIVM geïnventariseerd welke dreigingen mogelijk kunnen leiden tot een zwaar ongeval met gevaarlijke stoffen.

[1] Een "zwaar ongeval" wordt in de Seveso-richtlijn en ARIE-regeling gedefinieerd als: een gebeurtenis zoals een zware emissie, brand of explosie als gevolg van onbeheerste ontwikkelingen tijdens de bedrijfsuitoefening in een inrichting waarop deze richtlijn van toepassing is, waardoor hetzij onmiddellijk, hetzij na verloop van tijd ernstig gevaar voor de menselijke gezondheid of het milieu, binnen of buiten de inrichting ontstaat en waarbij een of meer gevaarlijke stoffen betrokken zijn.

Deze inventarisatie kan als basis dienen voor verder, meer toegespitst onderzoek naar de weerbaarheid van bedrijven. In deze notitie wordt geen uitspraak gedaan over de mate van weerbaarheid van de bedrijven in kwestie of over manieren om hier invloed op uit te oefenen. Ook bevat de notitie geen onderlinge prioritering van de geselecteerde dreigingen wat betreft waarschijnlijkheid en gevolgen.

Hieronder wordt eerst ingegaan op enkele in dit onderzoek gehanteerde definities. Vervolgens worden de gehanteerde criteria voor de selectie van dreigingen besproken. Hierna komen de gehanteerde bronnen en het selectieproces zelf aan bod. Dit wordt gevolgd door een overzicht van de geselecteerde dreigingen en bijbehorende categorieën in tabelvorm en een nadere toelichting op deze categorieën. Het laatste deel van de notitie bevat een reflectie op de inventarisatie van dreigingen en hoe deze toe te passen in eventueel verder onderzoek.

3. Definities

Alvorens in te gaan op verschillende soorten dreigingen, is het van belang om een aantal definities vast te stellen. Te meer omdat een aantal begrippen verschillend geïnterpreteerd kan worden. Zo wordt 'klimaatverandering' in verschillende publicaties zowel gepresenteerd als ontwikkeling, als dreiging en/of als risico.

Het algemene begrip *dreiging* refereert aan een bepaalde gebeurtenis of set aan gebeurtenissen met een bepaalde waarschijnlijkheid en een mogelijk negatief gevolg (samen: het 'risico') voor bijvoorbeeld de maatschappij, een bedrijf, een individu of een specifieke groep mensen. Voorbeelden hiervan zijn overstromingen of een cyberaanval.[2] Het vaststellen van de precieze waarschijnlijkheid of de exacte gevolgen van verschillende dreigingen valt buiten de scope van dit onderzoek. De mate van gevolgen of ernst is daarentegen wel relevant voor de selectie van dreigingen. Binnen dit onderzoek ligt de nadruk op dreigingen die voor een bedrijf een externe oorsprong hebben, maar binnen het bedrijf (potentieel) kunnen leiden tot een zwaar ongeval met gevaarlijke stoffen met gevolgen voor de fysieke veiligheid van medewerkers. In deze notitie gaat het om dreigingen van een danige omvang dat ook (een deel van) de maatschappij mogelijk ontwricht als ze plaatsvinden. Bedreigingen voor de arbeidsveiligheid zoals beknellingen of vallen van hoogte worden daarom in deze notitie niet meegenomen.

Onder arbeidsveiligheid wordt in deze verstaan het voorkomen van gezondheidsschade bij medewerkers als gevolg van ongevallen op het werk (RIVM, 2024; RIVM & TNO, 2023). De nadruk in dit onderzoek ligt dus op het fysieke veiligheidscomponent van zware ongevallen als gevolg van externe dreigingen. Hierbij kan als gevolg in de praktijk uiteraard ook sprake zijn van de mentale gezondheidsschade van medewerkers. Dit component blijft hier buiten beschouwing, maar kan wel relevant zijn voor een vervolgonderzoek rond weerbaarheid.

De term weerbaarheid wordt veelvuldig gebruikt, en wordt ook wel veerkracht of *resilience* genoemd. Er bestaat echter geen eenduidige definitie (NIPV, 2024). Weerbaarheid wordt in deze notitie gedefinieerd als het vermogen van bijvoorbeeld een organisatie om de negatieve gevolgen en/of waarschijnlijkheid van een dreiging te mitigeren. In het geval van het onderwerp van deze notitie gaat het hier dan om het mitigeren van de waarschijnlijkheid dat een externe dreiging leidt tot een zwaar ongeval.

[2] Deze definitie komt voort uit een samenvoeging van de definities van dreiging en risico zoals gehanteerd in de Rijksbrede Risicoanalyse 2022 (ANV, 2022, p. 81).

Onderdeel van weerbaarheid is het vermogen om weer terug te keren naar een normale situatie volgend op het plaatsvinden van een dreiging.[3] Om beter te kunnen werken met de term weerbaarheid, is het nuttig om deze onder te verdelen in verschillende fasen, verbonden aan de veiligheidscyclus (RAND Europe, 2024; Ganin et al., 2016):

- Plannen: voorbereiden op eventuele dreigingen;
- Absorberen: respons op de dreiging en het verwerken van de initiële schok van een dreiging door de organisatie;
- Herstellen: terugkeren naar een normale werking van bijvoorbeeld de organisatie;
- Aanpassen: wijzigingen maken (op systeemniveau) gericht op betere toekomstige absorptie en herstel.

4. Selectiecriteria

Voor dit project wordt specifiek gekeken naar dreigingen die aan *elk* van vier criteria voldoen:

1. Ze hebben een oorsprong buiten de grenzen van bedrijven;
2. Ze hebben redelijkerwijs een substantieel effect;
3. De veiligheid van medewerkers wordt potentieel getroffen;
4. Relevantie: Ze zijn actueel, of aan verandering onderhevig.

Bovenstaande criteria komen voort uit de gehanteerde definities binnen dit onderzoek, de doelstelling van het onderzoek én uit de taken van de NLA.[4] Elk van de criteria wordt hieronder verder toegelicht.

Criterium 1: oorsprong
Alleen de dreigingen waarbij de oorsprong buiten de grenzen van bedrijven ligt worden meegenomen in de selectie. In het geval van Seveso-inrichtingen en ARIE-bedrijven zijn er dreigingen die zich voor kunnen doen binnen de reguliere bedrijfsvoering. Bijvoorbeeld het lekken van een brandbaar gas met als gevolg een brand, veroorzaakt door technisch of menselijk falen. Aan dit soort 'interne' dreigingen wordt al uitgebreid aandacht besteed in de bestaande veiligheidsrapporten (zie o.a. IPLO, 2026). Het is denkbaar dat een grootschalige brand van een naburig bedrijf overslaat naar de omgeving (domino-effect[5]). Deze effecten vallen om dezelfde reden buiten de scope. Wat wel binnen de scope valt zijn cascade-effecten. Zo kan het zijn dat een externe dreiging (bijvoorbeeld een cyberaanval, extreme weersomstandigheden of een ongeval bij een naburig bedrijf) ertoe leidt dat er binnen het bedrijf zelf processen worden verstoord waardoor er een zwaar ongeval ontstaat.

Criterium 2: substantieel effect
Het tweede criterium is dat dreigingen een substantieel effect dienen te hebben, wat inhoudt dat ze niet binnen de reguliere bedrijfsvoering kunnen worden opgevangen. Dus de reguliere aan het bedrijf verbonden logistieke, BHV of IT-processen zijn niet in staat om de situatie te verhelpen. Het gaat dus om een substantieel vertrek van de 'normaal' situatie en het (mogelijk) ontstaan van een zwaar ongeval. Dit betekent in de praktijk dat het ook zal gaan om dreigingen die de veiligheid van meerdere medewerkers raken en veelal dus om meer ernstige uitingen van bepaalde typen dreigingen. Zo kunnen cyberaanvallen veel verschillende vormen aannemen. Van het verkrijgen van

[3] Deze definitie is in de kern gebaseerd op de definitie naar voren gebracht door RAND Europe (2024, p.17) als onderdeel van een inventarisatie van verschillende definities en het gebruik van de term weerbaarheid.
[4] De NLA houdt toezicht op de Seveso III-richtlijn zoals opgenomen in het Besluit Activiteiten Leefomgeving (Bal) en de Aanvullende risico-inventarisatie en -evaluatie (ARIE-regeling). Ter beperking van de risico's voor werknemers en de omgeving van bedrijven die werken met grote hoeveelheden gevaarlijke stoffen (NLA, 2026).
[5] In het Besluit kwaliteit leefomgeving (Bkl) en het Omgevingsbesluit staan regels over hoe het bevoegd gezag om moet gaan met domino-effecten bij een Seveso-inrichting.

persoonsgegevens waarbij het minder aannemelijk is dat dit kan leiden tot een zwaar ongeval, tot gerichte sabotageacties gericht op industriële controleprocessen waarbij dit wel tot de mogelijkheden behoort.

Criterium 3: veiligheid
Dreigingen worden alleen meegenomen als zij een negatief effect hebben op de veiligheid van medewerkers. De nadruk voor de selectie van dreigingen ligt hierbij op de fysieke component.[6] Dat wil enerzijds zeggen dat de dreiging rechtstreeks binnen het bedrijf leidt tot een (mogelijk) zwaar ongeval met gevolgen voor de (arbeids)veiligheid. Anderzijds kan het ook zijn dat de dreiging leidt tot beïnvloeding van werknemers in een andere (privé)context, waardoor vervolgens de veiligheid en het welzijn van collega's op de werkplek in het geding komt. Een voorbeeld hiervan is als medewerkers in periodes van extreem hoge temperaturen thuis veel hittestress ervaren en als gevolg minder scherp zijn waardoor de kans op een zwaar ongeval toeneemt.

Criterium 4: relevantie
Dreigingen worden alleen meegenomen als:

- Ze in de toekomst mogelijk vaker voorkomen of zij als meer urgent of reëel worden gezien dan voorheen. Extreme hitte is bijvoorbeeld niet een nieuwe dreiging, maar wel één waar bedrijven steeds vaker en steeds langer mee te maken zullen krijgen en die daardoor vanuit het onderwerp weerbaarheid steeds interessanter wordt;
- Of als er meer kennis over beschikbaar ze is dan voorheen. Als gevolg van de Covid-19 pandemie is er bijvoorbeeld meer inzicht dan voorheen in hoe een dergelijke dreiging zich vertaalt naar de werkvloer
- Of als ze veranderlijk zijn van aard. Dit wil zeggen dat er nieuwe uitingen van een bepaalde dreiging zijn. Een voorbeeld is het gebruik van nieuwe op AI gebaseerde technieken door cybercriminelen.

Voor dit criterium is onder meer gekeken naar de Trendanalyse Nationale veiligheid 2024 (ANV, 2024), waarin voor veel verschillende soorten dreigingen een overzicht wordt gegeven van eventuele ontwikkelingen.

5. Bronnen en selectieproces

Voor het creëren van een groslijst van dreigingen is voortgebouwd op reeds bestaande inventarisaties van bredere, maatschappelijke dreigingen van (relatief) substantiële omvang op twee niveaus:[7]

- De Rijksbrede Risicoanalyse (RbRa), opgesteld door het Analistennetwerk Nationale Veiligheid (ANV). In deze documenten worden dreigingen opgenomen die mogelijk de maatschappij als geheel kunnen ontwrichten.
- De regionale risicoprofielen, opgesteld door de 25 veiligheidsregio's. In deze documenten worden dreigingen in kaart gebracht die op regionaal niveau van belang zijn. Binnen dit onderzoek zijn de regionale risicoprofielen van vijf veiligheidsregio's meegenomen: Rotterdam-Rijnmond (2022-2025), Amsterdam Amstelland, Zeeland (2020-2023, Limburg Noord en Zuid (2023-2027) en Midden- en West-Brabant (2023-2027). Deze vijf regio's zijn gekozen omdat zij relatief veel (chemische) industrie in hun verzorgingsgebied hebben samen met het feit dat de uitgebrachte risicoprofielen nog (relatief) actueel zijn.

[6] In het geval van een blootstelling aan gevaarlijke stoffen als gevolg van een zwaar ongeval, vallen ook de gezondheidsgevolgen hiervan op de langere termijn onder deze afbakening.
[7] Alle genoemde documenten zijn opgenomen in de referentielijst onderaan dit document.

Gezamenlijk bevatten de bovenstaande documenten in totaal ongeveer 300 dreigingen, voor een groot deel uitgewerkt in scenario's of korte omschrijvingen. Het hoge aantal komt primair voort uit een overlap aan dreigingen tussen de verschillende documenten. Voor veel dreigingen geldt namelijk dat deze zowel op nationaal als (door heel Nederland) op regionaal niveau relevant zijn. Ook kan één dreiging in veel verschillende scenario's worden uitgewerkt. Voor een infectieziektenuitbraak kan bijvoorbeeld sprake zijn van veel verschillende soorten ziekteverwekkers, elk ook met een eigen transmissieroute.

Wanneer de 300 dreigingen naast de vier eerdergenoemde criteria voor dit onderzoek worden gelegd, blijven er ruim 100 dreigingen over. Deze overgebleven dreigingen zijn vervolgens gegroepeerd en gecategoriseerd.

6. Inventarisatie en categorisering van dreigingen

In de onderstaande tabel wordt de gegroepeerde selectie van dreigingen weergegeven aan de hand van zes categorieën: infectieziekten; natuurrampen; vitale infrastructuur; digitale veiligheid; geweld en geopolitiek. De linkerkolom geeft waar nodig een indeling in subcategorieën weer. De rechterkolom bevat voorbeeldscenario's. Deze voorbeelden zijn gebaseerd op de scenario's uit de bestaande inventarisaties (zie paragraaf 5). Soms is de benaming letterlijk (bijv. 'sneeuwstorm') overgenomen uit de bestaande inventarisaties, in andere gevallen zijn benamingen samengevoegd of zo omschreven dat ze zelfstandig leesbaar zijn.

Tabel 1: inventarisatie van dreigingen

(Sub)categorie	**Voorbeeldscenario's**
[1] Infectieziekten	
Infectieziekten humaan	(Griep)epidemie
Infectieziekten humaan	(Griep)pandemie
Infectieziekten humaan	Pandemie door een mens overdraagbaar respiratoir virus (zoals Covid-19)
Infectieziekten humaan	Door voedsel overdraagbare infectieziekte
Infectieziekten humaan	Exotische ziekteverwekker als gevolg van klimaatverandering (malaria, knokkelkoorts etc.)
Infectieziekten humaan	Besmettingsgevaar vanuit buitenland met in Nederland niet-voorkomende ziekte
[2] Natuurrampen	
Extreem weer	Sneeuwstorm
Extreem weer	Extreme hitte (en droogte)
Extreem weer	Extreme droogte (en hitte)
Extreem weer	Storm en windhozen
Extreem weer	Extreme neerslag (o.a. wateroverlast)
Extreem weer	Koudegolf
Extreem weer	Combinatie extreme kou, sneeuw en ijzel
Overstroming	Overstroming vanuit de zee
Overstroming	Overstroming vanuit een rivier
Overstroming	Dijkdoorbraak rivier
Overstroming	Vollopen van een polder

(Sub)categorie	**Voorbeeldscenario's**
Natuurbrand	Onbeheersbare natuurbranden met grootschalige evacuatie
Natuurbrand	Bermbrand, brand groenstroken, heide, veen- en/of duinbrand
Aardbevingen	Natuurlijke aardbeving
Aardbevingen	Geïnduceerde aardbeving als gevolg van menselijke activiteiten in de ondergrond
Instorting	Zinkgat
[3] Vitale infrastructuur	
Verstoring vitale infrastructuur	Landelijke black-out
Verstoring vitale infrastructuur	(Gedeeltelijke) uitval/verstoring elektriciteitsvoorziening
Verstoring vitale infrastructuur	Verontreiniging of uitval drinkwaternet
Verstoring vitale infrastructuur	Uitval/verstoring spraak- en datacommunicatie
Verstoring vitale infrastructuur	Verstoring voedselvoorziening
Verstoring vitale infrastructuur	Verstoring afvalverwerking en afvalwaterzuivering
Verstoring vitale infrastructuur	Uitval/verstoring gasvoorziening
[4] Digitale veiligheid	
Moedwillig	Aanval op *cloud service provider* (online dataopslag)
Moedwillig	Digitale sabotage, bijvoorbeeld cyberaanval op industriële controlesystemen
Moedwillig	Nevenschade eigen systemen als gevolg van cyberaanval elders (bijv. virus)
Moedwillig	Grootschalige cyberaanval op systemen (bijv. DDoS)
Moedwillig	Doelgerichte verstoring telecommunicatie (internet) en ICT (uitval infrastructuur)
Moedwillig	Cybercriminaliteit waaronder *ransomware* aanvallen
Niet-moedwillig	Uitval belangrijke systemen door configuratie-fout grote internetdienstverlener
Niet-moedwillig	Uitval robots/AI in technologische processen
Niet-moedwillig	Uitval infrastructuur telecommunicatie (internet) en ICT door technisch/menselijk falen
[5] Geweld	
Georganiseerde criminaliteit	Criminele inmenging bedrijfsleven
Georganiseerde criminaliteit	Geweld vanuit georganiseerde criminaliteit
Maatschappelijke onrust/ verstoring openbare orde	Verstoring openbare orde (bijv. blokkades)
Maatschappelijke onrust/ verstoring openbare orde	Rel rondom demonstraties en andere manifestaties
Maatschappelijke onrust/ verstoring openbare orde	Onrust bij groot industrieel/chemisch incident
Maatschappelijke onrust/ verstoring openbare orde	Polarisatie rond complottheorieën
Gewelddadig extremisme	Gewelddadige uitingen als '*homevisits*', brandstichting, geweldpleging en vernielingen

(Sub)categorie	Voorbeeldscenario's
Terrorisme	Gewelddadige bestorming (en gijzeling)
Terrorisme	Terrorisme gericht tegen personen
Terrorisme	Terrorisme gericht tegen (vitale) infrastructuur en voorzieningen
Hybride dreigingen	(Digitale) sabotage[8] bijvoorbeeld d.m.v. brandstichting, plaatsen explosieven, drones, vernielingen
Hybride dreigingen	(Digitale) spionage
Hybride dreigingen	Infiltratie en beïnvloeding (bijvoorbeeld door chantage)
[6] Geopolitiek	
Hybride dreigingen	Alle uitingen van uitingen van ongewenste buitenlandse hybride operaties onder de categorie geweld
Gewapend conflict[9]	Grootschalig militair conflict met betrokkenheid Nederland
Gewapend conflict	Grootschalig (nucleair) militair conflict zonder betrokkenheid Nederland
Verstoring in internationale handelsstromen	Handelsbeperkingen in grondstoffen of andere goederen, bijvoorbeeld als gevolg van een handelsoorlog of als politiek drukmiddel

7. Toelichting op de dreigingscategorieën

De bovenstaande dreigingen worden hieronder toegelicht per categorie.

Categorie 1: infectieziekten

Deze categorie bevat meerdere soorten dreigingen die te maken hebben met besmettingsgevaar richting medewerkers als gevolg van verschillende typen infectieziekten. Om te beginnen vallen hieronder grootschalige uitbraken van humane infectieziekten, zoals Covid of influenza. In deze gevallen kan de bedrijfscontinuïteit in het geding komen doordat veel medewerkers tegelijkertijd ziek zijn of wegens mogelijk contact met besmette personen tijdelijk thuis moeten blijven.[10] De werkplek zelf is uiteraard ook een potentiële bron van besmetting, waardoor deze mogelijk anders moet worden ingericht, zoals tijdens de recente Covid-19 pandemie. Deze pandemie demonstreerde tegelijkertijd ook het effect van een dergelijk wereldwijde, ingrijpende gebeurtenis op wereldwijde aanvoerketens. Een tekort aan grondstoffen, technische materialen, persoonlijke beschermingsmiddelen en andere verbruiksgoederen met gevolgen voor de bedrijfscontinuïteit. Deze tekorten kunnen er bijvoorbeeld voor zorgen dat de vervanging van verouderde installatieonderdelen wordt uitgesteld, met het risico dat deze worden gebruikt tot dat zij falen. Ook kan voorkomen dat er voor medewerkers geen geschikte of alleen verouderde beschermingsmiddelen beschikbaar zijn voor het omgaan met gevaarlijke stoffen. Daardoor kunnen de gevolgen van infectieziekten ook invloed hebben op de waarschijnlijkheid van een zwaar ongeval.

[8] Bij de dreigingen sabotage en spionage staat ook het digitale component toegevoegd om te benadrukken dat moedwillige digitale dreigingen ook onder hybride conflictvoering kunnen vallen indien hier een statelijke actor direct of indirect voor verantwoordelijk is.
[9] Deze dreiging komt niet expliciet naar voren in de geraadpleegde risicoanalyses. Echter, gezien de toenemende relevantie van deze dreiging (zie o.a. ANV, 2024) is deze wel toegevoegd aan de lijst.
[10] In de scenario's grieppandemie en pandemie door een mens overdraagbaar respiratoir virus in de RbRa 2022 worden personeelstekorten in onder andere vitale sectoren en de gevolgen daarvan aangemerkt als onderdeel van een dergelijke gebeurtenis (ANV, 2022b). Het scenario infectieziekten (hieronder) is hier ook op gebaseerd.

Onder de categorie infectieziekten vallen ook de steeds meer aanwezige exotische dieren- of insectensoorten in Nederland die ziektes op mensen kunnen overdragen. Denk hierbij aan malariamuggen en aan de tijgermug (die o.a. knokkelkoorts en gele koorts kan veroorzaken). Verder valt onder deze categorie ook de gevolgen door de aanwezigheid van medewerkers die in het buitenland een overdraagbare infectieziekte op hebben gelopen. Hierbij kan worden gedacht aan ziekten als Ebola. Voor deze twee typen geldt dat alhoewel ze in theorie kunnen leiden tot de uitval van medewerkers, en daardoor druk zetten op de continuïteit van bedrijfsprocessen, ze (veel) kleinschaliger van aard zullen zijn dan een epidemie of pandemie. Het gaat hier in de praktijk dus eerder om maatregelen op de werkplek gericht op het tegengaan van besmetting dan om continuïteitsproblemen als gevolg een beperktere beschikbaarheid van materialen.

Scenario: infectieziekte
Er breekt een pandemie uit van een nieuw mens-overdraagbaar respiratoir virus. Alhoewel de symptomen voor veel mensen relatief mild zijn, duurt het vaak relatief lang voordat mensen weer volledig hersteld zijn. Als gevolg hebben bedrijven moeite om voldoende gekwalificeerd technisch personeel op de werkvloer te hebben. Te meer doordat hier ook voor de pandemie al een tekort aan was. Wanneer er tijdens het leegpompen van een opslagtank een probleem voordoet, is er te weinig personeel aanwezig om op tijd in te grijpen. Er is sprake van een uitstroom van waterstofsulfide, dat een acute vergiftiging veroorzaakt bij de aanwezige medewerkers.

Categorie 2: natuurrampen
Deze categorie bevat verschillende weersextremen en natuurlijke fenomenen. Als gevolg van extreme hitte kan bijvoorbeeld de gezondheid en de alertheid (op o.a. gevaren) van medewerkers in het geding komen. Te meer als zij tijdens hun werk gebruik moeten maken van beschermende kleding (RIVM, 2021). (Sneeuw)storm en windhozen, extreme neerslag in de vorm van regen of hagel, overstromingen en (oprukkende) natuurbranden kunnen leiden tot schade aan kantoren en productie-of opslaglocaties met gevaarlijke stoffen. Ruimtes kunnen onderlopen, stroomvoorzieningen kunnen worden aangetast en (dak)constructies kunnen mogelijk bezwijken onder bijvoorbeeld extreme windstoten of sneeuwval. Al deze situaties kunnen in potentie de kans op een zwaar ongeval vergroten. Dit kan op meer directe wijze door het ontstaan van schade aan installaties als op meer indirecte wijze. Bijvoorbeeld doordat personeel zelf (samen met eventuele familieleden) als gevolg van gevaarlijke weersomstandigheden een gebied moet verlaten en daardoor fysiek niet aanwezig kan zijn op het bedrijf (RIVM, 2021).

Ook langere periodes van extreme droogte hebben in dit kader mogelijk gevolgen voor de bedrijfsprocessen. Droogte kan bijvoorbeeld invloed hebben op de beschikbaarheid van koel- en bluswater en kan (samen met perioden van extreme neerslag) leiden tot veranderingen in grondwaterpeil en daarmee ook mogelijk verzakking dan wel opstuwing van de bodem (NCTV, 2025b; RIVM, 2021). Tot slot zijn aardbevingen een dreiging om rekening mee te houden. Dit betreft aardbevingen van zowel natuurlijke als geïnduceerde aard (bijv. als gevolg van geothermie, mijnbouw of gaswinning), waarbij dit vooral in bepaalde regio's van Nederland een rol speelt (Groningen en Brabant). Aardbevingen worden, samen met andere natuurfenomenen, al expliciet genoemd als dreigingen waarmee Seveso-inrichtingen die grote hoeveelheden gevaarlijke stoffen opslaan (de zogenoemde hogedrempelinrichtingen, waar de hoogste wettelijke drempelwaarden worden overschreden) rekening moeten houden in hun veiligheidsrapport (IPLO, 2026).

Scenario natuurramp[11]
Als gevolg van uitzonderlijk veel regenval, treedt een grote rivier buiten de oevers. Resultaat is een groot gebied waar 10 tot 20 centimeter water staat. De bodem is verzadigd met water en bij een nabijgelegen bedrijf dat werkt met gevaarlijke stoffen, drijven meerdere, op lagere grond gelegen ondergrondse opslagtanks op. Door deze beweging, raken de koppelingen van de tanks beschadigd en komen er stoffen vrij in de omgeving. Doordat de stof lichter is dan water, verspreidt deze zich snel aan de oppervlakte.

Categorie 3: vitale infrastructuur
Verstoringen in de vitale infrastructuur kunnen grote gevolgen hebben voor de bedrijfsprocessen en daarmee ook impact hebben op het mogelijk ontstaan van een zwaar ongeval. Hoe zorgt een bedrijf er bijvoorbeeld voor dat processen veilig blijven verlopen bij de plotselinge uitval van elektriciteit, (koel)water of gas? Vooral wanneer deze uitval het gevolg is van een andere gebeurtenis zoals één van de eerdergenoemde natuurrampen. Het kan hier ook gaan om de uitval van spraak- en datacommunicatiediensten waardoor medewerkers op de werkvloer bijvoorbeeld niet meer goed met elkaar kunnen communiceren of hulpdiensten moeilijk bereikbaar zijn in het geval van een calamiteit. Voor vitale infrastructuur geldt verder dat de uitval van één proces kan leiden tot de uitval van één of meerdere andere processen. Vooral de uitval van elektriciteit kan leiden tot grote keteneffecten (NCTV, 2025b). Bij de uitval van vitale infrastructuur speelt het tijdscomponent ook een rol. Naarmate uitval langduriger is (bijvoorbeeld één of meerdere dagen), vraagt dit bijvoorbeeld meer van de capaciteit (en bevoorrading) van back-up systemen als noodgeneratoren.

Scenario vitale infrastructuur[12]
Een groot deel van Nederland krijgt te maken met een stroomstoring van 24 uur. Naast de levering van elektriciteit zelf, is er ook moeite om zonder stroom de druk op de gasleidingen op peil te houden. Te meer wegens de hoge vraag door winters weer. Als gevolg hiervan gaat bij een bedrijf in de regio de waakvlam uit die nodig is voor het eventueel affakkelen van stoffen. Wegens problemen in de installatie door een gebrek aan elektriciteit, is dit affakkelen echter wel noodzakelijk. De druk in de installatie neemt snel toe, met uiteindelijk een explosieve uitstroom tot gevolg.

Categorie 4: digitale veiligheid
Deze categorie betreft zowel moedwillige als niet-moedwillige gebeurtenissen die leiden tot het verstoren van de digitale processen. Onder moedwillige dreigingen vallen verschillende vormen van cyberaanvallen. Bijvoorbeeld *ransomware* aanvallen of cyberaanvallen specifiek gericht op het verstoren van industriële controlesystemen of operationele technologie. In dit laatste geval kunnen actoren bijvoorbeeld ongewenst de controle overnemen van systemen. Ook van systemen die van belang zijn voor de veiligheid. In het ergste geval kan hiermee doelbewust een zwaar ongeval worden veroorzaakt. De toenemende digitalisering van deze systemen zorgt voor een steeds grotere kwetsbaarheid en steeds meer mogelijke doelwitten voor cyberaanvallen (NCTV, 2025b).

[11] De aanloop van dit scenario is een minder ernstige variant van die in de RbRa 2022 (ANV, 2022c). Het opdrijven van ondergrondse opslagtanks is een punt van aandacht uit eerder onderzoek (RIVM, 2021).
[12] Dit scenario is een combinatie van verschillende inzichten. De omvang en duur van de stroomstoring zijn afkomstig uit het scenario landelijke black-out van het ANV (2022c). Het moeten affakkelen als gevolg van een stroomstoring is gebaseerd op de stroomstoring eind 2024 in de regio Rotterdam (RTV Rijnmond, 2024). De beschikbaarheid van gas tijdens een stroomstoring is ingebracht als aandachtspunt tijdens een eerder onderzoek (RIVM, 2021). De Nederlandse gasvoorziening kan niet functioneren zonde elektriciteit (NCTV, 2025b).

Aanvallen op bijvoorbeeld derde partijen die digitale diensten leveren aan bedrijven vallen ook onder deze moedwillige dreigingen. Bijvoorbeeld cloudopslag of aansturingssystemen. Wanneer belangrijke documentatie over bijvoorbeeld te volgen processen alleen digitaal in de cloud zijn opgeslagen, kan het niet toegankelijk zijn hiervan leiden tot veiligheidsproblemen. Er kan tot slot ook sprake zijn van niet-moedwillige gebeurtenissen rond cyberveiligheid. Zoals storingen in aansturingssystemen of bij de leveranciers dan wel beheerders van deze systemen als gevolg van menselijk handelen of een technische fout.

Scenario digitale veiligheid[13]
Een bedrijf dat werkt met gevaarlijke stoffen wordt slachtoffer van een geraffineerde, gerichte malware campagne. Met behulp van een LLM[14] worden personeelsleden benaderd met een zeer overtuigende mail die afkomstig lijkt te zijn van personeelszaken. Meerdere medewerkers klikken op een malafide link, waardoor de groep achter de campagne via malware toegang krijgt tot de systemen van het bedrijf. Andere gebruikers worden buitengesloten en de groep gebruikt hun nu ongehinderde toegang om grote hoeveelheden gevaarlijke stof weg te laten lekken uit een opslagtank.

Categorie 5: geweld
Deze categorie betreft veel verschillende soorten gebeurtenissen, waarvoor zowel statelijke, criminele als extremistische actoren verantwoordelijk kunnen zijn. Vanuit het oogpunt van een mogelijk zwaar ongeval gaat het hier primair om verschillende vormen van fysieke sabotagehandelingen of (terroristische) aanslagen zoals het plaatsen van explosieven of brandstichting gericht op installaties.[15] Het sturen van poederbrieven, al dan niet met 'echt' schadelijk materiaal, kan hier ook onder vallen. Onder de categorie geweld vallen verder ook manifestaties[16] die mogelijk bedrijfsprocessen kunnen verstoren (pogingen tot binnendringen, blokkades, etc.), bijvoorbeeld doordat personeel of grondstoffen moeilijk op locatie kunnen komen.

Alhoewel de link met het ontstaan van een zwaar ongeval wat indirecter is, omvat deze categorie ook de (dreiging van) geweld richting medewerkers. Hierbij kan sprake zijn van (doods)bedreigingen, mishandeling of, in het meest extreme geval, een gerichte liquidatie(poging). Recent voorbeeld hiervan is de voorgenomen liquidatie door Rusland van een topman van een Duitse wapenfabrikant (NCTV, 2025b). Dit type situatie kan leiden tot de uitval (vanwege angst of vanwege letsel) van voor het veilig verloop van bedrijfsprocessen belangrijk personeel.

Tot slot omvat deze categorie het ongewenst invloed uitoefenen over bedrijven en medewerkers. Het gaat hier oftewel om niet-gewelddadige dreigingen gericht op het verkrijgen van informatie of het manipuleren van handelingen. Concrete dreigingen die hier onder vallen zijn chantage, inmenging en infiltratie. Hierbij kunnen wel de omstandigheden worden geschept waarbij de kans op een zwaar ongeval toeneemt.

[13] Dit scenario is qua gebeurtenissen gebaseerd op het scenario *cyberaanval ICS - chemische sector* uit de RbRa 2022 (ANV, 2022d) en op ontwikkelingen rondom het gebruik van *large language models* bij phishing uit het CSBN (NCTV, 2025a).
[14] LLM staat voor *large language model*. Dit is een vorm van kunstmatige intelligentie die onder meer in staat is om tekst te verwerken en te genereren.
[15] Digitale sabotage valt al onder de categorie cyberveiligheid.
[16] Bij manifestaties zoals het blokkeren van een bedrijventerrein kan ook sprake zijn van activisme (i.p.v. extremisme). Zo hebben activisten in de zomer van 2024 de Botlekbrug geblokkeerd, een belangrijke transportroute van- en naar de Maasvlakte (NCTV, 2025b).

Scenario geweld[17]
Twee personen werken zich door het hek heen van een bedrijf dat gevaarlijke stoffen opslaat. Eenmaal op het omvangrijke terrein doen zij zich voor als extern onderhoudspersoneel en kunnen ze zich ongestoord bewegen. De mannen plaatsen een brandbom bij één van de opslagtanks van het bedrijf. Nadat ze het terrein weer hebben verlaten, wordt het explosief tot ontsteking gebracht.

Categorie 6: geopolitiek
Onder deze categorie valt onder meer het uitbreken van een internationaal gewapend conflict. Alhoewel het uiteraard denkbaar is dat sommige bedrijven in Nederland zelf doelwit zullen worden van militair handelen in een dergelijke situatie, zal het hier primair ook gaan om zogenoemde hybride dreigingen. Er is hier dus nog geen sprake van rechtstreeks, openlijk militair handelen (NCTV, 2025b). Bijvoorbeeld sabotage. Deze en andere dreigingen staan grotendeels al in één van de andere categorieën.

Een geopolitieke dreiging die nog niet is meegenomen in andere categorieën betreft verstoringen in internationale handelsstromen en daarmee de vrije beschikbaarheid van (grond)stoffen die van belang zijn voor het veilige verloop van bedrijfsprocessen. Een verstoring van deze stromen kan ontstaan door technisch falen (buiten de scope van deze categorie) en door politiek handelen in de vorm van sancties, heffingen, exportbeperkingen en andere maatregelen. Door verstoring van de handelsstromen kan de productie van een bedrijf tijdelijk stopgezet moeten worden (World Economic Forum, 2026). Het stoppen en opstarten zijn de meest kritieke momenten van een chemisch bedrijf (Müller, 2015). Ook kan het zijn dat de productie wel doorgaat maar sterk verminderd wordt waardoor de procescondities af zullen wijken van normaal. In extreme gevallen zal een bedrijf sluiten met als gevolg dat het bedrijf leeggehaald moet worden en gereinigd wat beide gevaarlijke klussen zijn vanwege de niet-routinematige werkzaamheden.

Scenario geopolitiek[18]
De spanningen tussen en landen en machtsblokken op het wereldtoneel lopen hoog op. Een land dat een belangrijke leverancier is van technische onderdelen voor de chemische industrie, legt de EU en daarmee ook Nederland exportbeperkingen op. Er is grote moeite om binnen afzienbare tijd vervangende leveranciers te vinden. Naarmate de situatie voortduurt, is er een toenemend gebrek aan reserveonderdelen. De bedrijfsprocessen blijven doordraaien omdat de chemische industrie al economisch tegenwind ervaart. Bij een bedrijf breekt een rubberdichting die weken geleden vervangen had moet worden. Een stroom van toxische gassen ontsnapt.

[17] De kerngebeurtenis (brandstichting) is gebaseerd op een soortgelijk incident bij een Duitse wapenfabriek. Het vermoeden is dat de Russische overheid achter dit voorval zit (Nöstlinger & Klöckner, 2024).
[18] Gebaseerd op trend van toenemende competitie en conflict tussen machtsblokken op het wereldtoneel ten koste van samenwerking (Instituut Clingendael, 2026a; 2026b).

8. Reflectie en conclusie

Binnen dit onderzoek zijn op basis van vier selectiecriteria uiteindelijk zes categorieën van dreigingen geïdentificeerd waarvan uitingen kunnen leiden tot een zwaar ongeval bij bedrijven met gevolgen voor de arbeidsveiligheid. Dit zijn: infectieziekten, natuurrampen, vitale infrastructuur, digitale veiligheid, geweld en geopolitiek.

Alhoewel de bovenstaande categorieën in deze notitie afzonderlijk worden gepresenteerd, is het belangrijk om bewust te zijn van de onderlinge afhankelijkheid van sommige categorieën in de praktijk. Dit geldt vooral voor de categorie vitale infrastructuur. Deze categorie vertegenwoordigt bijvoorbeeld dreigingen die zowel het beginpunt kunnen zijn van een keten van gebeurtenissen (als gevolg van bijvoorbeeld technisch falen) als juist een gevolg van een andere dreiging zoals een natuurramp, een infectieziektenuitbraak of kwaadwillend handelen (sabotage). Anders gezegd, zijn er meerdere routes die maken dat bedrijven te maken kunnen krijgen met de uitval van vitale infrastructuur.

Ondanks de vier gehanteerde selectiecriteria, is er nog steeds een groot aantal relevante individuele dreigingen dat valt onder deze zes categorieën. Voor elk van de genoemde dreigingen geldt bovendien dat er veel verschillende specifieke uitingsvormen denkbaar zijn wanneer deze meer concreet worden gemaakt door middel van bijvoorbeeld een scenario. Naarmate er een lager abstractieniveau is, nemen de opties logischerwijs toe. Het gevaar bestaat hier om te verzanden in een woud van mogelijkheden en voorbij te gaan aan beschikbare capaciteit voor de analyse hiervan.

Het is daarom aan te raden om bij vervolgonderzoek naar weerbaarheid een abstractieniveau hoger te beginnen, op het niveau van de zes categorieën. Nadat er inzicht is verkregen in de huidige mate van weerbaarheid kan er vanuit dit niveau vervolgens per categorie worden bepaald welke aanpassingen invloed kunnen hebben op het mitigeren van de gevolgen van de dreigingen. Denk hierbij bijvoorbeeld aan het inrichten van de werkplek, aanvullende (risico)communicatie of het beïnvloeden van gedrag. Deze aanpassingen kunnen worden ingedeeld aan de hand van de vier eerdergenoemde fasen van weerbaarheid (plannen, absorberen, herstellen en aanpassen). Voor de categorie infectieziekten kan bijvoorbeeld in de planningsfase worden geïnventariseerd of er voldoende opgeleid personeel beschikbaar is om taken over te nemen als er sprake is van veel uitval. Voor natuurrampen is in diezelfde fase een mogelijke eigenschap dan weer de vraag of de ligging van installatie-onderdelen, technische ruimtes en opslagtanks tot problemen kan leiden. Bij digitale veiligheid kan het in de absorptiefase dan weer gaan om de vraag of, als de controle over een digitaal systeem wordt verloren, er nog een fysiek alternatief bestaat. Tot slot, voor de categorie geweld komen in de planfase weer andere elementen van de inrichting van de installatie aan de orde: zijn er bijvoorbeeld barrières (hekwerk; paslezers) die voorkomen dat onbevoegden toegang krijgen tot bepaalde installatie onderdelen?

Referenties

Analistennetwerk Nationale Veiligheid (2022). Hoofdrapport *Rijksbrede Risicoanalyse Nationale Veiligheid 2022*. Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Analistennetwerk Nationale Veiligheid (2022b). *Rijksbrede Risicoanalyse Nationale Veiligheid: Themarapportage Infectieziekten*. Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Analistennetwerk Nationale Veiligheid (2022c). *Rijksbrede Risicoanalyse Nationale Veiligheid: Themarapportage Bedreiging Vitale Infrastructuur*. Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Analistennetwerk Nationale Veiligheid (2022d). *Rijksbrede Risicoanalyse Nationale Veiligheid: Themarapportage Cyberdreigingen*. Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Analistennetwerk Nationale Veiligheid (2024). *Trendanalyse Nationale veiligheid – Verdieping op de Trendanalyse*. Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Analistennetwerk Nationale Veiligheid (2024). *Trendanalyse Nationale veiligheid – Hoofdrapport: Stapeling van dreigingen in tijden van onzekerheid.* Via: https://www.rivm.nl/nationale-veiligheid/publicatie-overzicht-anv.

Baumann, M & Pynnöniemi, K. (2025). *European Security in the Era of Hybrid Warfare*. DGAP Policy Brief 20 (2025). German Council on Foreign Relations. November 2025. Via: https://doi.org/10.60823/DGAP-25-42888-en.

Ganin, A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J., Kott, A., Mangoubi, R. & Linkov, I. (2016). Operational resilience: concepts, design and analysis. *Scientific Reports, 6*(19540, 1-12. DOI: 10.1038/srep19540.

Informatiepunt Leefomgveing (2026). *Veiligheidsrapport opstellen voor Seveso-inrichtingen*. Geraadpleegd op 23-01-2026. Via: https://iplo.nl/regelgeving/regels-voor-activiteiten/seveso-inrichting/regels-veiligheid/veiligheidsrapport-opstellen-seveso-inrichtingen/.

Instituut Clingendael. (2026a). *Strategische Monitor 2025-2030: Geopolitiek changement op het wereldtoneel*. Via: https://www.clingendael.org/publication/strategische-monitor-2025-2030-geopolitiek-changement-op-het-wereldtoneel.

Instituut Clingendael. (2026b). *Europe's Selective Blindness on Gas: US LNG and the Limits of Supply Diversification*. Via: https://www.clingendael.org/publication/europes-selective-blindness-gas.

Koninklijk Nederlands Meteorologisch Instituut. (2023*). KNMI'23: Klimaatscenario's voor Nederland*. Via: https://www.knmi.nl/kennis-en-datacentrum/achtergrond/knmi-23-klimaatscenario-s/

Müller, G (2015). *Managing risk during turnarounds and large capital projects: Experience from the chemical industry*. Journal of Business Chemistry, 12 (3), 117-124.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025a). *Cybersecuritybeeld Nederland 2025*. Via: https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025b). *Dreigingslandschap Vitale Infrastructuur*. Via: https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur.

Nederlandse Arbeidsinspectie. (2026) *Taken* Geraadpleegd op 23-01-2026. Via: https://www.nlarbeidsinspectie.nl/nederlandse-arbeidsinspectie/taken.

Nederlands Instituut Publieke Veiligheid. (2024). *Werken aan weerbaarheid en veerkracht.* Via: https://nipv.nl/wp-content/uploads/2024/12/20241204-NIPV-Werken-aan-weerbaarheid-en-veerkracht.pdf.

Nöstlinger, N. & Klöckner, J. (24 juni 2024). Russia started Berlin factory fire as part of hybrid war on Europe, report says. *Politico*. Via: https://www.politico.eu/article/russia-berlin-fire-diehl-behind-arson-attack-on-factory/.

RAND Europe. (2024). *Weerbaarheid becijferd: Een methode om weerbaarheid tegen dreigingen voor de nationale veiligheid inzichtelijk te maken*. Via: https://www.rand.org/pubs/research_reports/RRA2357-1.html/

Rijksinstituut voor Volksgezondheid en Milieu & TNO. (2023). *De Toekomst van Gezond en Veilig Werken: Een brede horizonscan*. Via: DOI 10.21945/RIVM-2022-0197.

Rijksinstituut voor Volksgezondheid en Milieu. (2021). *Voorbereiding van Brzo bedrijven op klimaatverandering*. DOI: 10.21945/RIVM-2021-0050.

Rijksinstituut voor Volksgezondheid en Milieu. (2024). *Indicatoren voor veilige arbeid*. DOI: 10.21945/RIVM-2023-0418.

RTV Rijnsmond. (3 september 2024). *Affakkelen door de stroomstoring, waarom is dat nodig?* Geraadpleegd op 26-01-2026. Via: https://www.rijnmond.nl/nieuws/1885763/affakkelen-door-de-stroomstoring-waarom-is-dat-nodig.

Veiligheidsregio Amsterdam-Amstelland. (2025). *Risicoprofiel 2025-2028*. Via: https://stukken.veiligheidsregioaa.nl/risicoprofiel-2025-2028/.

Veiligheidsregio Rotterdam-Rijnmond. (2022). *Regionaal Risicoprofiel 2022-2025*. Via: https://vr-rr.nl/over/rc/crisisbeheersing/regionaal/.

Veiligheidsregio Limburg-Noord & Veiligheidsregio Zuid-Limburg. (2023). *Provinciaal Risicoprofiel Veiligheidsregio's Limburg-Noord en Zuid-Limburg*. Via: https://www.vrln.nl/sites/vrln/files/2024-04/Veiligheidsregio_LN-ZL_Provinciaal_risicoprofiel.pdf.

Veiligheidsregio Midden- en West-Brabant. (2023). *Regionaal Risicoprofiel 2023-2027*. Via: https://www.vrmwb.nl/media/qnmkutwa/regionaal-risicoprofiel-2023_2027.pdf.

Veiligheidsregio Zeeland. (2020). *Regionaal Risicoprofiel Zeeland 2020-2023*. Via: https://www.zeelandveilig.nl/sites/zeelandveilig/files/2020-10/risicoprofiel%202020-2023%20versie%202.0%20datum%2002-02-2020.pdf

World Economic Forum (2026). The Global Risks Report 2026, 21st Edition. Via: https://www.weforum.org/publications/global-risks-report-2026/