APPENDIX A – HET DREIGINGSBEELD

Zoals beschreven in het hoofdrapport kent het Nederlandse dreigingsbeeld zowel een grote variëteit als omvang. Ter illustratie volgt hieronder een beknopt – en zeker niet uitputtend – overzicht dat de breedte van het nationale dreigingsbeeld schetst.

Sociaal & maatschappelijk	
Polarisatie rond complottheorieën	Groeiende verdeeldheid door samenzweringstheorieën die het onderlinge en institutionele vertrouwen ondermijnen en conflicten aanwakkeren in de samenleving en de politiek.
Anti-overheidsextremisme	Acties of overtuigingen van individuen of groepen die, uit extreem wantrouwen en ideologie, het gezag van de overheid actief verwerpen.
Meervoudige terroristische aanslag	Gelijktijdige of opeenvolgende aanvallen door terroristen gericht op meerdere locaties, bedoeld om angst en massale schade te veroorzaken.
Radicalisering van individuen	Proces waarbij personen extreme overtuigingen aannemen en mogelijk gewelddadig worden, beïnvloed door ideologie of frustraties.
Rechts-extremisme	Ideologie die racistische, nationalistische en xenofobe overtuigingen verspreidt, vaak leidend tot discriminatie en geweld tegen minderheden.
Groeiende ongelijkheid	Toenemende verschillen in de verdeling van vermogen en inkomen, binnen en tussen landen, leiden tot armoede, onvrede en ondermijnen de sociale en politieke stabiliteit.
Gewapend conflict binnen staten	Interne gewelddadige confrontaties, zoals burgeroorlogen, die stabiliteit aantasten en humanitaire crises veroorzaken.
Economisch	
Verstoringen in productieketens	Onderbrekingen in leveringen en productieprocessen door logistieke problemen, conflicten of natuurrampen, waardoor economische schade ontstaat.
Economische sancties en handelsbeperkingen	Maatregelen zoals import- en exportverboden, bedoeld om politieke doelen te bereiken, maar leidend tot economische problemen.
Risicovolle strategische afhankelijkheden grondstoffen en technologie	Een te grote afhankelijkheid van enkele landen of leveranciers voor essentiële grondstoffen en technologie vergroot strategische kwetsbaarheid en economische risico's.
Concurrentie om schaarse middelen	Competitie tussen landen of bedrijven om beperkte grondstoffen, zoals water of mineralen, leidend tot conflicten en economische spanningen.
Inflatie	Algemene stijging van prijzen, waardoor koopkracht daalt en economische onzekerheid ontstaat voor huishoudens en bedrijven.
Stijgende energie- en gasprijzen	Toenemende kosten voor energie, waardoor economische groei wordt beperkt, productie duurder wordt en koopkracht afneemt.
Recessie	Periode van economische krimp, met verlies van banen, dalende inkomens en verhoogde onzekerheid voor bedrijven en consumenten.
Arbeidstekorten	Gebrek aan voldoende gekwalificeerd personeel, waardoor economische groei, productiviteit en innovatie beperkt worden.

Ecologisch	
Hitte en droogte (extreem weer)	Langdurige hittegolven en droogte bedreigen landbouw, gezondheid, infrastructuur en verhogen de kans op bosbranden en verlies van biodiversiteit.
Verlies van biodiversiteit	Het verlies van biodiversiteit verstoort ecosystemen, schaadt milieu en natuur, en bedreigt voedselzekerheid door afnemende landbouwproductiviteit, mede veroorzaakt door het uitsterven van soorten op land en in zee.
Tekort aan drinkwater door verzilting en vervuiling	Tekorten aan water voor gebruik door mensen, industrieën of ecosystemen, veroorzaakt door verdroging, verzilting en vervuiling van water (versterkt door klimaatverandering).
Overstroming vanuit de zee of een rivier	Stijgende zeespiegel en extreme neerslag verhogen de kans op grote overstromingen, met verwoestende gevolgen voor steden, dorpen en infrastructuur.
Overschrijden kritieke kantelpunten	Langdurige, mogelijk onomkeerbare en zichzelf versterkende veranderingen in belangrijke systemen van de planeet door het overschrijden van kritieke klimaat- of ecologische grenzen ('kantelpunten').
Vervuiling (lucht, bodem, water)	Vervuiling door schadelijke stoffen die via huishoudelijke en industriele activiteiten, milieu gerelateerde ongelukken zoals olielekkages in lucht, water en bodem terechtkomen.
(Overige) natuurrampen	Verlies van mensenlevens, schade aan ecosystemen, vernietiging van eigendommen en/of financiële schade veroorzaakt door niet-weersgerelateerde natuurverschijnselen zoals (geïnduceerde) aardbevingen en opzettelijk aangestoken bosbranden
Geopolitiek & militair	
Innovatie nucleaire overbrengingsmiddelen	De ontwikkeling van geavanceerdere systemen voor kernwapens vergroot het risico op nucleaire confrontatie.
Geo-economische confrontatie	Economische conflicten waarbij landen handelsmaatregelen en economische druk gebruiken om geopolitieke invloed te vergroten.
Heimelijke beïnvloeding en hybride operaties	Strategieën waarbij staten of actoren op verborgen wijze maatschappelijke processen verstoren via bijvoorbeeld desinformatie, cyberaanvallen, economische druk of een combinatie daarvan.
Uiteenvallen van de NAVO	Mogelijke fragmentatie van de NAVO door interne verdeeldheid, leidend tot verminderde collectieve veiligheid en verhoogde kwetsbaarheid
Tijdelijke bezetting van een EU-lidstaat	Militaire bezetting van EU-grondgebied, waardoor Europese stabiliteit en veiligheid ernstig worden bedreigd
Klassieke statelijke spionage	Het heimelijk verzamelen van informatie door een staat om politieke, militaire of economische voordelen te behalen.
Strategische rivaliteit grootmachten	Toenemende spanningen en concurrentie tussen grootmachten, wat kan leiden tot conflicten en internationale instabiliteit.
Militair conflict tussen staten	Gewapende conflicten tussen landen, leidend tot verwoesting, mensenrechtenschendingen en vluchtelingenstromen.

Technologisch & digitaal	
Cyberaanvallen	Digitale aanvallen gericht op computersystemen om gegevens te stelen, systemen uit te schakelen of infrastructuur te verstoren.
Cyberspionage	Digitale spionage om gevoelige informatie te verkrijgen, vaak via heimelijke toegang tot netwerken en databases.
Mis- en desinformatie	(Bewust) verspreiden van onjuiste of misleidende informatie om publieke opinie, besluitvorming of stabiliteit te beïnvloeden.
AI aanvallen op autonome systemen	Gebruik van kunstmatige intelligentie om autonome systemen zoals drones of voertuigen te misleiden, verstoren of manipuleren.
Gebruik van generatieve AI voor deepfakes en desinformatie	Gebruik van AI-technologie om realistische nepbeelden, -audio of -video te creëren en verspreiden, bedoeld om mensen te misleiden.
Kwantumencryptie	Encryptiemethoden die kwetsbaar kunnen worden door kwantumcomputers, waardoor gevoelige informatie makkelijker kan worden onderschept of ontcijferd.
Ontwikkelingen in de ruimte	Nieuwe activiteiten in de ruimte zoals wapensystemen of doelgerichte verstoringen van satellieten die potentiële bedreigingen vormen voor wereldwijde veiligheid en communicatie.
Gezondheid	
Pandemie door een via de mens overdraagbaar virus	Nieuwe virussen kunnen zich wereldwijd verspreiden via mens-op-mensbesmetting, met ingrijpende gevolgen voor gezondheid, economie en maatschappij.
Epidemie	Lokale of regionale uitbraken van infectieziekten die druk op zorgsystemen en maatschappelijke ontregeling veroorzaken.
Antibioticaresistentie	Bacteriën worden ongevoelig voor antibiotica, waardoor infecties moeilijk behandelbaar zijn en sterfte en ziekenhuisopnames toenemen.
Gezondheidsrisico's klimaatverandering	De groeiende incidentie van klimaatgerelateerde ziekten, zoals hitteberoerte en infecties die via bijvoorbeeld muggen worden overgedragen, doordat warmere temperaturen hun verspreiding en voortplanting bevorderen.
Chemische, biologische, radiologische bedreigingen	Opzettelijke of accidentele blootstelling aan gevaarlijke stoffen kan acute en langdurige gezondheidsschade veroorzaken in grote populaties.
Toename in chronische ziekten	Toename van aandoeningen zoals diabetes, hart- en vaatziekten en kanker door leefstijl en vergrijzing van de bevolking.

APPENDIX B – METHODOLOGIE KNOOPPUNTENANALYSE

Het netwerk van dreigingen dat in dit rapport wordt gepresenteerd, is tot stand gekomen via een knooppuntenanalyse die in samenwerking met Kickstart AI is ontwikkeld. Deze appendix beschrijft de opzet van de analyse, de gebruikte aannames en de methodologische keuzes. Het volledige model is te vinden op https://denkwerk-kickstartai.nl/knooppuntenanalyse

De analyse maakt gebruik van het principe van 'out-degree eigenvectorcentraliteit'.[a] [1] Die meet hoeveel uitgaande verbindingen een dreiging heeft richting andere dreigingen die ook veel uitgaande verbindingen hebben, en meet daarnaast de invloed van een dreiging in het netwerk waartoe het behoort (het houdt dus rekening met de impact). Met de analyse brengen we de causale relaties tussen nationale dreigingen in kaart, en identificeren we de meest invloedrijke knooppunten. De aanpak omvat vijf stappen, die in de volgende paragrafen verder worden toegelicht.

1. **Verzameling en filtering van data -** Uit een breed palet aan publieke bronnen is een groot aantal documenten verzameld waarin actuele dreigingen aan bod komen. De verzamelde documenten zijn door ons met hulp van AI gefilterd op relevantie en actualiteit.
2. **Afbakening van nationale dreigingen -** Voor de analyse is een lijst van 71 nationale dreigingen vastgesteld, gebaseerd op bestaande risicoanalyses. De lijst is aangepast voor tekstuele verwerking: termen zijn aangescherpt en overlappende dreigingen zijn samengevoegd of verduidelijkt.
3. **Extractie van causale verbanden met taalmodellen -** Met behulp van Large Language Models (LLMs) zijn in de documenten semantisch causale relaties geïdentificeerd: situaties waarin de ene dreiging leidt tot een andere. Deze stap maakt de samenhang tussen dreigingen zichtbaar die in traditionele risicoanalyses vaak onderbelicht blijft.
4. **Constructie van het dreigingsnetwerk -** De geïdentificeerde verbanden zijn gebruikt om een netwerk te bouwen waarin dreigingen verbonden zijn via oorzakelijke relaties.
5. **Analyse van knooppunten binnen het netwerk -** Op het netwerk is een knooppuntenanalyse uitgevoerd, gericht op het berekenen van de out-degree eigenvectorcentraliteit van elke dreiging (de knooppuntwaarde). Hiermee zijn knooppunten in kaart gebracht: dreigingen die het meest verweven zijn met andere, en daarmee het grootste systeemrisico of aangrijpingspunt voor interventie vormen.

Stap 1 - verzameling en filtering van data

Dataverzameling

De basis voor deze analyse is een samengestelde dataset, opgebouwd uit publiek beschikbare bronnen. Tabel 1 geeft een overzicht van de herkomst van deze data, inclusief het aantal geëxtraheerde documenten per bron. Het overgrote deel van de documenten is automatisch verzameld via data scraping.[b] Deze bronnen zijn geselecteerd vanwege hun herkomst uit gezaghebbende Nederlandse instituten die gedegen onderzoek verrichten, met een duidelijke focus op beleidsondersteuning en maatschappelijke relevantie. Gezamenlijk bieden ze een breed spectrum aan relevante onderwerpen, zoals economie (CPB), technologie en innovatie (TNO), sociaal-maatschappelijke ontwikkelingen (SCP, SER), klimaat en milieu (PBL, KNMI, IPCC) en internationale betrekkingen en veiligheid (Clingendael, HCSS, NAVO). Daarnaast zijn enkele internationale bronnen handmatig toegevoegd om de analyse aan te vullen met belangrijke

a Theoretisch gezien kan eigenvectorcentraliteit in gerichte netwerken een score van nul toekennen aan invloedrijke eerste knooppunten in de keten, als hun invloed 'weglekt' in de langetermijn-berekening en niet terugkeert. Hier is dit echter geen praktische zorg gezien de analyse beperkt blijft tot twee stappen; de invloed van een invloedrijke dreiging wordt meegewogen nog voordat de problematische nulscores kunnen ontstaan.

b Voor het geautomatiseerd verzamelen van gegevens (data scraping) is gebruikgemaakt van gangbare Python-bibliotheken, waaronder requests en BeautifulSoup, en playwright (voor dynamisch geladen content). Deze toolset maakte het mogelijk om op schaal actuele en relevante documenten te verzamelen, met behoud van structuur en inhoudelijke volledigheid.

internationale perspectieven op het Nederlandse risicolandschap. Hieronder vallen het Jaarverslag 2024 van de Secretaris-Generaal van de NAVO en het hoofdstuk over Europa uit het Sixth Assessment Report van het IPCC.

Tabel 1. Bron	Aantal documenten	Webadres
open overheid	81555	https://open.overheid.nl/zoekresultaten
tno	9383	https://repository.tno.nl/lang/nl-NL
pbl	5502	https://www.pbl.nl/publicaties
clingendael	4290	https://www.clingendael.org/publications
ser	2553	https://www.ser.nl/nl/publicaties
cpb	961	https://www.cpb.nl/publicaties
hcss	704	https://hcss.nl/research/
wrr	558	https://www.wrr.nl/publicaties
scp	486	https://www.scp.nl/publicaties
knmi	330	https://www.knmi.nl
oecd	48	https://www.oecd.org/en/publications
ipcc	1	N.v.t. (handmatige selectie)
navo	1	N.v.t. (handmatige selectie)

De dataverzameling verliep vervolgens in twee fasen. Eerst is van elke bron een overzicht geëxtraheerd van beschikbare documenten, inclusief bijbehorende metadata zoals titel, beschrijving, publicatiedatum, documenttype en downloadlink. In de tweede fase zijn de corresponderende PDF-documenten gedownload en opgeslagen.

Voor de meeste bronnen zijn initieel alle rapporten opgehaald. Omdat de site Open Overheid documenten van veel verschillende overheidsorganisaties bundelt, was een gerichte zoekstrategie nodig om alleen de relevante stukken te behouden. Daarom is specifiek gezocht op de termen "dreiging" en "kwetsbaarheid", zodat alleen documenten over nationale risico's werden meegenomen.

Filtering van documenten

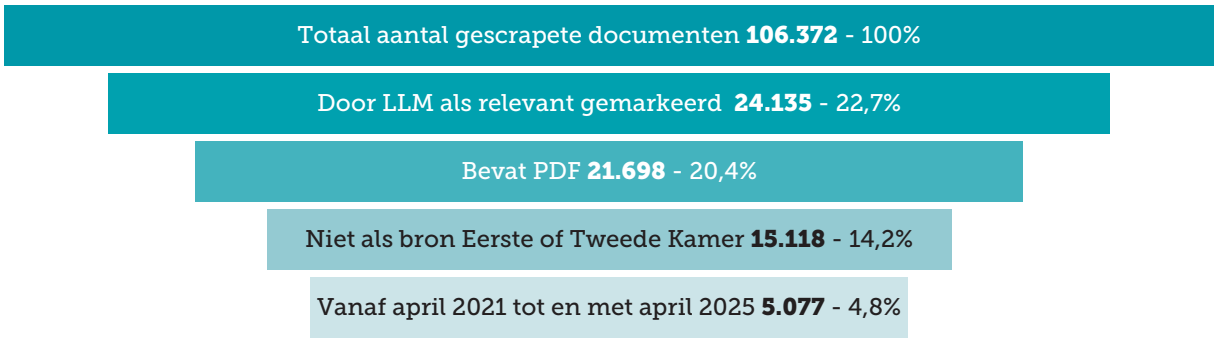
Na het extraheren van de documenten bleef een set van 106.000 documenten over. Om deze terug te brengen tot een selectie met relevante informatie over nationale dreigingen, is een meerstaps filterproces toegepast (zie Figuur B1).

De eerste stap was een automatische selectie met een licht taalmodel (GPT-4o mini), dat elk document beoordeelde op inhoudelijke relevantie. Deze aanpak bood meer precisie dan een eenvoudige zoektermfilter, die ook veel te specifieke of niet-relevante documenten zou meenemen. Na deze stap bleef een gerichte selectie van 24.000 documenten over.

Door ontbrekende of niet-werkende PDF-links bleef uiteindelijk een bruikbare dataset van 22.000 documenten over. In de daaropvolgende stap zijn documenten van de Eerste en Tweede Kamer – zoals Kamervragen en moties – verwijderd, om de politieke component van de analyse te beperken. Beleidsstukken van ministeries zijn wel behouden gebleven. Hierdoor bestaat de dataset voor ongeveer 80% uit documenten van ministeries en voor 20% uit publicaties van onderzoeksinstituten (zie Figuren B2 en B3).

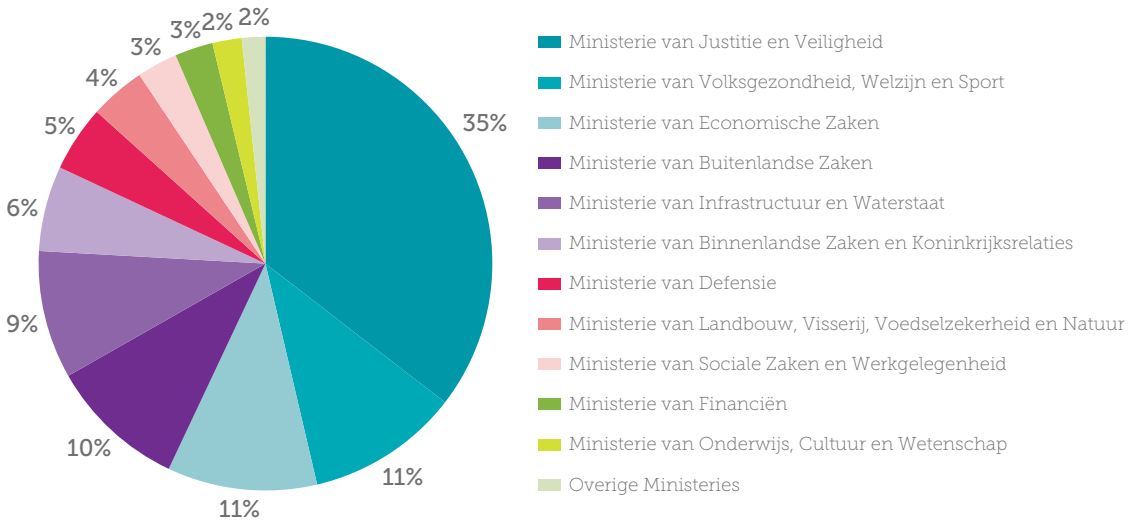
Als laatste stap zijn de documenten gesorteerd op publicatiedatum, waarna een actualiteitsfilter is toegepast: alleen publicaties van de afgelopen vier jaar (vanaf april 2021 tot april 2025) zijn meegenomen. Dit resulteerde in een finale dataset van 5.077 documenten, verspreid over verschillende ministeries en onderzoeksinstituten (zie Figuur B2 en B3).

Figuur B1 Schematische weergave filterproces



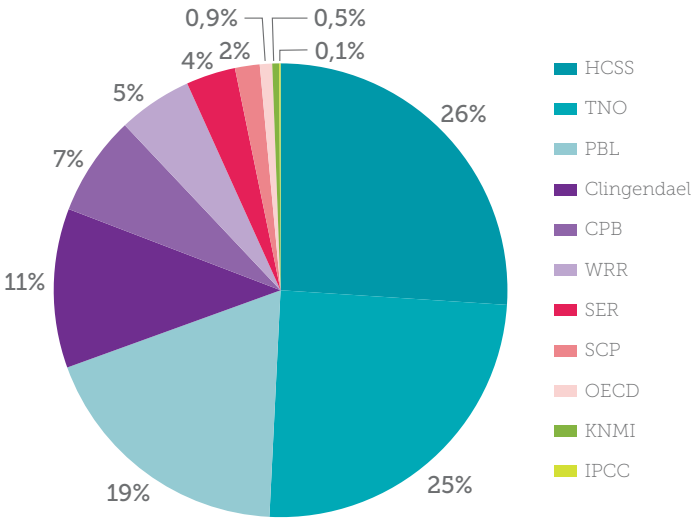
Bron: DenkWerk en Kickstart AI (2025)

Figuur B2 Verdeling ministeries na filtering (80% van de data)



Bron: DenkWerk en Kickstart AI (2025)

Figuur B3 Opmaak onderzoeksinstituten na filtering (20% van de data)



Bron: DenkWerk en Kickstart AI (2025)

Stap 2 - afbakening van nationale dreigingen

Voor de analyse is gekozen voor een afgebakende lijst van nationale dreigingen. De keuze voor een vooraf gedefinieerde lijst – in plaats van een volledig unsupervised benadering – zorgt voor consistentie met bestaande beleidsanalyses en methodieken. De lijst is samengesteld op basis van de dreigingen die zijn geïdentificeerd in de Rijksbrede Risicoanalyse Nationale Veiligheid en de Trendanalyse Nationale Veiligheid 2024.[2 3] Beide rapporten zijn opgesteld door het Analistennetwerk Nationale Veiligheid.

Om de lijst geschikt te maken voor tekstuele analyse, zijn enkele aanpassingen doorgevoerd. Daarbij is onder meer gezorgd voor eenduidigere formuleringen en het voorkomen van overlap tussen deels overlappende dreigingen. De definitieve lijst omvat 71 nationale dreigingen en vormt het inhoudelijke fundament van de knooppuntenanalyse. De volledige lijst is beschikbaar op onze website.[c] Elk van deze dreigingen is door het model vervolgens gegroepeerd in een van de volgende zes categorieën: Gezondheid, Geopolitiek & Militair, Economisch, Sociaal & Maatschappelijk, Digitaal & Technologisch en Ecologisch.

Stap 3 – in kaart brengen van verbanden.

Voor het identificeren van verbanden tussen de afgebakende set dreigingen is een tweestapsaanpak toegepast met het taalmodel Gemini 2.5 Flash, gekozen vanwege de optimale balans tussen prestaties en kosten. In de eerste stap zijn causale verbanden uit de teksten geëxtraheerd; in de tweede stap zijn deze gemapt op de vooraf gedefinieerde lijst van nationale dreigingen.

Extractie van causale verbanden

In de eerste stap krijgt het taalmodel de opdracht om semantisch causale verbanden te identificeren. Dat wil zeggen: situaties waarin de ene dreiging op betekenisvolle wijze aanleiding geeft tot een andere. Het model herkende in de documenten bijvoorbeeld de volgende typen causale relaties:

- 'De kans op een zoetwatertekort neemt toe door opwarming en zeespiegelstijging.'[4]
- 'De activiteiten van cybercriminelen kunnen ook ondersteunend zijn aan de meer klassieke vormen van criminaliteit, zoals drugshandel of het witwassen van crimineel geld.'[5]
- 'Door het bestaan van strategische afhankelijkheden, kunnen indirect ook mogelijkheden ontstaan voor economische dwang, ongewenste toegang tot kennis of informatie, spionage, of sabotage.' [6]
- 'De pandemie trekt niet alleen een zware wissel op de levens van veel mensen, maar op onze hele manier van samenleven . Tegenstellingen worden scherper. Het publieke debat verhardt.' [7]
- 'Furthermore, the increasing threat of disinformation – worsened by significant developments in artificial intelligence and a rapidly changing (social) media landscape – will likely continue to affect NATO Allies.' [8]

Voor deze extractie van causale verbanden heeft het model per document toegang tot de eerste 10.000 tokens[d] (ongeveer 5.000 Nederlandse woorden), en tot de seedlist met nationale dreigingen om het juiste abstractieniveau te waarborgen. Voor elk gevonden verband genereert het model een gestructureerde output bestaande uit drie onderdelen: de geïdentificeerde oorzaak, het gevolg en een bijbehorend citaat uit het document[e]. Dit resulteerde bijvoorbeeld in de volgende output:

c https://denkwerk-kickstartai.nl/knooppuntenanalyse

d Een token is de basiseenheid van tekst voor taalmodellen. Deze limiet van 10.000 tokens per document is gekozen omdat de meeste documenten (mediaan: 9.663 tokens) hiermee volledig worden verwerkt, terwijl uitschieters van >1 miljoen tokens de analyseresultaten niet kunnen vertekenen.

e De authenticiteit van citaten is geverifieerd met n-gram matching, waarbij per citaat werd gecontroleerd of minstens 50% van de 3-grammen (groepjes van drie opeenvolgende woorden) ook daadwerkelijk in de originele brontekst aanwezig was. Deze methode werd gekozen vanwege variaties in tekstopmaak na conversie naar markdown.

- Citaat: "De kans op een zoetwatertekort neemt toe door opwarming en zeespiegelstijging."
- Oorzaak: "zeespiegelstijging"
- Gevolg: "kans op zoetwatertekort neemt toe"

Toewijzing causale verbanden aan geïdentificeerde dreigingen

In de tweede stap zijn de geïdentificeerde oorzaken en gevolgen geclassificeerd op basis van de vooraf gedefinieerde lijst van nationale dreigingen. Het model krijgt hierbij toegang tot de output van stap 1, bijvoorbeeld 'kans op een zoetwatertekort neemt toe', en koppelt deze aan de meest passende dreiging, zoals in dit geval: 'tekort aan drinkwater door verzilting en vervuiling'.

Oorzaken of gevolgen die niet gekoppeld kunnen worden aan een van de vastgestelde nationale dreigingen zijn uitgesloten van verdere analyse. Ook relaties waarbij zowel oorzaak als gevolg binnen één en dezelfde dreiging vallen, worden verwijderd om dubbeltellingen binnen het netwerk te voorkomen.

Na deze filterstap resteert een dataset van 5.091 unieke causale verbanden tussen nationale dreigingen, die de basis vormt voor de hierop volgende netwerkconstructie en knooppuntenanalyse.

Stap 4 – constructie van het dreigingsnetwerk

Op basis van de geïdentificeerde causale verbanden is een netwerkdiagram opgebouwd, waarin elke knoop een nationale dreiging representeert (toegewezen aan een specifieke categorie zoals "Ecologisch" of "Technologisch en Digitaal"), en elke verbinding een causaal verband tussen twee dreigingen weergeeft.

Bij de constructie van dit netwerk is uitsluitend gekeken naar de aanwezigheid van een betekenisvol causaal verband, en dus niet naar hoe vaak dat verband in de brondocumentatie wordt genoemd. Het aantal keren dat een verbinding wordt benoemd in de verschillende teksten, is immers sterk afhankelijk van de bronselectie en kan leiden tot vertekening.

Om de betrouwbaarheid van het netwerk te waarborgen, zijn alleen relaties opgenomen die worden ondersteund door ten minste zes unieke citaten, afkomstig uit verschillende documenten. Hierbij zijn vrijwel identieke citaten samengevoegd (de-duplicatie) om dubbelingen te voorkomen. Deze drempel voorkomt dat incidentele of brongebonden uitschieters een onevenredige invloed krijgen.

In het ontwerp van het netwerk zijn daarnaast twee methodologische keuzes gemaakt met betrekking tot de wijze waarop dreigingen met elkaar zijn verbonden. Deze keuzes worden geïllustreerd in de onderstaande paragrafen, ondersteund door schematische visualisaties.

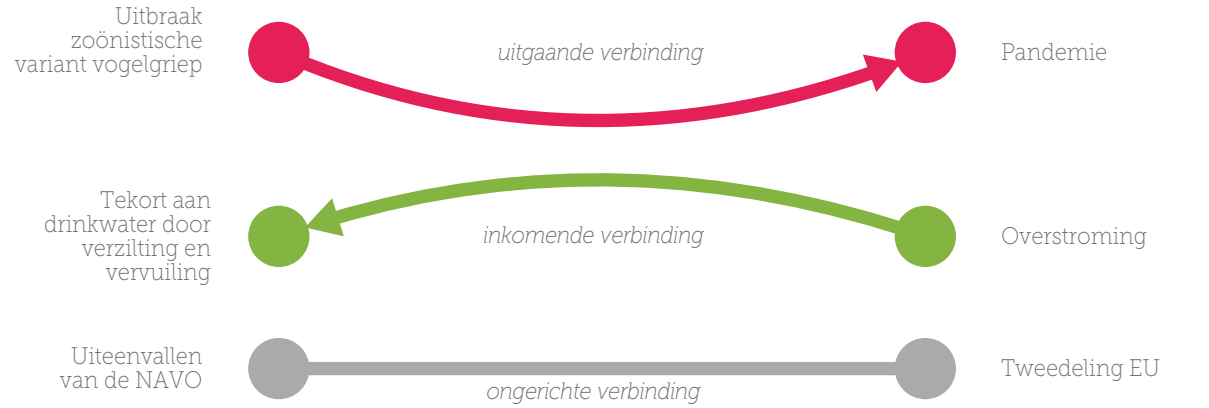
Gerichte verbanden: inzicht in oorzaak en gevolg

In onze analyse maken wij gebruik van gerichte causale verbanden. Dat betekent dat tussen twee dreigingen een richting wordt onderscheiden: een verbinding kan uitgaand zijn (waarbij een dreiging een andere dreiging veroorzaakt of beïnvloedt) of inkomend (waarbij een dreiging het gevolg is van een andere).

Voor het bepalen van de meest invloedrijke dreigingen - de centrale knooppunten in het netwerk - richten wij ons specifiek op de uitgaande verbindingen. Daarbij gaat het om dreigingen die andere dreigingen in gang kunnen zetten. Een voorbeeld hiervan is de uitbraak van een voor mensen besmettelijke vogelgriep, die kan leiden tot een pandemie (zie Figuur B4).

Ter volledigheid: inkomende verbindingen laten zien welke dreigingen voornamelijk worden veroorzaakt of versterkt door andere dreingen. Zo wordt een tekort aan drinkwater bijvoorbeeld veroorzaakt door vervuiling als gevolg van de uitspoeling van verontreinigende stoffen tijdens overstromingen. Gerichte benaderingen met uitgaande en inkomende verbindingen wijken daarnaast af van een ongerichte analyse, waarin uitsluitend wordt gekeken naar samenhang tussen dreigingen zonder onderscheid te maken tussen oorzaak en gevolg (zie het derde voorbeeld in Figuur B4). Met de ongerichte analyse zouden rol en richting van de onderlinge relaties buiten beeld blijven.

Figuur B4 Stilistische weergave richting van de verbanden



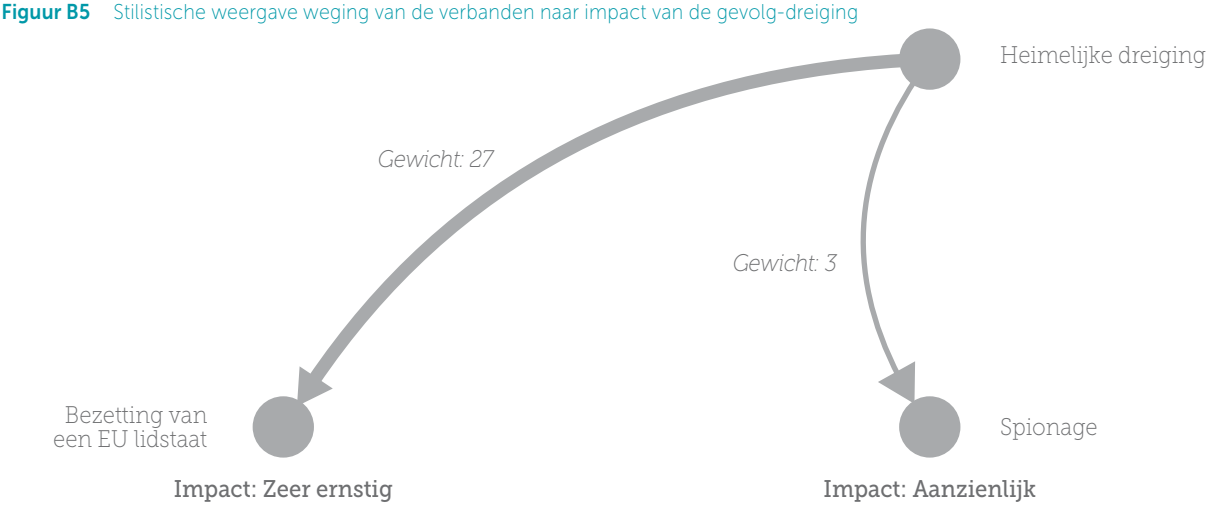
Bron: DenkWerk en Kickstart AI (2025)

Weging van de verbanden: het meenemen van impact van de gevolgen

Naast de richting van elk causaal verband is in onze analyse ook de verwachte impact meegewogen. Nadat in stap 3 een oorzaak-gevolgrelatie is vastgesteld, worden de geïdentificeerde verbanden gewogen op basis van de geschatte impact van de gevolgdreiging.

Voor deze weging is de methodiek uit de Rijksbrede Risicoanalyse Nationale Veiligheid ongewijzigd overgenomen. Dit houdt in dat zowel de vijf gehanteerde impactcategorieën - beperkt, aanzienlijk, ernstig, zeer ernstig en catastrofaal - als de daaraan gekoppelde exponentiële schaalwaarden (respectievelijk 1, 3, 9, 27 en 81) zijn toegepast. Daarmee tellen verbanden die leiden tot dreigingen met grotere impact zwaarder mee in het netwerk (zie Figuur B5). In de volgende stap gebruiken we deze gewogen uitgaande verbanden om de knooppunten te identificeren.

Figuur B5 Stilistische weergave weging van de verbanden naar impact van de gevolg-dreiging



Bron: DenkWerk en Kickstart AI (2025)

Stap 5 – Knooppuntenanalyse

Na het opstellen van het netwerk, waarin dreigingen met elkaar zijn verbonden via gerichte verbindingen en de weging de geschatte impact van de gevolgdreiging representeert, volgt de analyse naar knooppunten in het systeem.

Het doel is om de dreigingen te identificeren die, los van hun eigen directe impact, aantoonbaar invloed uitoefenen op andere dreigingen met een hoge impact. Met andere woorden: welke dreigingen kunnen andere, mogelijk catastrofale, dreigingen in gang zetten of versterken?

Om deze invloedrijke knooppunten te identificeren, berekenen we voor elke dreiging een zogenoemde knooppuntwaarde, op basis van het 'out-degree eigenvectorcentraliteitsprincipe'. Voordat we toelichten op welke wijze deze knooppuntwaarde is berekend, lichten we eerst twee methodologische keuzes toe die bepalen welke typen verbanden in de berekening zijn meegenomen.

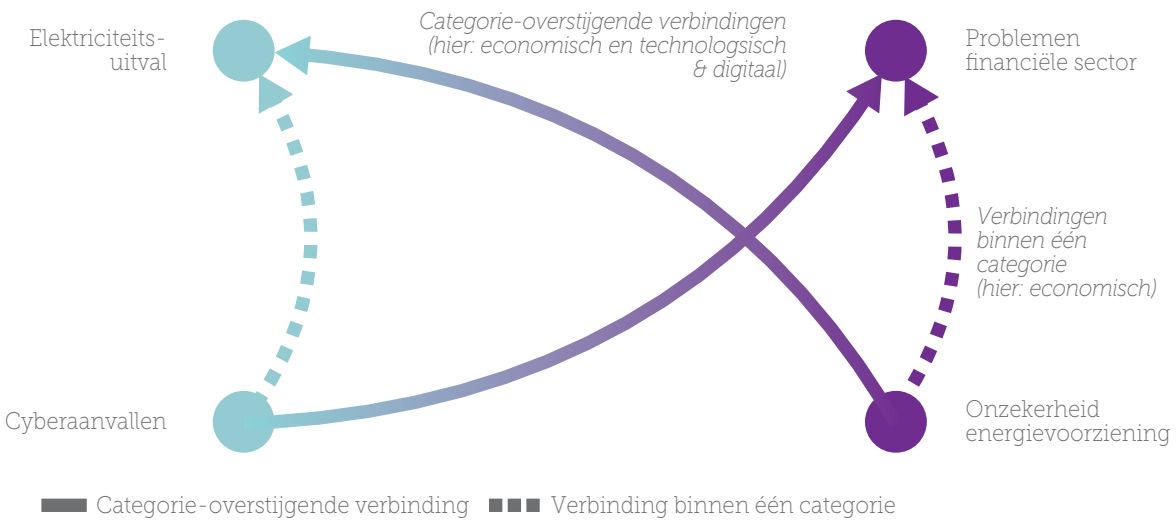
Categorie-overstijgende verbanden

Onze analyse richt zich uitsluitend op causale verbanden tussen dreigingen uit verschillende categorieën, weergegeven met doorgetrokken lijnen in Figuur B6. Verbindingen tussen dreigingen binnen één en dezelfde categorie, aangeduid met gestippelde lijnen, blijven buiten beschouwing bij de berekening van de knooppuntwaarde.

Onze analyse is immers gericht op het blootleggen van categorie-overschrijdende relaties. We zijn specifiek geïnteresseerd in deze verbanden omdat juist daar systeemrisico's ontstaan: ketens van oorzaak en gevolg die zich over meerdere domeinen verspreiden. Door ons te richten op deze verbindingen kunnen we de dreigingen identificeren die het grootste multiplier-effect genereren. Deze dreigingen vormen de logische aangrijpingspunten voor gericht beleid en gerichte interventies.

Hoewel ook de onderlinge relaties binnen één dreigingscategorie waardevol kunnen zijn – met name voor een volledig begrip van het dreigingslandschap – staan deze in onze analyse niet centraal. Om keteneffecten effectief te kunnen doorgronden én voorkomen, richten wij ons specifiek op dreigingen die categorie-overschrijdende systeemrisico's in gang zetten.

Figuur B6 Stilistische weergave categorie-overstijgende verbanden



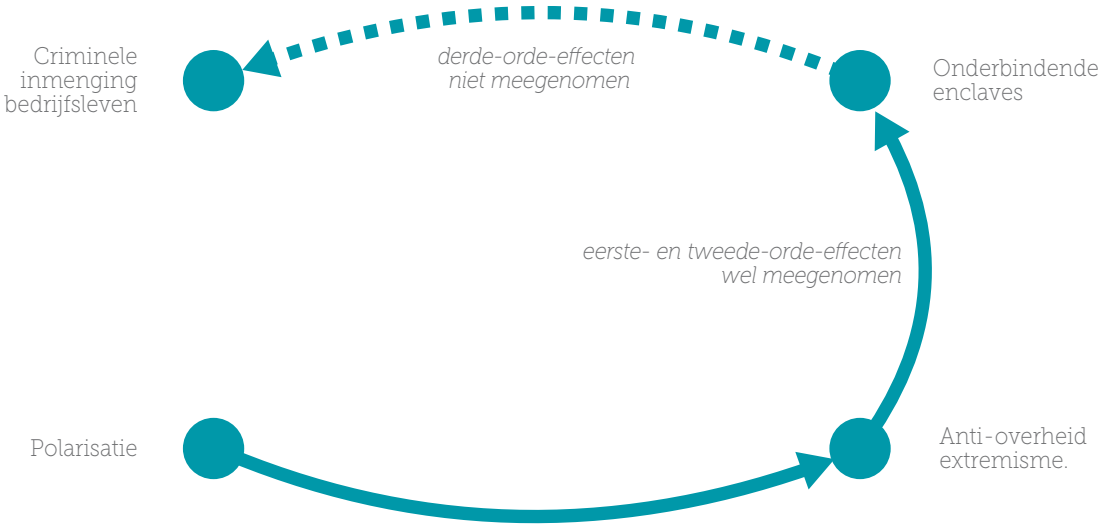
Bron: DenkWerk en Kickstart AI (2025)

Beperking tot tweede-orde-effecten

De knooppuntanalyse is bewust begrensd tot maximaal tweede-orde-effecten. Dit betekent dat we enkel verbanden meenemen die zich uitstrekken over ten hoogste twee stappen in het causale netwerk. Deze afbakening waarborgt zowel de uitvoerbaarheid als de interpretatie van de analyse.

Complexere ketens van drie of meer schakels (derde-orde-effecten en verder) blijven buiten beschouwing. In Figuur B7 zijn deze verbanden aangeduid met een gestippelde lijn.

Figuur B7 Stilistische weergave beperking tot tweede-orde-effecten



Bron: DenkWerk en Kickstart AI (2025)

Knooppuntwaarde op basis van 'out-degree eigenvectorcentraliteit'

Zoals in de voorgaande paragrafen toegelicht, omvat de knooppuntanalyse uitgaande, categorie-overschrijdende verbindingen, gewogen naar de geschatte impact van de gevolgdreiging, met een maximum van één tussenschakel (tweede-orde-effect).

Voor het bepalen van de knooppuntwaarde is vervolgens gebruikgemaakt van eigenvectorcentraliteit, berekend op basis van het aantal uitgaande verbindingen (out-degree) van een dreiging. Deze maat geeft niet alleen gewicht aan het aantal verbindingen dat een knooppunt heeft, maar ook aan het belang van de knooppunten waarnaar het verbonden is. Met andere woorden: een dreiging wordt als invloedrijk beschouwd – en krijgt een hoge knooppuntwaarde – wanneer deze linkt naar een andere dreiging die zelf ook veel en/of impactvolle uitgaande verbindingen heeft. Het gaat dus alleen over de uitgaande verbindingen en niet om de inkomende verbindingen. Zoals eerder beschreven, zijn de verbindingen gewogen op basis van de geschatte impact van de gevolg-dreiging. Dreigingen die (direct of via één tussenschakel) leiden tot andere dreigingen met hoge impact, krijgen daarmee een zwaarder gewicht in het netwerk.

Bronvermelding

1 Wolitzky, A. (2022). Lecture 3: Eigenvector centrality measures. MIT OpenCourseWare. Course 14.15 / 6.207 Networks, Spring 2022. URL: https://ocw.mit.edu

2 Analistennetwerk Nationale Veiligheid (2022). Rijksbrede Risicoanalyse Nationale Veiligheid. Technical report, Analistennetwerk Nationale Veiligheid.

3 Analistennetwerk Nationale Veiligheid (2024). Trendanalyse Nationale Veiligheid 2024. Technical report, Analistennetwerk Nationale Veiligheid. Hoofdrapport

4 Sociaal-Economische Raad (SER) (2025) - Naar een toekomstbestendige omgang met water. Signalering 25/01, Sociaal-Economische Raad, Den Haag. Signalering van de commissie Duurzame Ontwikkeling

5 Yeşilgöz-Zegerius, D. (2024). Voortgang van de integrale aanpak cybercrime en de bevoegdheden voor de opsporing in het digitale domein. Kamerstuk 26 643, nr. 1204, Ministerie van Justitie en Veiligheid, Den Haag

6 Keijser, B., and van Scheepstal, P. (2024). Beschikbare methoden voor beoordelen aantasting van nationale veiligheid door strategische afhankelijkheden. Technical Report TNO 2024 R11040, TNO Defensie & Veiligheid

7 Rutte, M. (2022). Regeringsverklaring kabinet-Rutte IV: Omzien naar elkaar, vooruitkijken naar de toekomst. Uitgesproken in de Tweede Kamer der Staten-Generaal

8 Zandee, D., van Loon, K., and de Baedts, R. (2025). Nato and the need to strengthen resilience - the Dutch case. Policy brief, Clingendael - Netherlands Institute of International Relations, The Hague