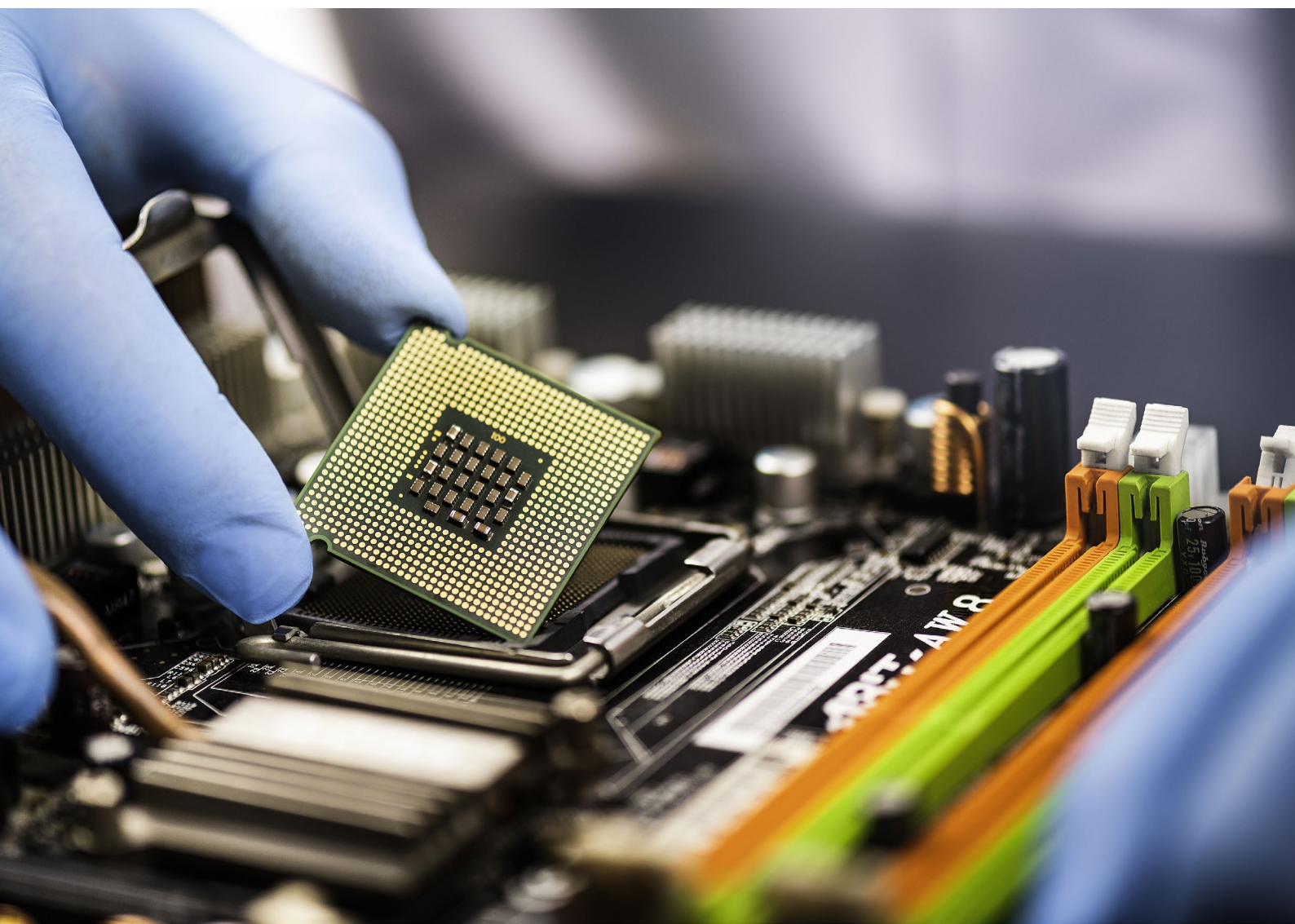


Rijksbrede Risicoanalyse Nationale Veiligheid 2026

Themarapport Combinatiescenario
De duistere kanten van *Big Tech*



Rijksbrede Risicoanalyse
Nationale Veiligheid 2026
Themarapport Combinatiescenario
De duistere kanten van *Big Tech*

Analistennetwerk Nationale Veiligheid (ANV)

Colofon

© RIVM 2026

Delen uit deze publicatie mogen worden overgenomen op voorwaarde van bronvermelding: Analistennetwerk Nationale Veiligheid (ANV). (2026). Rijksbrede Risicoanalyse Nationale Veiligheid 2026, Themaraapport Combinatiescenario De duistere kanten van *Big Tech*.

Contact:

anv@rivm.nl

De Rijksbrede Risicoanalyse Nationale Veiligheid 2026, Themaraapport Combinatiescenario De duistere kanten van *Big Tech* is opgesteld door het Analistennetwerk Nationale Veiligheid (ANV) in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-natuur-wetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale Betrekkingen
'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

Inhoudsopgave

1	Inleiding — 5
1.1	Doel — 5
1.2	Relatie met Trendanalyse — 5
1.3	Leeswijzer — 6
2	Methodiek nationale veiligheid — 7
2.1	Nationale veiligheidsbelangen — 7
2.2	Scenario's — 10
2.2.1	Enkelvoudige scenario's — 10
2.2.2	Combinatiescenario's — 11
2.3	Resultaten en beschouwing — 13
2.4	Geografische reikwijdte — 13
3	Combinatiescenario: De duistere kanten van <i>Big Tech</i> — 15
3.1	Inleiding combinatiescenario — 16
3.2	Het scenario: De duistere kanten van <i>Big Tech</i> – op aanvraag — 17
3.3	Wat als...? — 17
3.4	Beschouwing combinatiescenario De duistere kanten van <i>Big Tech</i> — 18
3.4.1	Kwetsbaarheden — 19
3.4.2	Handelingsperspectief — 22
4	Literatuur — 23
	Bijlage 1 Samenstelling Analistennetwerk Nationale Veiligheid — 29

1 Inleiding

De Rijksbrede Risicoanalyse Nationale Veiligheid 2026 brengt verschillende typen dreigingen die de nationale veiligheid kunnen raken in kaart. De risicoanalyse dient daarmee als onderbouwing voor het actualiseren van de Veiligheidsstrategie voor het Koninkrijk der Nederlanden. Deze risicoanalyse is opgesteld door het Analistennetwerk Nationale Veiligheid (ANV) op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

1.1 Doel

In 2023 is de Veiligheidsstrategie voor het Koninkrijk der Nederlanden opgesteld (hierna: 'de Veiligheidsstrategie'; Rijksoverheid, 2023). De Veiligheidsstrategie is mede gebaseerd op het dreigingsbeeld zoals geschetst in de Rijksbrede Risicoanalyse (hierna: 'RbRa') 2022 (ANV, 2022) en vertaalt deze naar strategische thema's, doelstellingen en actielijnen. Voorliggende Rijksbrede Risicoanalyse 2026 vormt inhoudelijke input voor de aankomende actualisatie van de Veiligheidsstrategie. Het doel van de RbRa daarbij is het in kaart brengen van verschillende typen dreigingen die de nationale veiligheid kunnen raken. Hiertoe worden mogelijke dreigingen geïdentificeerd en wordt een inschatting gemaakt van waarschijnlijkheid en mogelijke impact (gezamenlijk het risico). Ook worden onderliggende kwetsbaarheden beschouwd. De inschatting van het risico vindt plaats aan de hand van door het ANV opgestelde fictieve, plausibele scenario's. De dreigingen in kwestie zijn verdeeld over acht dreigingsthema's, elk onderverdeeld in meerdere dreigingscategorieën met daarin een aantal enkelvoudige scenario's. Daarnaast zijn vier combinatiescenario's opgesteld waarin meerdere centrale kernebeurtenissen uit verschillende dreigingsthema's zijn samengevoegd.

Omdat de nationale veiligheid door veel verschillende soorten dreigingen kan worden aangetast, is een *all hazard*-aanpak gebruikt. Zowel moedwillige (*security*) als niet-moedwillige (*safety*) en zowel interne als externe dreigingen worden beschouwd.

1.2 Relatie met Trendanalyse

De Rijksbrede Risicoanalyse 2026 bouwt voort op de bevindingen uit de in 2024 door het ANV opgestelde Trendanalyse Nationale Veiligheid (ANV, 2024). In de Trendanalyse zijn ontwikkelingen gesignaleerd en geduid die invloed hebben op de dreigingen voor de nationale veiligheid. Deze kunnen worden samengevat in vier hoofdboodschappen:

1. De directe en indirecte gevolgen van klimaatverandering worden steeds merkbaarder;
2. Technologische ontwikkelingen zullen in grote mate de toekomstige veiligheidsomgeving gaan beïnvloeden;
3. Het geopolitieke conflict- en escalatiepotentieel neemt substantieel toe;
4. Structurele economische uitdagingen worden urgenter.

Deze hoofdboodschappen en veel van de andere ontwikkelingen uit de Trendanalyse zijn nog steeds actueel. De Trendanalyse vormt daarmee het startpunt voor deze RbRa. Dit is ook de reden dat er binnen deze risicoanalyse geen uitgebreide uiteenzetting van trends en ontwikkelingen wordt gegeven.

1.3 Leeswijzer

De Rijksbrede Risicoanalyse Nationale Veiligheid 2026 bestaat uit een hoofdrapport en de volgende twaalf themaraapporten:

- Themaraapport combinatiescenario Water, een zegen of een vloek?;
- Themaraapport combinatiescenario De duistere kanten van *Big Tech*;
- Themaraapport combinatiescenario Oorlog in Europa;
- Themaraapport combinatiescenario Sanctiepolitiek tegen geïsoleerd Nederland;
- Themaraapport Klimaat- en natuurrampen;
- Themaraapport Infectieziekten;
- Themaraapport Zware ongevallen;
- Themaraapport Polarisatie, extremisme en terrorisme;
- Themaraapport Ongewenste inmenging en beïnvloeding democratische rechtsstaat;
- Themaraapport Internationale en militaire dreigingen;
- Themaraapport Economische dreigingen;
- Themaraapport Cyberdreigingen.

Anders dan in voorgaande risicoanalyses is het thema *Bedreiging vitale infrastructuur* niet meer als apart thema opgenomen. Hiervoor is gekozen omdat de andere thema's oorzaken van dreigingen zijn, terwijl dreigingen voor de vitale infrastructuur eerder een gevolg zijn. De gevolgen van dreigingen voor de vitale processen van de Nederlandse maatschappij — zoals drinkwatervoorziening, olievoorziening en scheepvaartafwikkeling¹ — worden nu explicieter weergegeven in de scenario's.

De themaraapporten dienen als basis voor het hoofdrapport van de RbRa. Daarin worden de dreigingen gezamenlijk beschouwd. Het hoofdrapport geeft daarmee de belangrijkste uitkomsten en conclusies van de Rijksbrede Risicoanalyse 2026 voor de nationale veiligheid.

In dit themaraapport is het combinatiescenario De duistere kanten van *Big Tech* weergegeven. Het themaraapport bestaat uit twee onderdelen. In het eerste onderdeel wordt een algemene beschrijving gegeven van de gehanteerde methodiek. Hierin wordt ingegaan op hoe de beoordeling van de impact van de dreigingen aan de hand van de zes nationale veiligheidsbelangen en voor de eenvoudige scenario's ook de waarschijnlijkheid is uitgevoerd. In het tweede onderdeel wordt ingegaan op het uitgewerkte combinatiescenario. Naast de verhaallijn is de beoordeling van de impact weergegeven. In de beschouwing wordt vervolgens een reflectie gegeven op de implicaties van het combinatiescenario op de nationale veiligheid (zoals ook opgenomen in het Hoofdrapport).

¹ Zie voor een actueel en compleet overzicht: NCTV (2025). Overzicht vitale processen.

2 Methodiek nationale veiligheid

Dit onderdeel bevat een algemene beschrijving van de methodiek die is gehanteerd bij de beoordeling van de impact en de waarschijnlijkheid van de dreigingen aan de hand van de zes nationale veiligheidsbelangen.

In de risicoanalyse zijn twee soorten scenario's opgenomen: enkelvoudige scenario's en combinatiescenario's. Een enkelvoudig scenario kijkt naar een op zichzelf staande gebeurtenis, zoals een overstroming, terroristische aanslag of handelsoorlog. De enkelvoudige scenario's zijn analyses van dreigingen die een plek hebben in een van de dreigingsthema's. Combinatiescenario's omvatten meerdere centrale kerngebeurtenissen die samenkomen (multi-dreiging). Dit zijn gebeurtenissen die als zelfstandige gebeurtenis passen binnen een dreigingscategorie en binnen het combinatiescenario gezamenlijk worden beschouwd. Denk bijvoorbeeld aan een overstroming in combinatie met zowel uitval van vitale processen als maatschappelijke polarisatie. Het idee is dat in de praktijk verschillende dreigingen gelijktijdig kunnen plaatsvinden, elkaar snel kunnen opvolgen of op elkaar kunnen inwerken.

Voor elk van de scenario's zijn door het ANV in samenspraak met de werkgroep methodiek de mogelijke gevolgen (impact) voor de nationale veiligheid in kaart gebracht. Dit is gedaan aan de hand van de door het ANV opgestelde methodiek. Voor de enkelvoudige scenario's geldt dat naast de impact ook de waarschijnlijkheid van optreden volgens de methodiek is ingeschat.

2.1 Nationale veiligheidsbelangen

Binnen de methodiek wordt gekeken of en in welke mate een scenario de zes nationale veiligheidsbelangen raakt. De nationale veiligheid is in het geding als één of meer van de zes nationale veiligheidsbelangen zodanig wordt bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting (ANV, 2026). De zes belangen zijn elk opgesplitst in meerdere meetbare impactcriteria die helpen bij het in kaart brengen van een mogelijke aantasting. Onderstaande tabel geeft een overzicht van alle belangen en criteria. Een uitgebreide uitleg voor elk van deze onderdelen bevindt zich in de door het ANV opgestelde Leidraad Risicobeoordeling (ANV, 2026).

Tabel 1 Veiligheidsbelangen en impactcriteria behorende tot de methodiek nationale veiligheid

Veiligheidsbelang	Impactcriteria
1. Territoriale veiligheid	1.1 Aantasting van de integriteit van het grondgebied van het Koninkrijk der Nederlanden
	1.2 Aantasting van de integriteit van de internationale positie van het Koninkrijk der Nederlanden
	1.3 Aantasting van de integriteit van informatie en digitale ruimte

<i>Veiligheidsbelang</i>	<i>Impactcriteria</i>
	1.4 Aantasting van de integriteit van het grondgebied van EU en NAVO lidstaten inclusief het Koninkrijk der Nederlanden
2. Fysieke veiligheid	2.1 Doden 2.2 Ernstig gewonden en chronisch zieken 2.3 Gebrek aan primaire levensbehoeften
3. Economische veiligheid	3.1 Kosten 3.2 Aantasting van de vitaliteit van de economie van het Koninkrijk der Nederlanden
4. Ecologische veiligheid	4.1 Langdurige aantasting van natuur- en landschappelijke gebieden die als beschermwaardig zijn aangewezen 4.2 Langdurige aantasting van het milieu en de natuur in algemene zin
5. Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtsstaat 5.3 Sociaal-maatschappelijke impact
6. Internationale rechtsorde en stabiliteit	6.1 Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting 6.2 Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens 6.3 Aantasting van de effectiviteit, legitimiteit van multilaterale instituties en internationale regimes 6.4. Instabiliteit van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie

Voor het geven van een oordeel over de precieze omvang van de gevolgen van een scenario, wordt aan elk van de criteria een impactscore toegekend, namelijk: niet van toepassing (0), beperkt (A), aanzienlijk (B), ernstig (C), zeer ernstig (D) of catastrofaal (E). Er is sprake van maatschappelijke ontwrichting als één of meer van de belangen ernstig (klasse C) of hoger wordt aangetast. De classificering is gebaseerd op een logaritmische schaal. Voor criterium 2.1 (aantal doden) betekent dit bijvoorbeeld dat een beperkte score staat voor 0-10 doden, een aanzienlijke score voor 10-100 doden, et cetera. Eenzelfde redenatie wordt gehanteerd voor criterium 3.1 (kosten).

Tabel 2 Voorbeeld van verschillende klassen van gevolg binnen de methodiek nationale veiligheid

<i>Klasse van gevolgen</i>	<i>Voorbeeld criterium: Aantal doden (2.1)</i>	<i>Voorbeeld criterium: Kosten (3.1)</i>
A. Beperkt	Minder dan 10	<100 miljoen euro
B. Aanzienlijk	10 tot 100	<1 miljard euro
C. Ernstig	100 tot 1000	<10 miljard euro
D. Zeer ernstig	1000 tot 10.000	<100 miljard euro
E. Catastrofaal	Meer dan 10.000	>100 miljard euro

In tegenstelling tot de bovenstaande criteria 2.1 en 3.1, zijn sommige criteria niet uit te drukken in een absoluut aantal. Een voorbeeld hiervan

is criterium 5.2, aantasting van de democratische rechtsstaat. Hiervoor wordt de score bepaald door de mate waarin de verschillende onderdelen van de democratische rechtsstaat worden aangetast. Deze onderdelen zijn:

- Het functioneren van de politieke vertegenwoordiging;
- Het functioneren van het openbaar bestuur en daaraan verbonden ambtenaren;
- Het functioneren van het openbare orde en veiligheidssysteem;
- Het functioneren van een onafhankelijke rechtspraak;
- Functioneren van onafhankelijke media en wetenschap;
- Vrijheden en rechten zoals vastgelegd in grondwet en wetgeving (vrijheid van godsdienst, meningsuiting, vereniging, kiesrecht, etc.).

Naarmate de aantasting groter is en voor meerdere onderdelen van toepassing blijkt neemt de score toe.

Voor elk van de in de risicoanalyse beoordeelde scenario's is aan de hand van een scorekaart per criterium weergegeven wat de verwachte impact is. De totale impact van een scenario is vervolgens berekend op basis van de impact op de zes veiligheidsbelangen. Voor een gedetailleerde toelichting hierop wordt verwezen naar de leidraad risicobeoordeling (ANV, 2026).

Binnen de methodiek wordt bij de enkelvoudige scenario's niet alleen gekeken naar de impact van gebeurtenissen, maar ook naar de waarschijnlijkheid van voorkomen. Voor het bepalen van deze waarschijnlijkheid wordt gekeken naar de kans van voorkomen binnen de komende vijf jaar. Deze kans wordt afhankelijk van het type gebeurtenis kwalitatief of kwantitatief weergegeven op een vijfpuntschaal van zeer onwaarschijnlijk (klasse A) tot zeer waarschijnlijk (klasse E). Voor het bepalen van de waarschijnlijkheid wordt er een onderscheid gemaakt tussen moedwillige en niet-moedwillige dreigingen (zie onderstaande tabel).

Tabel 3 Klassen van waarschijnlijkheid binnen de methodiek nationale veiligheid

<i>Klasse van waarschijnlijkheid</i>	<i>Kwantitatieve inschatting niet-moedwillige dreiging in % per 5 jaar</i>	<i>Kwalitatieve omschrijving moedwillige dreiging</i>
A. Zeer onwaarschijnlijk	<0,05	Geen concrete aanwijzingen en het scenario wordt niet voorstelbaar geacht
B. Onwaarschijnlijk	0,05 - 0,5	Geen concrete aanwijzingen, maar het scenario wordt enigszins voorstelbaar geacht
C. Enigszins waarschijnlijk	0,5 - 5	Geen concrete aanwijzingen, maar het scenario is voorstelbaar
D. Waarschijnlijk	5 - 50	Het scenario wordt zeer voorstelbaar geacht; er zijn enige aanwijzingen dat het scenario zich daadwerkelijk zal voordoen

<i>Klasse van waarschijnlijkheid</i>	<i>Kwantitatieve inschatting niet-moedwillige dreiging in % per 5 jaar</i>	<i>Kwalitatieve omschrijving moedwillige dreiging</i>
E. Zeer waarschijnlijk	50 - 100	Concrete aanwijzingen dat het scenario geëffectueerd zou kunnen worden

Ook de ingeschatte waarschijnlijkheid wordt voor elk van de enkelvoudige scenario's weergegeven in de eerdergenoemde scorekaart.

2.2 Scenario's

De methodiek voor het tot stand komen van de enkelvoudige scenario's en van de combinatiescenario's wordt hieronder nader toegelicht.

2.2.1 Enkelvoudige scenario's

Binnen de RbRa zijn de geanalyseerde dreigingen onderverdeeld in dreigingsthema's, zoals *Klimaat- en natuurrampen*, *Cyberdreigingen*, *Zware ongevallen* en *Internationale en militaire dreigingen*. Elk dreigingsthema is uitgewerkt in dreigingscategorieën. Enkelvoudige scenario's worden gebruikt om de dreiging behorende tot een bepaalde dreigingscategorie te illustreren en de impact en waarschijnlijkheid te helpen beoordelen. Zo illustreren de scenario's hoe de dreiging zich mogelijk kan manifesteren.

Ten behoeve van het identificeren en uitwerken van de scenario's is gebruik gemaakt van 'bouwstenen'. Bouwstenen typeren de relevante factoren voor een dreigingscategorie. In onderstaande tabel zijn de bouwstenen voor de dreigingscategorie *Extreem weer* (onderdeel van *Klimaat- en natuurrampen*) als voorbeeld weergegeven. Door factoren te combineren kunnen meerdere situaties ofwel scenario's worden gecreëerd. Uiteraard zullen verschillende combinaties leiden tot verschillende scenario's met wisselende uitkomsten. In onderstaande tabel zijn de gecombineerde bouwstenen voor het scenario 'Hitte en droogte' dikgedrukt weergegeven. De bouwstenen helpen om in één oogopslag duidelijk te maken wat wel en wat niet is meegenomen in het scenario en dienen als referentiekader voor de uiteindelijke verhaallijn.

Tabel 4 Voorbeeld bouwstenen Extreem weer met dikgedrukt de gecombineerde bouwstenen voor het scenario 'Hitte en droogte'²

Weertype	Duur (tijd)	Intensiteit	Omvang getroffen gebied	Bereikbaarheid gebied na incident	Uitval voorzieningen³
Sneeuw	<1 dag	Licht	<50 km ²	Goed bereikbaar	Openbaar vervoer
Hagel	1 tot 3 dagen	Matig	50-100 km ²	Slecht bereikbaar	Water
IJzel	3 tot 7 dagen	Zwaar	100-1000 km ²	Zeër slecht bereikbaar	Stroom

² Vanuit de verschillende mogelijkheden uit de kolommen zijn verschillende scenario's denkbaar. De mogelijkheden uit een rij horen niet noodzakelijkerwijs bij elkaar.

³ Deze lijst is niet uitputtend; zie voor een actueel en compleet overzicht NCTV (2025). Overzicht vitale processen.

Weertype	Duur (tijd)	Intensiteit	Omvang getroffen gebied	Bereikbaarheid gebied na incident	Uitval voorzieningen ³
Storm	1 week tot 1 maand	Extreem zwaar	1.000-10.000 km ²		Voedsel
Regenval	>3 maanden		>10.000 km²		Hulpdiensten
Mist					Communicatie voorzieningen
Droogte					
Hitte					

Op basis van de selectie van de bouwstenen wordt een scenario uitgewerkt in de vorm van een verhaallijn (narratief). Dit gebeurt in samenspraak met deskundigen behorende tot organisaties verbonden aan het ANV.

De in deze risicoanalyse opgenomen scenario's betreffen fictieve, plausibele scenario's van hoe een dreiging zich de komende jaren kan manifesteren. Ze zijn nadrukkelijk niet uitputtend, maar zijn bedoeld als duidelijke illustraties van een dreigingscategorie.

2.2.2 Combinatiescenario's

Het achterliggend idee van de combinatiescenario's is om uit te lichten hoe verschillende typen dreigingen elkaar kunnen beïnvloeden. Het doel is om inzicht te krijgen in kwetsbaarheden en andere risicofactoren, die onderbelicht zouden blijven als wordt gewerkt met alleen enkelvoudige scenario's. Daarom bevat elk combinatiescenario meerdere centrale kerngebeurtenissen. Er zijn namelijk omstandigheden denkbaar waarbij verschillende van deze gebeurtenissen (nagenoeg) gelijktijdig plaatsvinden of elkaar versterken en gezamenlijk tot een grotere impact op de nationale veiligheid leiden. Waar een enkelvoudig scenario als focus de uitwerking van één dreiging heeft, gaat het bij een combinatiescenario om het samenkomen van meerdere dreigingen (multi-dreiging). Omdat in de RbRa 2026 voor het eerst gewerkt wordt met combinatiescenario's, zijn de gehanteerde uitgangspunten, selectiecriteria, wijze van beoordeling en mogelijke beperkingen van dit type scenario hieronder opgenomen.

2.2.2.1 Uitgangspunten

Er zijn een aantal uitgangspunten waar de in de RbRa opgenomen combinatiescenario's als set aan voldoen. Een aantal hiervan zijn meer gericht op de analytische functie van de combinatiescenario's en een aantal meer op de inhoudelijke balans van het set als geheel. Deze uitgangspunten zijn als volgt:

- Combinatiescenario's identificeren aanvullende, nieuwe of onderbelichte risico's voor de nationale veiligheid die kunnen voortkomen uit het gelijktijdig plaatsvinden of uit elkaar voortkomen (cascade) van verschillende dreigingen;
- Er is aandacht voor verschillende gronddoorzaken van combinaties van dreigingen: dreigingen die uit elkaar voortkomen, dreigingen met een gedeelde oorzaak en dreigingen die (toevallig) gelijktijdig plaatsvinden;
- De set aan scenario's biedt een plek aan (uitingen van) elk van de vier transities voor de nationale veiligheid die zijn geïdentificeerd in de Trendanalyse 2024 (ANV, 2024);

- Er is voldoende aandacht voor de onderlinge interactie tussen moedwillige en niet-moedwillige dreigingen. Bijvoorbeeld door te laten zien hoe deze elkaars gevolgen versterken of hoe ze in sommige gevallen een beroep doen op dezelfde capaciteiten.

2.2.2.2 Selectiecriteria

In lijn met bovenstaande uitgangspunten zijn meerdere selectiecriteria geformuleerd, waarmee vervolgens de combinatiescenario's zijn opgesteld:

- Elk combinatiescenario moet drie kerngebeurtenissen bevatten. Er zijn omstandigheden denkbaar waarbij verschillende van deze gebeurtenissen (nagenoeg) gelijktijdig plaatsvinden of elkaar versterken en gezamenlijk tot een grotere impact op nationale veiligheid leiden;
- Voor deze kerngebeurtenissen geldt dat er binnen de set van combinatiescenario's een goede afspiegeling moet zijn van de verschillende dreigingsthema's uit de RbRa. Oftewel, de opgenomen kerngebeurtenissen moeten divers van aard zijn;
- Voor de kerngebeurtenissen zelf moet een diverse set aan achterliggende factoren, ontwikkelingen en actoren worden gekozen. Zo moet bijvoorbeeld worden voorkomen dat telkens dezelfde actor centraal staat;
- Bij tenminste één van de combinatiescenario's is er in één van de kerngebeurtenissen een verbinding met het Caribisch deel van het Koninkrijk. Voor de andere combinatiescenario's geldt dat er bijvoorbeeld in de 'wat als' of beschouwing aandacht moet zijn voor het Caribisch deel van het Koninkrijk;
- De gevolgen van elk combinatiescenario moeten structureel zijn. Dat wil zeggen dat de gevolgen niet gemakkelijk terug kunnen worden gedraaid. Er is blijvend iets veranderd in bijvoorbeeld de maatschappij, de internationale gemeenschap of de leefomgeving. Dit betekent dat combinatiescenario's ingrijpende kerngebeurtenissen omvatten met relatief grote gevolgen voor de nationale veiligheid;
- Het scenario moet als geheel een *plausibele worst case*-variant zijn. Dit wil zeggen dat de kerngebeurtenissen uit het scenario redelijkerwijs zouden kunnen plaatsvinden, ook al is de impact hoog. Het scenario is dus geen 'wild card' of doorkijk naar een bijzonder extreme situatie;
- Het scenario moet binnen nu en vijf jaar merkbare gevolgen hebben óf het scenario vereist binnen nu en vijf jaar actie om de weerbaarheid te verhogen ter voorbereiding op dreigingen.

Bovenstaande uitgangspunten en selectiecriteria vormen het kader van de selectie van de combinatiescenario's. De verhaallijnen van de combinatiescenario's die op basis hiervan zijn uitgewerkt, bevatten vervolgens een mogelijke uitwerking van de combinatie van de geselecteerde dreigingen. Er zijn echter meerdere alternatieve uitwerkingen mogelijk. Daarom zijn er bij elk combinatiescenario in de vorm van een 'Wat als?' enkele alternatieve uitwerkingen weergegeven. Verder vormen de combinatiescenario's in de RbRa een eerste vertrekpunt en kunnen na de RbRa andere combinatiescenario's worden uitgewerkt.

De selectie van (het aantal) combinatiescenario's is gebaseerd op de belangrijkste trends uit de Trendanalyse 2024, waarbij in de uitwerking ook wordt voldaan aan de bovengenoemde uitgangspunten en criteria.

2.2.2.3 Beoordeling

De combinatiescenario's worden — anders dan de enkelvoudige varianten — alleen beoordeeld op gevolgen en niet op waarschijnlijkheid. De combinatiescenario's worden geschreven vanuit de gedachte dat deze plausibel *worst case* moeten zijn. De kerngebeurtenissen uit het scenario kunnen dus redelijkerwijs plaatsvinden ook al is de impact hoog. Ze zijn daarmee ook (in combinatie) een relevant onderwerp voor de nationale veiligheid. Wat betreft de beoordeling, ligt de nadruk op het uiteenzetten van logische, impactvolle verbanden tussen de verschillende kerngebeurtenissen en niet op het beoordelen van de waarschijnlijkheid hiervan.

Voor de beoordeling van de gevolgen wordt net als bij de enkelvoudige scenario's gebruik gemaakt van de veiligheidsbelangen en impactcriteria uit de Leidraad Risicobeoordeling. Het combinatiescenario wordt hierbij in zijn geheel beoordeeld. Er is dus uiteindelijk voor elk impactcriterium één impactscore voor alle gebeurtenissen uit het scenario samen.

2.3 Resultaten en beschouwing

Om de resultaten van de losse scenariobeoordelingen nader te duiden, wordt per dreigingsthema en per combinatiescenario een beschouwing opgesteld. Om te helpen bij de uiteindelijke vergelijking van alle enkelvoudige scenario's, bevat de slotbeschouwing van elk dreigingsthema een risicodiagram met een overzicht van de scenario's geplot langs de assen waarschijnlijkheid en impact.

In de beschouwing van de combinatiescenario's wordt, naast de impact op de nationale veiligheidsbelangen, ingegaan op onderliggende ontwikkelingen. Verder wordt gekeken naar welke kwetsbaarheden naar voren komen. Hierbij gaat het om aspecten als afhankelijkheden en beperkingen in capaciteit. Aanvullend kan worden ingegaan op de 'wat als' varianten die bij de combinatiescenario's zijn benoemd. Deze beschouwing is niet strak gekaderd, maar geeft de onderzoekers juist de ruimte om een stap terug te doen en te reflecteren op het scenario.

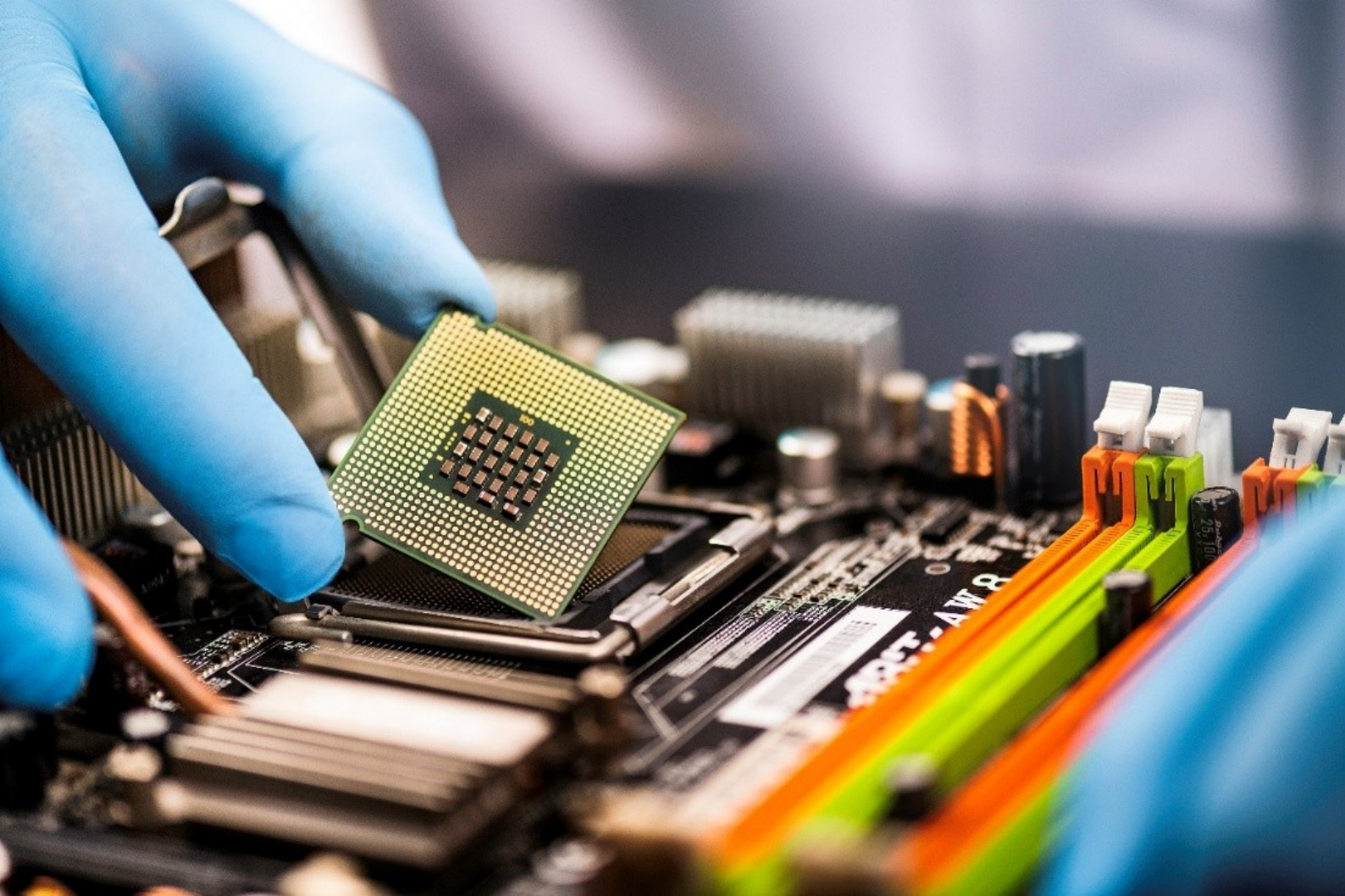
De resultaten van de beschouwingen van de combinatiescenario's en de dreigingsthema's vormen vervolgens input voor de hoofdbeschouwing van in het hoofdrapport van de RbRa 2026. Deze hoofdbeschouwing bestaan uit de belangrijkste dreigingen, kwetsbaarheden (in de zin van afhankelijkheden en capaciteiten) en handelingsperspectief (opties om de weerbaarheid te vergroten). Daarbij ligt de nadruk op de dreigingen en kwetsbaarheden, de handelingsperspectieven zijn niet volledig geanalyseerd.

2.4 Geografische reikwijdte

Geografisch is de reikwijdte van de Rijksbrede Risicoanalyse het gehele Koninkrijk der Nederlanden. Dit betekent dat risico's en dreigingen inzichtelijk worden gemaakt voor zowel Europees Nederland als het Caribisch deel van het Koninkrijk. Daarbij is het van belang om te

benadrukken dat uitsluitend scenario's geselecteerd en uitgewerkt worden die invloed hebben op de nationale veiligheid van het Koninkrijk in zijn geheel. Scenario's met uitsluitend lokale of regionale gevolgen — door bijvoorbeeld (lokale) manifestaties van zware ongevallen, verstoring van vitale infrastructuur en infectieziekten — vallen buiten de scope van de RbRa. Deze zijn veelal reeds opgenomen in regionale risicoprofielen, zoals de risicoprofielen van Curaçao (IFV, 2017) en van de Veiligheidsregio Zuid-Holland Zuid (Veiligheidsregio ZHZ, 2024). De scenario's die betrekking hebben op het Caribisch deel van het Koninkrijk zullen daardoor met name gaan over natuurrampen en internationale en territoriale dreigingen. Bij het beoordelen van de scenario's betreffende het Caribisch deel van het Koninkrijk wordt dezelfde methodiek gehanteerd als voor het beoordelen van de scenario's voor Europees Nederland.

Bij het lezen van de RbRa is het van belang om bewust te zijn van het feit dat de eilanden in het Caribisch deel van het Koninkrijk relatief kwetsbaar zijn voor een breed scala aan dreigingen. Dit heeft te maken met hun kleine omvang, laag niveau aan redundantie op het gebied van (vitale) infrastructuur en afhankelijkheden. Er is bijvoorbeeld vaak slechts één aanbieder per vitale sector, bijvoorbeeld één ziekenhuis en één bedrijf dat elektriciteit opwekt. Uitval van een dergelijke aanbieder heeft daardoor grote gevolgen.



3 Combinatiescenario: De duistere kanten van *Big Tech*

Big Tech is een verzamelterm voor de grootste en meest invloedrijke technologiebedrijven ter wereld die een dominante positie innemen in de digitale economie. Het gaat meestal om bedrijven zoals Alphabet (Google), Apple, Amazon, Meta (Facebook) en Microsoft uit de Verenigde Staten (VS) en Baidu, Alibaba, Tencent en Xiaomi uit China.

Big Tech als sector controleert in toenemende mate meningsuiting, verzamelt inlichtingen en is van belang in het beschermen van kritieke infrastructuur (Schaake, 2025). De bedrijfsvoering en informatievoorziening van zowel publieke als private partijen zijn vrijwel volledig afhankelijk van *Big Tech* (Stikker, 2025). Digitalisering gaat voor uitvoeren van publieke diensten vaak gepaard met uitbesteding via private digitale infrastructuur bij commerciële dienstverleners. Hierdoor krijgt *Big Tech* (als private partijen) steeds meer invloed op publieke processen, terwijl politiek en overheid vaker buiten spel staan (Schaake, 2025) (Hubert, 2026).

Tegelijkertijd groeit de afhankelijkheid van digitale technologie en van grote buitenlandse aanbieders (Wetenschappelijke Raad voor het Regeringsbeleid, 2019). De EU ontbeert technologische soevereiniteit op diverse terreinen, waaronder technologieën die digitalisering mogelijk maken. Dit leidt tot afhankelijkheid van Amerikaanse en Aziatische partijen, wat ten koste gaat van het Europese concurrentievermogen (Draghi, 2024). Onlineplatforms zijn essentieel geworden voor communicatie, maar worden steeds minder transparant. Door verschillende processen (bijvoorbeeld moderatiebeleid) waarbij data wordt gebruikt om bijvoorbeeld sociale interactie te interpreteren en te voorspellen en selecties te maken in informatie die gebruikers te zien krijgen, beïnvloeden deze platforms online interacties op manieren die moeilijk te doorzien zijn (de Bakker, van Kampen, & van Belkom, 2025).

Toch is er steeds meer maatschappelijke en politieke bewustwording van de risico's van afhankelijkheid van een klein aantal *Big Tech* bedrijven. Zo zijn er vanuit verschillende sectoren waarschuwingen voor de risico's van digitale afhankelijkheden (zoals de financiële sector (DNB, AFM, 2025), het onderwijs (de Moor, Boiten, & Stone, 2024) en de overheid (Algemene Rekenkamer, 2025)). Onder meer in de Nederlandse Digitaliseringsstrategie is aandacht voor het versterken van de digitale weerbaarheid en het verminderen van de afhankelijkheid (Rijksoverheid, 2025). Bovendien zijn er op Europees niveau verschillende wetgevingstrajecten gaande, zoals de Digital Services Act, de Digital Markets Act en de AI Act, die pogen middels regelgeving de macht van *Big Tech* bedrijven in te perken.

3.1 Inleiding combinatiescenario

Dit combinatiescenario komt voort uit de in de Trendanalyse 2024 gesignaleerde trend *technologiewedloop met technologie als machtsinstrument, wapen en kwetsbaarheid*. In het scenario zijn drie pijlers gecombineerd, te weten:

- Technologie: in het scenario is sprake van technologische dominantie van een *Big Tech*-bedrijf en worden grote stappen gezet in de implementatie van *Artificial Intelligence* (Kunstmatige Intelligentie, AI) in allerlei (overheids)systemen.

- Sociaal-maatschappelijk: transparantie (in de zin dat menselijk gedrag openbaar en zichtbaar zou moeten zijn) is in het scenario een leidend beginsel. De effecten van het scenario op sociaal-maatschappelijk niveau zijn onder meer polarisatie en wantrouwen.
- Overheid: publieke diensten zijn in het scenario goeddeels uitbesteed aan het *Big Tech*-bedrijf, waarbij de overheid grip op deze diensten verliest.

Deze drie pijlers zijn hieronder uitgewerkt in een fictief scenario. Het doel van dit scenario is om kwetsbaarheden ten aanzien van de afhankelijkheid van *Big Tech* te signaleren. Dit scenario is, hoewel voorstelbaar, een scenario dat nu onwaarschijnlijk lijkt. Tegelijkertijd is het van belang om door middel van het scenario na te denken over wat de vergaande gevolgen van een grote(re) macht van technologiebedrijven kunnen zijn op maatschappij en politiek.

3.2 **Het scenario: De duistere kanten van *Big Tech* – op aanvraag**

Voor professionals en inhoudelijke belanghebbenden is dit scenario op aanvraag beschikbaar.

3.3 **Wat als...?**

Bovenstaande scenario is een mogelijke uitwerking van de combinatie van een technologische dominantie van een *Big Tech*-bedrijf, transparantie in de samenleving en grootschalige uitbesteding van publieke diensten aan het *Big Tech*-bedrijf. Er zijn echter meerdere alternatieve uitwerkingen mogelijk. In deze paragraaf worden in de vorm van 'wat als' enkele van deze alternatieven weergegeven.

Wat als...?

Een bedrijf met niet-Westerse waarden een dergelijke cruciale positie krijgt in Europa?

Wat als...?

Door een grote cyberaanval geen toegang meer is tot overheidsdiensten in een dergelijke app?

Wat als...?

Nooddiensten (het 112 noodnummer) in Nederland worden geprivatiseerd?

Wat als...?

De onderliggende algoritmes van een dergelijk systeem kunnen worden gemanipuleerd door kwaadwillende actoren?

Wat als...?

Een dergelijk bedrijf ook cruciale diensten levert in het defensie- en veiligheidsdomein, op het gebied van AI-gedreven inlichtingenanalyse, waarmee bijvoorbeeld de inzet van politie en justitie wordt gestuurd?

3.4 **Beschouwing combinatiescenario De duistere kanten van *Big Tech***

In het combinatiescenario 'De duistere kanten van *Big Tech*' zorgen verschillende sluimerende ontwikkelingen voor zeer verstrekkende gevolgen voor de nationale veiligheid.

In het scenario wordt initieel door de Nederlandse overheid (vanuit een noodzaak grote crises het hoofd te bieden) bewust de keuze gemaakt om het *Big Tech*-bedrijf OpenSphere toe te laten in diverse publieke dienstverleningen. OpenSphere krijgt in het scenario steeds meer macht, waardoor een *lock-in* ontstaat. Omdat meer (toegang tot) data leidt tot betere AI-prestaties, komt er een dynamiek van concentratie op gang, waardoor een steeds kleiner aantal partijen steeds meer toegang heeft tot steeds meer data (Vorst, 2025). Dit heeft in het scenario aanzienlijke gevolgen voor de digitale veiligheid, die niet vergelijkbaar zijn met andere scenario's ten aanzien van digitale dreigingen (zie het themaraapport Cyberdreigingen). Het gaat hier namelijk om een structurele verandering in de manier waarop onder meer digitale dienstverlening vanuit de overheid wordt voorzien, die niet zomaar weer terug is te draaien. De impact op het impactcriterium digitale ruimte (en dus de nationale veiligheid) is dan ook structureel en niet tijdelijk.

Bovendien komt duidelijk de sociaal-maatschappelijke impact naar voren in dit scenario. Langzaam maar zeker heeft OpenSphere steeds meer elementen van het dagelijks leven overgenomen, waardoor de impact breed maatschappelijk gevoeld wordt. Initieel zal de impact op de fysieke veiligheid positief zijn: efficiëntere gezondheidszorg en in algemene zin minder criminaliteit, waardoor minder mensen sterven. Maar sluipenderwijs ervaren mensen in het scenario steeds meer druk om te voldoen aan de door OpenSphere gestelde norm, waardoor er sprake is van ernstig psychisch lijden door angst, onzekerheid, stress, burn-outklachten en gevoelens van vervreemding onder een groot deel van de bevolking. Recente onderzoeken laten al een klein nadelig verband zien (naast ook positieve effecten (Raad voor Volksgezondheid & Samenleving, 2025)) tussen het dagelijks functioneren van kinderen en het problematisch gebruik van sociale media (compulsief en verslavend) (Stichting KidsRights, 2025; Montag, et al., 2024; Boer, Stevens, Finkenauer, & van den Eijnden, 2022; Casale, Akbari, Seydavi, Bocci Benucci, & Fioravanti, 2023). In het scenario zijn deze nadelige gevolgen voor de mentale gezondheid sterker aangezet gezien de alomvattende invloed van OpenSphere op het dagelijks leven.

Tot slot laat het scenario zien dat er grote impact is op de democratische rechtsstaat. Beleidskeuzes worden gestuurd door algoritmes van OpenSphere, waardoor transparantie en democratische controle afnemen. Dit heeft een fundamentele en structurele impact op het functioneren van de democratische rechtsstaat, maar ook op het internationale multilaterale systeem. In het scenario worden internationale instituties langzaamaan vervangen door een alternatief *Big Tech*-systeem, waardoor het multilaterale bestel fundamenteel wordt ondermijnd. (Adviesraad Internationale Vraagstukken, 2025; Eerste Kamer der Staten-Generaal, 2025; Adriaanse, 2024).

3.4.1 *Kwetsbaarheden*

In het scenario worden ontwikkelingen op een dusdanige manier samengebracht dat er sprake is van een zeer vergaande systeemverandering. Dit lijkt een onvoorstelbaar en dystopisch beeld, maar het is van belang te onderkennen dat er nu al sprake is van grote ongewenste afhankelijkheden van diverse *Big Tech*-bedrijven. Bovendien is het belangrijk om de mogelijke risico's van die afhankelijkheden voor de toekomst te concretiseren.

3.4.1.1 *Ongewenste afhankelijkheden*

Steeds meer publieke en private processen zijn voor hun functioneren afhankelijk van private digitale dienstverlening. Deze uitbesteding aan private partijen is niet nieuw en hoeft op zichzelf ook geen ongewenste afhankelijkheid te creëren, zolang er een belangrijke mate van (publieke) controle is op deze processen. Bovendien kan (politiek) worden overwogen om afhankelijkheden toe te staan, omdat een proces, dienst of goed niet wordt gezien als 'strategisch' of 'sensitief' (Duijnhoven, Melman, & van Scheepstal, 2022).

Het scenario laat zien dat er op twee manieren geen controle meer is over de private partijen. Ten eerste leveren *Big Tech*-bedrijven (OpenSphere in het scenario) diensten gebaseerd op algoritmiek. Wanneer het niet (meer) duidelijk is op basis waarvan systemen keuzes maken en die keuzes niet transparant zijn, is er sprake van een beperking van de menselijke controle (European Union, 2024). Ten tweede, wanneer de overheid (bijvoorbeeld met het doel om kosten te besparen) steeds meer publieke diensten uitbesteedt, kan er een *lock-in* ontstaan. *Big Tech*-bedrijven bieden namelijk systemen en diensten aan die goed op elkaar aansluiten, maar niet altijd goed werken met diensten van andere bedrijven. Zo worden organisaties dus steeds meer gedwongen om van dezelfde aanbieder diensten te blijven afnemen en worden deze organisaties afhankelijker van een partij. Dit werkt niet alleen monopolievorming in de hand, maar levert op de lange termijn een kwetsbare afhankelijkheidspositie op (van Eeden, Karstens, Roolvink, & van Huijstee, 2025).

Deze afhankelijkheidspositie kan zeer nadelig uitpakken voor de afnemer in tijden van geopolitieke onrust. De 'thuisstaat' van het *Big Tech*-bedrijf kan namelijk de economische afhankelijkheidspositie uitbuiten en dreigen met het afsluiten van bepaalde diensten, het in beslag nemen van sensitieve of privacygevoelige data of zelfs tijdelijk daadwerkelijk de dienstverlening stopzetten. Zo hebben Amerikaanse sancties jegens het Internationaal Strafhof in Den Haag ertoe geleid dat Amerikaanse bedrijven in 2025 en 2026 meerdere medewerkers van het Strafhof uiteenlopende beperkingen hebben opgelegd. Er zijn financiële beperkingen (zoals geen toegang tot bankrekeningen en problemen bij internationale financiële transacties), digitale gevolgen (zoals beperking van toegang tot diensten van Amazon, Google en Microsoft) en visumintrekkingen (Alligood, 2026; Quell, 2025; Hartholt, 2025; van Trigt, Microsoft). Bovendien kan de Amerikaanse overheid onder voorwaarden eisen dat inzage wordt geboden in (persoons)gegevens van niet-Amerikanen die zijn opgeslagen op Amerikaanse clouddiensten. Amerikaanse (cloud)bedrijven zoals Amazon, Alphabet (Google) en Microsoft dienen zich namelijk te houden aan Amerikaanse wetgeving

zoals de Amerikaanse CLOUD Act en sectie 702 van de *Foreign Intelligence Surveillance Act* (FISA). Hoewel de waarschijnlijkheid dat daadwerkelijk gebruik wordt gemaakt van deze toegang tot gegevens als laag wordt geschat, staat deze wetgeving haaks op onder meer de Europese Algemene Verordening Gegevensbescherming (AVG) (van Eeden, Karstens, & van Huijstee, Koers zetten richting digitale autonomie. Handelingsopties voor beleidsmakers en inkopers, 2025). Tot slot zorgt de afhankelijkheid van een enkel bedrijf voor een toenemende kwetsbaarheid voor cyberaanvallen, zie ook het themaraapport Cyberdreigingen.

Zie bijvoorbeeld het scenario 'Aanval cloudbedrijf' (themaraapport *Cyberdreigingen*), waarin een supply-chain aanval op een aanbieder van clouddiensten door een statelijke actor wordt beschreven. Hierdoor vallen diensten van organisaties in diverse sectoren uit, inclusief vitale processen.

3.4.1.2 Digitale kwetsbaarheid

In een 'wat als' op het scenario is de bovenstaande kwetsbaarheid voor cyberaanvallen benoemd, evenals de mogelijkheid tot manipulatie van algoritmes onderliggend aan een systeem als dat van OpenSphere. Zo kunnen kwaadwillende actoren onder meer trainingsdata manipuleren of de input van het model, zodat het model bijvoorbeeld een uiting op sociale media verkeerd gaat classificeren. Ook kan worden geprobeerd om te achterhalen welke data zijn gebruikt om het model te trainen, om zo privacygevoelige informatie (zoals medische gegevens of profielen van personen in het scenario) te achterhalen. Dergelijke digitale kwetsbaarheden zijn van cruciaal belang te onderkennen, niet alleen in de context van een monopoliepositie van een *Big Tech*-bedrijf, maar ook in het algemeen. Immers, gegeven de digitalisering van de samenleving, worden steeds meer AI-(gebaseerde) systemen geïmplementeerd in allerlei (vitale) sectoren. De robuustheid en (cyber)veiligheid van deze systemen zijn daarom een belangrijk punt van aandacht, zeker omdat aanvalstechnieken vooruitlopen op verdedigingsmogelijkheden (Analistennetwerk Nationale Veiligheid, 2024; Brink, et al., 2023; Vassilev, et al., 2025).

3.4.1.3 Economische macht

Ook worden in het scenario allerlei datastromen samengebracht die het model van OpenSphere voeden. Dit levert niet alleen grote risico's op ten aanzien van privacyschending (TU Delft, sd), maar geeft het bedrijf ook een enorme macht. Immers, door het combineren van data kunnen nieuwe patronen worden ontdekt en daarmee de kennis over groepen en individuen worden vergroot (Austin, 2025). Bovendien, als bedrijven meer toegang krijgen tot data worden deze bedrijven dominanter en is het voor andere partijen moeilijker te concurreren (Amnesty International, 2025).

Deze monopolievorming zorgt ervoor dat *Big Tech*-bedrijven steeds machtiger worden, in sommige gevallen machtiger dan staten. Individuele CEO's van grote technologiebedrijven hebben in de afgelopen jaren al grote invloed gehad op het wereldtoneel. Zolang deze bedrijven meer macht naar zich toe kunnen trekken, reikt hun macht

steeds verder van economische macht naar ook (geo-)politieke macht (Amnesty International, 2025) (Khanal, Zhang, & Taeihagh, 2025) (Aiken, et al., 2025).

3.4.1.4 Versnippering

Onder meer in de Nederlandse Digitaliseringsstrategie wordt gesproken over de huidige versnippering van beleid ten aanzien van digitalisering en digitale veiligheid. Deze versnippering uit zich bijvoorbeeld in aparte aanpakken ten aanzien van clouddiensten en cyberveiligheid, digitale systemen die niet op elkaar aansluiten en beperkte coördinatie vanuit de overheid (Rijksoverheid, 2025). Ook zijn er veel verschillende wet- en regelgevingen ten aanzien van digitale veiligheid, zoals de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten, de Algemene Verordening Gegevensbescherming (AVG), de Digitaaldienstenverordening en de AI Verordening. In de Nederlandse Cybersecuritystrategie en de Nederlandse Digitaliseringsstrategie wordt daarom de noodzaak van een integrale aanpak voor digitale veiligheid benadrukt (NCTV, 2022) (Rijksoverheid, 2025).

Deze versnippering van beleid kan onder meer leiden tot een gebrek aan effectieve (centrale) coördinatie van handhaving van beleid. In het scenario worden bijvoorbeeld systemen ingezet door OpenSphere die onder meer de Europese AI Act expliciet verbiedt, zoals systemen bedoeld voor ‘*social scoring*’ en systemen ten behoeve van “*real time remote biometric identification*” (Future of Life Institute, 2024). Indien er geen overheidsbrede coördinatie plaatsvindt ten aanzien van de handhaving van regelgevingen, kunnen *Big Tech*-bedrijven pogen om door de mazen van de wet te kruipen. Bovendien, mocht er wel sprake zijn van handhaving, is het van belang te erkennen dat grote *Big Tech* bedrijven een enorme hoeveelheid middelen hebben om te procederen. Tot slot heeft de complexiteit van de verschillende Europese regelgevingen mogelijk het averechtse effect dat de juist kleinere concurrenten van *Big Tech* harder worden geraakt (de Gregorio & Demková, 2025) (Universiteit Leiden, 2026).

3.4.1.5 Vertrouwen in de overheid

Tot slot, in de aanleiding van het scenario wordt beschreven dat de Nederlandse overheid gebukt zou gaan onder een reeks grote crises die elkaar versterken: een economische recessie, een snel vergrijzende bevolking en hardnekkige tekorten in de publieke sector, met name in onderwijs en zorg. Daarbovenop komt de schaarste aan kritieke materialen en de steeds voelbaardere effecten van klimaatverandering. Deze ontwikkelingen zetten de overheid onder enorme druk om oplossingen te vinden en maken tegelijkertijd een efficiëntere werkwijze onvermijdelijk. Het publieke vertrouwen in de overheid om te komen met effectieve oplossingen om deze crises het hoofd te bieden is daardoor tot een kritiek punt gedaald in het scenario (van der Meer & den Ridder, 2025).

Dit maakt het aannemelijk dat de overheid op zoek gaat naar oplossingen aangeboden door private platforms. Burgers zijn dan mogelijk geneigd meer vertrouwen te hebben in deze bedrijven, zeker gezien de alomtegenwoordigheid van deze platforms in het dagelijks leven (Kool, et al., 2021).

3.4.2 *Handelingsperspectief*

Zoals al door meerdere (overheids)organisaties is gesignaleerd, is een langetermijnvisie en een Rijksbrede aanpak ten aanzien van het verminderen van digitale afhankelijkheden cruciaal. De focus moet verschuiven van *business continuity* naar *societal continuity*. Hierbij gaat het er niet zozeer om óf gebruik wordt gemaakt van (AI-)diensten van *Big Tech*, maar om de kaders die hierbij mee worden gegeven. Er dienen keuzes voor de lange termijn te worden gemaakt die mogelijk op de korte termijn economisch minder voordelig lijken.

Zo is versterking van strategische digitale autonomie cruciaal, onder meer door ontwikkeling en behoud van eigen (Europese) cloud-, data- en AI-capaciteiten en het stimuleren van interoperabiliteit en open standaarden om lock-in te voorkomen. Daarnaast vraagt dit om robuuste governance- en toezichtscapaciteit en versterkte handhaving op (Europese) regelgeving. Tegelijkertijd moet worden geïnvesteerd in cyberweerbaarheid en AI-veiligheid. Verder is een sterke Rijksbrede coördinatie en integrale beleidsvorming nodig om versnippering tegen te gaan en consistent op te treden richting *Big Tech*. Tot slot vereist dit een actieve inzet op internationale samenwerking en normstelling, gericht op het borgen van publieke waarden, het tegengaan van machtsconcentratie en het beschermen van het multilaterale systeem.

4 Literatuur

- Adriaanse, M. L. (2024, december 24). 'Big Tech heeft de democratische staat op feodale wijze aan zich onderworpen'. *NRC*. Retrieved from <https://www.nrc.nl/nieuws/2024/12/24/de-democratische-staat-wordt-op-feodale-wijze-onderworpen-door-big-tech-a4877735?t=1770713192>
- Adviesraad Internationale Vraagstukken. (2024). *Hybride dreigingen en maatschappelijke weerbaarheid*. Den Haag: Adviesraad Internationale Vraagstukken.
- Adviesraad Internationale Vraagstukken. (2025). *AI: technologie, macht en democratische waarden in het Nederlandse buitenlandbeleid*. Den Haag: AIV. Retrieved from <https://www.adviesraadinternationalevraagstukken.nl/site/binaries/site-content/collections/documents/2025/06/17/ai-technologie-macht-waarden/aiv-ai-technologie-macht-waarden-17jun2025-dt.pdf>
- Aiken, E., Allen, P., Baudin, A., Finkel, J., Fischer, E., Goldberg, L., . . . Schmollinger, R. (2025). *The Technopolar World: Do Tech Companies Matter as Geopolitical Actors?* Columbia University. Retrieved from <https://www.sipa.columbia.edu/sites/default/files/2025-06/Capstone%20Project%20SIPA%20-%20Eurasia%20Group%20%281%29.pdf>
- AIVD, MIVD. (2024). *Dreigingsbeeld militaire en hybride dreigingen*. Den Haag: AIVD, MIVD.
- AIVD, MIVD. (2026). *Tussen vrede en oorlog. De oorlog in Oekraïne en de Russische dreiging in Europa*. Den Haag: AIVD, MIVD. Retrieved from <https://www.aivd.nl/documenten/2026/02/19/tussen-vrede-en-oorlog.-de-oorlog-in-oekraïne-en-de-russische-dreiging-in-europa>
- AIVD, MIVD, NCTV. (2025). *Dreigingsbeeld Statelijke Actoren 2025: Aanhoudende dreigingen in tijden van groeiende onzekerheid*. Den Haag: AIVD, MIVD, NCTV.
- Algemene Rekenkamer. (2025). *Het Rijk in de cloud. Donkere wolken pakken samen*. Den Haag: Algemene Rekenkamer.
- Alligood, L. (2026, maart 16). *Sanctioning Justice: Trump's Clash with the ICC One Year On*. Retrieved from *Foreign Affairs Review*: <https://www.foreignaffairsreview.com/home/sanctioning-justice-trumps-clash-with-the-icc-one-year-on>
- Amnesty International. (2025). *Breaking up with Big Tech. A human-rights based argument for tackling Big Tech's market power*. Londen: Amnesty International. Retrieved from <https://www.amnesty.nl/content/uploads/2025/08/Breaking-Up-Big-Tech-Report.pdf?x90359>
- Analistennetwerk Nationale Veiligheid. (2024). *Trendanalyse Nationale Veiligheid 2024: Stapeling van dreigingen in tijden van onzekerheid*. ANV.
- Anghel, V. (2026). *Global risks to the EU 2026*. San Domenico di Fiesole: European University Institute.

- Austin, E. (2025, juli 16). *De realiteit van datamisbruik*. Retrieved from Bits of freedom: <https://www.bitsoffreedom.nl/2025/07/16/de-realiteit-van-datamisbruik/>
- Boer, M., Stevens, G. W., Finkenauer, C., & van den Eijnden, R. J. (2022). The course of problematic social media use in young adolescents: A latent class growth analysis. *Child Development*, 93(2). doi:10.1111/cdev.13712
- Brink, N., Kamphuis, Y., Maas, Y., Jansen-Ferdinandus, G., van Stijn, J., Poppink, B., . . . Chiscop, I. (2023). *Adversarial AI in the cyber domain*. The Hague: TNO.
- Casale, S., Akbari, M., Seydavi, M., Bocci Benucci, S., & Fioravanti, G. (2023). Has the prevalence of problematic social media use increased over the past seven years and since the start of the COVID-19 pandemic? A meta-analysis of the studies published since the development of the Bergen social media addiction scale. *Addictive Behaviors*, 147. doi:<https://doi.org/10.1016/j.addbeh.2023.107838>.
- de Bakker, E., van Kampen, L., & van Belkom, R. (2025). *Digitaal vervlochten, maar ook verbonden?* Den Haag: Sociaal en Cultureel Planbureau en Stichting Toekomstbeeld der Techniek.
- de Gregorio, G., & Demková, S. (2025, mei 19). *The Enforcement Dilemmas in Europe's Digital Rulebook*. Retrieved from Tech Policy.Press: <https://www.techpolicy.press/the-enforcement-dilemmas-in-europes-digital-rulebook/>
- de Moor, G., Boiten, M., & Stone, S. (2024). *Eindrapport - Alternatieven voor BigTech in het onderwijs*. Dialogic. Retrieved from <https://open.overheid.nl/documenten/d5e13904-9e52-4326-a5d5-dbd2bdcb8e24/file>
- De Toekomst Kamer. (2025). *Is onze kennis veilig in de toekomst?* Den Haag: Stichting Toekomstbeeld der Techniek.
- DNB, AFM. (2025). *Digitale afhankelijkheid in de financiële sector. Risico's, weerbaarheid en Europese autonomie*. Amsterdam: DNB, AFM. Retrieved from <https://www.dnb.nl/media/fmmnlf0m/brochure-atlas.pdf>
- Draghi, M. (2024). *The future of Europe's competitiveness*. Luxembourg: Publications Office of the European Union.
- Duijnhoven, H., Melman, I., & van Scheepstal, P. (2022). *Sensitieve Technologie*. Den Haag: TNO. Retrieved from <https://www.rivm.nl/sites/default/files/2022-09/Sensitieve%20Technologie.pdf>
- Eerste Kamer der Staten-Generaal. (2025, mei 27). *Deskundigen kritisch over Big Tech en de weerbaarheid van de democratische rechtsstaat*. Retrieved from Eerste Kamer der Staten-Generaal: https://www.eerstekamer.nl/nieuws/20250527/deskundigen_kritisch_over_big_tech
- European Commission. (2025). *European Preparedness Union Strategy*. Brussel: European Commission. Retrieved from https://www.eeas.europa.eu/eeas/preparedness-union-strategy_en
- European External Action Services. (2025). *3rd EEAS report on Foreign Information Manipulation and Interference Threats*. Brussel: EEAS. doi:<https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>

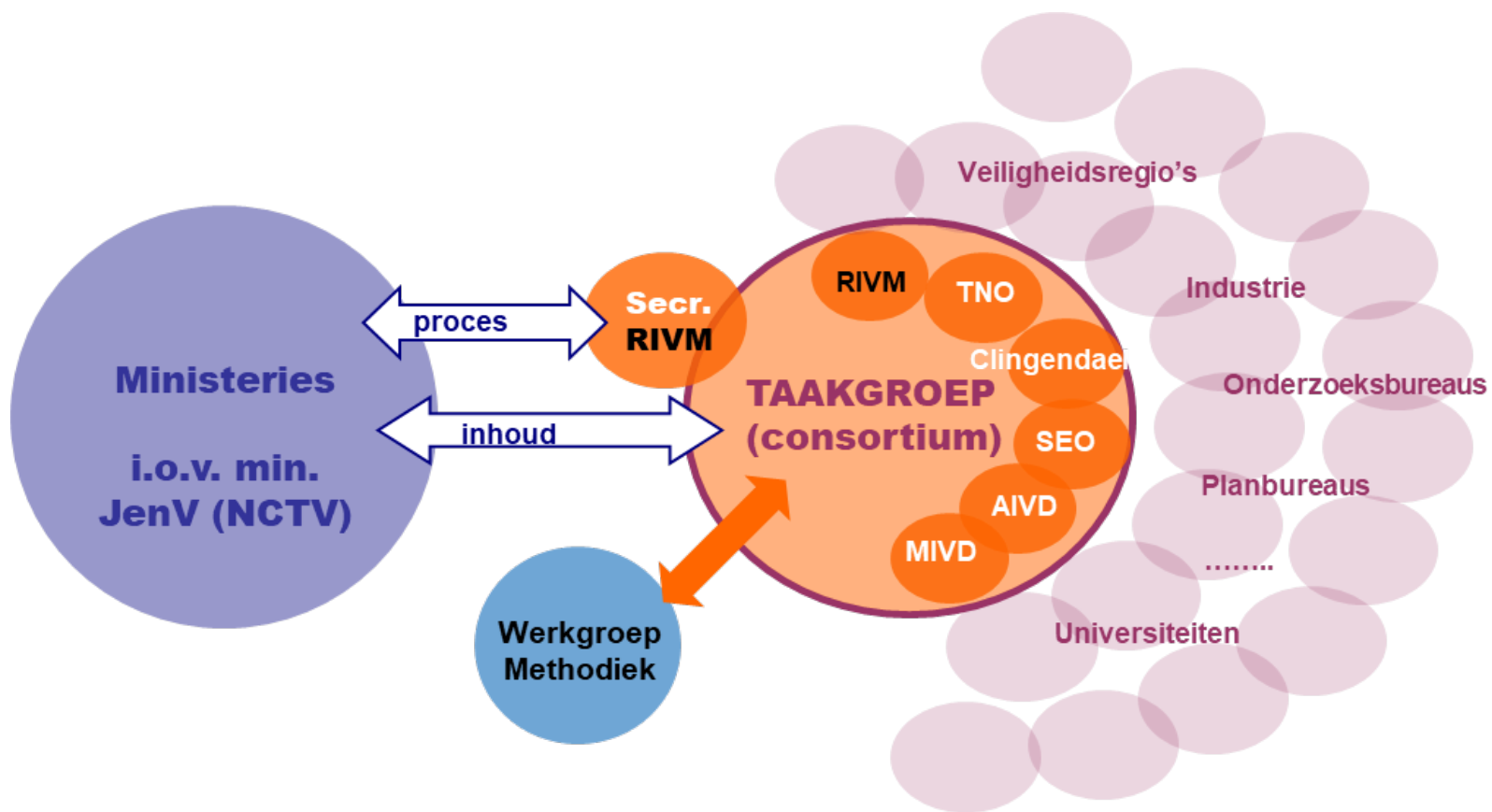
- European Union. (2024). *REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU Artificial Intelligence Act)*. Brussels: Official Journal of the European Union.
- Future of Life Institute. (2024). *High-level summary of the AI Act*. Future of Life Institute. Retrieved from <https://artificialintelligenceact.eu/high-level-summary/>
- Hahné, L. (2025). Beschikbaarheid van reservisten in een Artikel 5-scenario. *Militaire Spectator*.
- Hartholt, S. (2025, mei 19). *Wake-up call: Microsoft sluit e-mail ICC zonder pardon af*. Retrieved from Binnenlands Bestuur: <https://www.binnenlandsbestuur.nl/digitaal/wake-up-call-microsoft-sluit-e-mail-icc-zonder-pardon-af>
- Hubert, B. (2026). *Position paper Bert Hubert Rondetafelgesprek inzake de consequenties van de (beoogde) overname van Solvinity*.
- Khanal, S., Zhang, H., & Taeihagh, A. (2025). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, 44(1), 52–69. doi:<https://doi.org/10.1093/polsoc/puae012>
- Kool, E., Hamer, J., van Boheemen, P., Dekker, R., Deuten, J., van Est, R., . . . Verhoef, P. (2021). *De stand van digitaal Nederland. Naar zeggenschap en vertrouwen in de digitale samenleving*. Den Haag: Rathenau Instituut. Retrieved from https://www.rathenau.nl/sites/default/files/2021-09/Rapport_De_stand_van_digitaal_Nederland_Rathenau_Instituut.pdf
- Lysaght, H. (2025, oktober 13). *De 'just in time'-mentaliteit werkt niet als het oorlog wordt*. Retrieved from Universiteit Leiden: <https://www.universiteitleiden.nl/nieuws/2025/10/de-just-in-time-mentaliteit-werkt-niet-als-het-oorlog-wordt>
- Ministerie van Defensie. (2025). *Nationaal Programma Ruimte voor Defensie: Ruimte voor vrede, veiligheid en bescherming*. Den Haag.
- Ministerie van Defensie. (2025). *Onze mensen, onze toekomst; meer, beter en sneller*. Den Haag: Ministerie van Defensie.
- Ministerie van Defensie. (n.d.). *Host nation support voor troepenverplaatsingen*. Retrieved from Ministerie van Defensie: <https://www.defensie.nl/onderwerpen/internationale-samenwerking/host-nation-support>
- Ministerie van Justitie en Veiligheid. (2022). *Kader modernisering (staats)nood- en crisisrecht*. Den Haag: Ministerie van Justitie en Veiligheid. Retrieved from <https://www.nctv.nl/site/binaries/site-content/collections/documents/2022/12/06/kader-modernisering-staatsnoodrecht/Kader+modernisering+%28staats%29nood+en+crisisrecht.pdf>
- Ministerie van Justitie en Veiligheid. (2025). *Regels ter implementatie van Richtlijn (EU) 2022/2557 van het Europees Parlement en de 2022/2557 van het Europees Parlement en de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PbEU 2022, L 333)*. Den Haag: Tweede Kamer der Staten-Generaal.
- Ministerie van Justitie en Veiligheid, Ministerie van Defensie. (2025). *Maatschappelijke Weerbaarheid en Militaire Paraatheid tegen*

- Militaire en Hybride Dreigingen (Kamerbrief 30 821, nr. 304).*
Tweede Kamer der Staten-Generaal.
- MIVD. (2025). *Openbaar jaarverslag 2024*. Den Haag: Ministerie van Defensie.
- Montag, C., Demetrovics, Z., Elhai, J., Grant, D., Koning, I., Rumpf, H.-J., . . . van den Eijnden, R. (2024). Problematic social media use in childhood and adolescence. *Addictive Behaviors*, 153. doi:<https://doi.org/10.1016/j.addbeh.2024.107980>
- NATO. (2022). *NATO 2022 Strategic Concept*. NATO. Retrieved from <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>
- NATO. (2024, november 13). *Resilience, civil preparedness and Article 3*. Retrieved from NATO: <https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>
- NATO. (2025, april 2). *NATO Force Model*. Retrieved from NATO: <https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-force-model>
- NCTV. (2022). *Nederlandse Cybersecuritystrategie 2022-2028*. Den Haag: NCTV. Retrieved from <https://www.nctv.nl/documenten/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028>
- NCTV. (2025, juli 11). *RCB: Zorgen onder Nederlanders over geopolitieke en militaire dreigingen in 2025 flink gestegen*. Retrieved from NCTV: <https://www.nctv.nl/actueel/nieuws/2025/07/11/rcb-zorgen-onder-nederlanders-over-geopolitieke-en-militaire-dreigingen-in-2025-flink-gestegen>
- NCTV. (n.d.). *Wet weerbaarheid kritieke entiteiten*. Retrieved from NCTV: <https://www.nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten>
- NCTV. (n.d.). *Wetsvoorstellen in ontwikkeling*. Retrieved from NCTV: <https://www.nctv.nl/onderwerpen/w/wet-weerbaarheid-kritieke-entiteiten/wetsvoorstellen-in-ontwikkeling>
- NCTV, Ministerie van Defensie. (2024). *Weerbaarheidsopgave: Versterken van weerbaarheid in het licht van militaire en hybride dreigingen*. Rijksoverheid.
- Niinistö, S. (2024). *Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness*. Brussel: European Commission. Retrieved from https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf
- Overlegorgaan Fysieke Leefomgeving. (2025). *Tijd om te handelen: De weerbaarheidsopgave van het Nederlandse spoor*. Den Haag.
- Patterson, R. (2025). *NATO's Future Russia Strategy*. NATO Defence and Security Committee. Retrieved from <https://www.nato-pa.int/download-file?filename=/sites/default/files/2025-10/013%20DSC%2025%20E%20rev.%203%20fin%20-%20NATO%27S%20RUSSIA%20STRATEGY%20-%20PATTERSON%20REPORT.pdf>
- Quell, M. (2025, December 12). *Cut off by their banks and even iced out by Alexa, sanctioned ICC staffers remain resolute*. Retrieved from

- AP News: <https://apnews.com/article/international-court-sanctions-trump-icc-hague-4cdefe4de067432f6cdb9b137908c463>
- Raad voor Volksgezondheid & Samenleving. (2025). *Op de rem! Voorbij de hypernerveuze samenleving*. Den Haag: Raad voor Volksgezondheid & Samenleving.
- Rijksoverheid. (2025). *De Nederlandse Digitaliseringsstrategie. Samen versnellen*. Den Haag: Rijksoverheid. Retrieved from <https://open.overheid.nl/documenten/51bf0136-69cc-4d37-90c9-64d7ed3d9a5c/file>
- Rijksoverheid. (2025). *Denk vooruit*. Retrieved from Denk vooruit: <https://www.denkvooruit.nl/>
- Schaake, M. (2025). *Position Paper Deskundigenbijeenkomst Big Tech en de Weerbaarheid van de Democratische Rechtsstaat*. Stanford University.
- Sie Dhian Ho, M., Elchardus, M., Houtkamp, C., van der Laan, T., & Wessel, N. (2025). *Tussen hoop en vrees: Nederlanders één in vrees voor hybride dreigingen en oorlog te midden van voortdurende grote verdeeldheid*. Den Haag: Clingendael.
- Sociaal-Economische Raad. (2023). *Waardevol werk: publieke dienstverlening onder druk. Oplossingsrichtingen voor de arbeidsmarktkrapte*. Den Haag: SER. Retrieved from <https://www.ser.nl/-/media/ser/downloads/adviezen/2023/arbeidsmarktkrapte-publieke-sectoren.pdf>
- Stichting KidsRights. (2025). *The KidsRights Index 2025*. Amsterdam: Stichting KidsRights. Retrieved from <https://files.kidsrights.org/wp-content/uploads/sites/6/2025/06/11000023/KidsRights-Index-2025-Report.pdf>
- Stikker, M. (2025). *Big Tech en de weerbaarheid van de democratische rechtsstaat - Position paper Deskundigenbijeenkomst Eerste Kamer*. Waag Futurelab.
- TU Delft. (n.d.). *Ten strijde tegen de datahonger van big tech*. Retrieved from TUDelft: <https://www.tudelft.nl/stories/articles/ten-strijde-tegen-de-datahonger-van-big-tech>
- Universiteit Leiden. (2026, januari 6). *Big Tech is een van de grote vraagstukken van deze tijd*. Retrieved from Universiteit Leiden: <https://www.universiteitleiden.nl/in-de-media/2026/01/big-tech-is-een-van-de-grote-vraagstukken-van-deze-tijd>
- van der Meer, T., & den Ridder, J. (2025). *Vertrouwen in de politiek*. Parlement en Wetenschap. Retrieved from <https://www.scp.nl/documenten/2025/09/26/kennisnotitie-vertrouwen-in-de-politiek>
- van Eeden, Q., Karstens, B., & van Huijstee, M. (2025). *Koers zetten richting digitale autonomie. Handelingsopties voor beleidsmakers en inkoopers*. Den Haag: Rathenau Instituut. Retrieved from https://www.rathenau.nl/sites/default/files/2025-07/Koers_zetten_richting_digitale_autonomie_Rathenau_Instituut.pdf
- van Eeden, Q., Karstens, B., Roolvink, S., & van Huijstee, M. (2025). *Achter de macht van big tech. Verklarende factoren voor digitale macht*. Den Haag: Rathenau Instituut. Retrieved from <https://www.rathenau.nl/sites/default/files/2025->

- 07/Achter_de_macht_van_big_tech_Rapport_Rathenau_Instituut .pdf
- van Trigt, M. (2025, oktober 31). *Internationaal Strafhof neemt afscheid van Microsoft 365*. Retrieved from Binnenlands Bestuur: <https://www.binnenlandsbestuur.nl/digitaal/internationaal-strafhof-neemt-afschied-van-microsoft-365>
- van Trigt, M. (2025, mei 20). *Microsoft: 'Geen diensten aan ICC-organisatie gestopt'*. Retrieved from Binnenlands Bestuur: <https://www.binnenlandsbestuur.nl/digitaal/microsoft-geen-diensten-aan-icc-organisatie-gestopt>
- van Vark, A. (2025). *Separation and immersion: the changing role of the armed forces in Northwestern liberal democracies*. Leiden: Universiteit Leiden.
- Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). *Adversarial Machine Learning. A Taxonomy and Terminology of Attacks and Mitigations*. Gaithersburg: National Institute of Standards and Technology.
doi:<https://doi.org/10.6028/NIST.AI.100-2e2025>
- Verlinden, M. (2025). Wederkerigheid in civiel-militaire samenwerking. *Militaire Spectator*. Retrieved from <https://militairespectator.nl/artikelen/wederkerigheid-civiel-militaire-samenwerking>
- Vorst, R. v. (2025, november 26). Het einde van de markteconomie. *Financieel Dagblad*. Retrieved from <https://fd.nl/opinie/1578478/het-einde-van-de-markteconomie>
- Wetenschappelijke Raad voor het Regeringsbeleid. (2019). *Vorbereiden op digitale ontvricting*. Den Haag: WRR.

Bijlage 1 Samenstelling Analistennetwerk Nationale Veiligheid



Analistennetwerk Nationale Veiligheid

Dit is een uitgave van:

Het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)
Nederlandse Organisatie voor toegepast-
natuurwetenschappelijk onderzoek (TNO)
Stichting Nederlands Instituut voor Internationale
Betrekkingen 'Clingendael' (Clingendael)
SEO Economisch Onderzoek (SEO)
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

juli 2026