Rijksbrede Risicoanalyse Nationale Veiligheid 2026

Themarapport Cyberdreigingen

Rijksbrede Risicoanalyse Nationale Veiligheid 2026

Themarapport Cyberdreigingen

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, Themarapport Cyberdreigingen.

Contact:
anv@rivm.nl

De Rijksbrede Risicoanalyse Nationale Veiligheid 2026, Themarapport Cyberdreigingen 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 — 9
2.1 Nationale veiligheidsbelangen — 9
2.2 Scenario's — 12
2.2.1 Enkelvoudige scenario's — 12
2.2.2 Combinatiescenario's — 13
2.3 Resultaten en beschouwing — 15
2.4 Geografische reikwijdte — 15

3 Cyberdreigingen — 17
3.1 Inleiding — 18
3.1.1 Bouwstenen — 18
3.2 Dreigingscategorie Verstoren functioneren internet — 20
3.2.1 Het scenario ‘Aanval cloudbedrijf’ — 21
3.2.2 Het scenario ‘Misconfiguratie bij groot technologiebedrijf’ — 26
3.2.3 Beschouwing Verstoren functioneren internet — 32
3.3 Dreigingscategorie verstoren cyber-fysieke systemen — 33
3.3.1 Het scenario ‘Cyberincident Regionale Energievoorziening - op aanvraag — 33
3.3.2 Beschouwing verstoren cyber-fysieke systemen — 34
3.4 Slotbeschouwing thema cyberdreigingen — 35
3.4.1 De impact en waarschijnlijkheid van Cyberdreigingen — 35
3.4.2 Impact ontwikkelingen — 36
3.4.3 Kwetsbaarheden — 38

4 Literatuur — 41

Bijlage 1 Samenstelling Analistennetwerk Nationale Veiligheid — 45

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 kerngebeurtenissen 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 themarapporten:

- Themarapport combinatiescenario Water, een zegen of een vloek?;
- Themarapport combinatiescenario De duistere kanten van Big Tech;
- Themarapport combinatiescenario Oorlog in Europa;
- Themarapport combinatiescenario Sanctiepolitiek tegen geïsoleerd Nederland;
- Themarapport Klimaat- en natuurrampen;
- Themarapport Infectieziekten;
- Themarapport Zware ongevallen;
- Themarapport Polarisatie, extremisme en terrorisme;
- Themarapport Ongewenste inmenging en beïnvloeding democratische rechtsstaat;
- Themarapport Internationale en militaire dreigingen;
- Themarapport Economische dreigingen;
- Themarapport 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 scheepvaartafwikkeling[1] — worden nu explicieter weergegeven in de scenario's.

De themarapporten 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 themarapport zijn de verschillende enkelvoudige scenario's over het Themarapport Cyberdreigingen weergegeven. Het themarapport 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 enkelvoudige scenario's ook de waarschijnlijkheid is uitgevoerd. In het tweede onderdeel wordt ingegaan op de uitgewerkte scenario's. Allereerst volgt een algemene introductie op het thema en de dreigingscategorieën die onder het thema vallen. Vervolgens worden de verschillende dreigingscategorieën inhoudelijk besproken. Per dreigingscategorie worden relevante factoren besproken; de bouwstenen

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

op basis waarvan een scenario opgebouwd kan worden. Daarna volgen de verhaallijnen van de fictieve scenario's die zijn beoordeeld op impact en waarschijnlijkheid en een beschouwing per dreigingscategorie. Elk thema wordt afgesloten met een slotbeschouwing waarin een reflectie wordt gegeven op de implicaties van het thema als geheel voor de nationale veiligheid (zoals ook opgenomen in het Hoofdrapport). Ook wordt hier het risicodiagram voor het thema weergegeven.

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

Veiligheidsbelang	*Impactcriteria*
	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

Klasse van gevolgen	*Voorbeeld criterium: Aantal doden (2.1)*	*Voorbeeld criterium: Kosten (3.1)*
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

Klasse van waarschijnlijkheid	*Kwantitatieve inschatting niet-moedwillige dreiging in % per 5 jaar*	*Kwalitatieve omschrijving moedwillige dreiging*
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

Klasse van waarschijnlijkheid	*Kwantitatieve inschatting niet-moedwillige dreiging in % per 5 jaar*	*Kwalitatieve omschrijving moedwillige dreiging*
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 voorzieningen[3]**
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	Zeer 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 km^2**		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 grondoorzaken 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 Cyberdreigingen

3.1 Inleiding

Digitale systemen worden steeds complexer en ze raken steeds dieper verweven in onze samenleving. Een duidelijk onderscheid tussen het fysieke en digitale domein is hierdoor nauwelijks meer te maken. Deze verwevenheid brengt kwetsbaarheden met zich mee voor de nationale veiligheid: digitale systemen kunnen zowel het doelwit als middel zijn van aanvallen. Daarnaast kunnen niet-moedwillige verstoringen ontstaan door uiteenlopende zaken, zoals natuurrampen, technische storingen of menselijke fouten. Veel van deze oorzaken worden ook geadresseerd in andere thema's van de Rijksbrede Risicoanalyse, wat de urgentie van digitale dreigingen benadrukt.

In het digitale dreigingslandschap mengen zich steeds meer verschillende actoren. Cyberaanvallen worden onder meer gericht ingezet door statelijke actoren ten behoeve van geopolitieke doeleinden. Naast statelijke actoren maken ook steeds vaker *proxies*, criminele groeperingen of ingehuurde hackers, gebruik van cyberaanvallen. Hierbij is het vaak moeilijk te duiden wat de relatie is tussen deze groeperingen en statelijke actoren. Deze veranderende geopolitieke verhoudingen zorgen ervoor dat digitale afhankelijkheden een groter risico gaan vormen voor de nationale veiligheid (CSBN, 2025). Daarnaast maken technologische ontwikkelingen dat cyberaanvallen gerichter, op grotere schaal en gemakkelijker kunnen worden uitgevoerd.

In het thema *Cyberdreigingen* worden verschillende typen kwetsbaarheden samengebracht die specifiek voortkomen uit de digitalisering van de samenleving. Het dreigingsthema *Cyberdreigingen* omvat twee dreigingscategorieën; 'Verstoren functioneren internet' en 'Verstoren cyber-fysieke systemen'. Elke categorie bevat verschillende scenario's die de dreigingen illustreren.

In de eerste dreigingscategorie, verstoring functioneren internet, staat telkens een gebeurtenis centraal die ervoor zorgt dat de toegang of werking van het internet en internetdiensten belemmerd wordt. De tweede dreigingscategorie, verstoring cyber-fysieke systemen, richt zich op kwetsbaarheden die ontstaan door toenemende digitalisering van fysieke processen. De focus ligt in de uitgewerkte scenario's op het Europese deel van het Koninkrijk. Dit neemt echter niet weg dat deze dreigingen ook op het Caribisch deel van het Koninkrijk kunnen voorkomen.

3.1.1 Bouwstenen

Binnen het thema cyberdreigingen zijn er verschillende factoren van invloed op de ernst en waarschijnlijkheid van een gebeurtenis. Deze bouwstenen zijn in onderstaande tabel weergegeven en zijn voor beide dreigingscategorieën gelijk.

Tabel 5 Bouwstenen 'Verstoren functioneren Internet' en 'Verstoren cyber-fysieke systemen[4]

Oorzaak	Actor	Element	Middelen	Aard van de aantasting	Getroffenen (direct)	Getroffenen (keten-effecten)	Doordringingsgraad
Technisch falen	Criminelen	DNS (rootservers, name servers, DNS operators)	Distributed Denial of Service (DDoS)	Aantasting van beschikbaarheid	Vitale aanbieders	Vitale aanbieders	Klein deel van de betreffende categorieën is getroffen (<10%)
Menselijk falen	Statelijke actoren	BGP (routing tables)	Misconfiguratie	Aantasting van integriteit	Rijksoverheid	Rijksoverheid	Aanzienlijk deel van de betreffende categorieën is getroffen (10-50%)
Moedwillig	Extremisten	NTP	Fysieke aantasting (explosie, kabel stuk, etc.)	Aantasting van vertrouwelijkheid	Digitale dienstverleners	Digitale dienstverleners	Merendeel van de betreffende categorieën is getroffen is getroffen (>50%)
	cyber-vandalen en script-kiddies	Internet infrastructuur (e.g. kabels, IXen, datacenters)	Malware infectie (inclusief ransomware)		Topsectoren	Topsectoren	
	Hacktivisten	Vertrouwensdiensten (e.g. certificaten, public key infrastructure)	Misbruik van kwetsbaarheden		Kennisinstellingen	Kennisinstellingen	
	Interne actoren		Social engineering (incl. phishing)		Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	
	Private organisaties				Burgers	Burgers	

De **oorzaak** kan een moedwillige of niet-moedwillige aard hebben (waarbij nog onderscheid gemaakt kan worden tussen technisch of menselijk falen). Voor moedwillige gebeurtenissen is het van belang om onderscheid te maken tussen verschillende typen **actoren** en het motief dat zij hebben om een aanval uit te voeren. De aantasting kan betrekking hebben op verschillende **elementen** die een rol spelen bij

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

het functioneren van het Internet, hoewel er ook sprake kan zijn van een combinatie van elementen die aangetast worden. De manier waarop de aantasting ontstaat heeft voorts te maken met de (combinatie van) **middelen** die gebruikt worden of optreden (misconfiguratie of fysieke aantasting kan zowel een moedwillig als niet-moedwillige aanleiding hebben). Ook hiervoor geldt dat in de praktijk vaak een combinatie van verschillende middelen een rol speelt in een gebeurtenis.

Als het gaat om de impact van een gebeurtenis wordt onderscheid gemaakt in de **aard van de aantasting** (beschikbaarheid, integriteit of vertrouwelijkheid), waarbij het in deze dreigingscategorie veelal zal gaan om beschikbaarheid, eventueel in combinatie met andere vormen van aantasting. Verder kan de aantasting verschillende categorieën van organisaties treffen, waarbij het ook relevant kan zijn om onderscheid te maken tussen direct **getroffen partijen** en partijen die in tweede orde getroffen worden (bijvoorbeeld in geval van een supply chain aanval). De omvang en ernst van een aantasting van het functioneren van het internet is verder lastig in concrete factoren uit te drukken omdat dit heel erg afhangt van het type situatie. De **doordringingsgraad** (mate van verspreiding binnen en tussen categorieën van getroffen partijen) en duur van de aantasting zijn twee belangrijke factoren die van invloed zijn op de ernst van de impact.

3.2 Dreigingscategorie Verstoren functioneren internet

Internet en internetdiensten zijn cruciaal in de Nederlandse samenleving. Onder meer door de toenemende verwevenheid van digitale processen in het dagelijks leven, kan een verstoring van deze infrastructuur grote maatschappelijke gevolgen hebben. Om deze reden is het van belang om zicht te houden op gebeurtenissen die het functioneren van het internet kunnen verstoren evenals de potentiële gevolgen van deze gebeurtenissen voor de samenleving.

Deze dreigingscategorie richt zich op de beschikbaarheid, de integriteit en de vertrouwelijkheid van internet en internetdiensten. Het gaat hierbij om incidenten die ervoor zorgen dat het functioneren van deze infrastructuur wordt aangetast, zowel door technisch of menselijk falen als door moedwillige handelingen. De dreigingen die in deze categorie worden geanalyseerd zijn gerelateerd aan de manier waarop internet en internetdiensten zijn ingericht en de elementen die een rol spelen bij het functioneren van het internet. Hierbij wordt voortgebouwd op de scenario’s uit de Rijksbrede risicoanalyse van 2022.

In deze dreigingscategorie wordt één scenario beschreven waarin verstoring van het functioneren van Internet centraal staat. In het combinatiescenario “De duistere kanten van Big Tech” wordt verder ingegaan op de kwetsbaarheden die de digitale veiligheid in het geding brengen. Het grote verschil is dat het in het combinatiescenario niet gaat om een incident, maar om structurele verandering in de manier waarop digitale dienstverlening vanuit de overheid wordt voorzien. Daarnaast komt in het combinatiescenario de sociaal-maatschappelijke impact nog duidelijker naar voren.

3.2.1 *Het scenario 'Aanval cloudbedrijf'*

Al een aantal jaar waarschuwen verschillende (overheids-)instanties voor het grootschalig in gebruik nemen van clouddiensten van grote buitenlandse technologiebedrijven (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2011; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025; Digitale Overheid, 2025; Algemene Rekenkamer, 2025). De cloud kan worden gezien als een onlinenetwerk van servers met bestanden of applicaties. Via het internet kan men verbinding maken met die servers en daar allerlei bestanden en applicaties op opslaan. Het voordeel is dat je met een internetverbinding altijd toegang hebt tot deze servers (NCSC).

Vanwege de steeds grotere rol van clouddiensten in het internetlandschap is ervoor gekozen om een scenario uit te werken dat betrekking heeft op een leverancier van clouddiensten (*Cloud Service Provider*, CSP). Het scenario betreft een moedwillige aanval op een CSP die veel wordt gebruikt in Nederland door overheden, bedrijven en burgers. De aanvallers voeren hierbij een *supply chain*- aanval uit (waarbij de verspreiding van de aanval plaatsvindt via een toeleveranciersketen (ANV, 2022)) met als gevolg een crash van de CSP. De crash raakt een deel van de Nederlandse klanten van de CSP en kan, afhankelijk van de specifieke configuratie van de clouddiensten die klanten afnemen, leiden tot het tijdelijk niet beschikbaar zijn van clouddiensten, verlies van data en ongewenste toegang tot data door de aanvallers (CBS, 2025).

Het scenario beschrijft een grootschalige verstoring van de clouddienst veroorzaakt door een statelijke actor met zowel een geopolitiek als economisch motief (Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2024). In het scenario zorgt spionage in combinatie met een aanval voor schade aan verschillende processen, waardoor organisaties niet meer bij gegevens kunnen komen terwijl deze wel kunnen worden ingezien door de statelijke actor.

De impact van aanvallen op clouddiensten is moeilijk in te schatten omdat dit sterk afhangt van de manier waarop afnemers clouddiensten inrichten en gebruiken, en of er mitigatiemaatregelen zijn getroffen die het verlies van gegevens kunnen voorkomen. Doordat steeds meer IT-functionaliteiten en software naar de Cloud verhuizen, wordt de afhankelijkheid groter. Dit maakt dat de impact van een aanval op een Cloud Service Provider toeneemt (Schellevis, 2024; Schellevis, 2026; de Koning, 2025).

In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario Aanval cloudbedrijf gebaseerd is.

Tabel 6 Bepalende bouwstenen voor het scenario 'Aanval cloudbedrijf'

Oorzaak	Actor	Element	Middelen	Aard van de aantasting	Getroffenen (direct)	Getroffenen (keten-effecten)	Doordringingsgraad
Moedwillig	Statelijke actoren	Internet infrastructuur (e.g. kabels, IX-en, datacenters)	*Supply chain*-aanval	Aantasting van beschikbaarheid	Digitale dienstverlener	Vitale aanbieder	Een aanzienlijk deel van de betreffende categorieën is getroffen, 60-75%.
			Misbruik van kwetsbaarheden	Aantasting van vertrouwelijkheid		Rijksoverheid	
				Aard van de Integriteit		Digitale dienstverleners	
						Topsectoren	
						Kennisinstelling	
						Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB)	
						Burgers	

3.2.1.1 Scenario: Aanval cloudbedrijf

Op een doordeweekse avond valt een groot deel van de systemen van de CSP Cirrocumulus Networks (een niet-Europese clouddienst) in Nederland uit. Overheidsinstellingen, zorgorganisaties, onderwijsinstellingen en bedrijven die afhankelijk zijn van Cirrocumulus Networks kunnen niet meer inloggen, communiceren of toegang krijgen tot hun bestanden. De storing lijkt technisch van aard, maar na een dag blijkt dat het om een moedwillige aanval gaat door een statelijke actor met toegang tot kritieke onderdelen van het Cloud platform. Het blijkt om spionage te gaan gecombineerd met een cyberaanval met als gevolg ook schade aan systemen en processen, waardoor bredere verstoringen merkbaar worden. Opvallend is dat dit gebeurt in een periode waarin er

al eerder berichten naar buiten zijn gekomen over verdachte activiteiten in de Cloud omgeving van meerdere klanten van Cirrocumulus Networks.

De gevolgen zijn verstrekkend: gemeenten kunnen geen uitkeringen verwerken, ziekenhuizen hebben geen toegang tot patiëntendossiers en scholen kunnen hun digitale lesomgevingen niet gebruiken. Ook de communicatie tussen ministeries, de inlichtingen- en veiligheidsdiensten, de politie en het Nationaal Cyber Security Centrum (NCSC) verloopt stroef, waardoor vertraging ontstaat in besluitvorming over de reactie op de uitval van het Cloud platform. Burgers en bedrijven ervaren de impact direct: van niet-werkende DigiD-portalen tot het stilvallen van een deel van de bedrijfsprocessen. De afhankelijkheid van één Cloud leverancier wordt pijnlijk zichtbaar en dat geeft grote maatschappelijke onrust, onder andere op sociale media.

Na ongeveer 24 uur komt Cirrocumulus naar buiten met de mededeling dat er sprake is van een geavanceerde cyberaanval gericht tegen de data van bedrijven in Nederland, waardoor een groot deel van de Nederlandse CSP-gebruikers geraakt is. Cirrocumulus Networks doet er alles aan om de dienstverlening zo snel mogelijk weer te herstellen. Het zal enkele uren tot een dag duren om weer operationeel te zijn. Maar het kan enkele weken duren om alle functionaliteiten weer te laten werken, afhankelijk van de specifieke situatie van de getroffen gebruikers.

In de Kamer ontstaat wederom discussie over de concentratie van digitale infrastructuur bij grote technologiebedrijven en het gebrek aan regie over vitale cloudvoorzieningen. Experts pleiten opnieuw voor een versnelling van de ontwikkeling van een Europese cloud en betere monitoring van digitale afhankelijkheden. Het incident fungeert als wake-up call: digitale autonomie is niet alleen een technische kwestie, maar een strategische noodzaak.

In de weken die volgen komt langzaam meer informatie over het incident naar buiten. Het lijkt erop dat het om een *supply chain*-aanval gaat. Aanvallers hebben namelijk via een derde partij toegang gekregen tot het Cloud platform door misbruik te maken van veelgebruikte software. In deze aanval werd vermoedelijk gebruik gemaakt van een gecompromitteerde softwarecomponent binnen een legitieme updateketen, waardoor de aanvallers toegang konden krijgen tot systemen van Cirrocumulus Networks.
Voor het herstel van de dienstverlening heeft Cirrocumulus Networks verschillende activiteiten opgezet. Allereerst werden alle getroffen klanten geïnformeerd en voorzien van herstelinstructies. Vervolgens wordt er ook bepaald of nadere analyse nodig is om te bepalen of gegevens, waar ten tijde van de crash aan gewerkt werd, hersteld moeten en kunnen worden. Dit hangt af van de configuratie van het Cloud platform van een gebruiker en het type werkzaamheden dat de klant op de getroffen systemen uitvoert. Het wordt duidelijk dat voor een aanzienlijk deel van de organisaties, inclusief organisaties in vitale sectoren, herstelinstructies nodig zijn. Voor klanten waarvan (een deel van) de software gereset kunnen worden, geldt dat zij enkele minuten of maximaal een paar uur nadat de systemen gereset worden weer de

beschikking hebben over hun Cloud platform. Bij gebruikers waar nader onderzoek nodig is, kan dit dagen of zelfs enkele weken duren.

3.2.1.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario 'Aanval cloudbedrijf'.

Tabel 7 Beoordelingstabel scenario 'Aanval cloudbedrijf

Thema	**Cyberdreigingen**
Dreigingscategorie	Verstoring functioneren internet
Scenario	Aanval cloudbedrijf
Scenariotoelichting	Dit scenario beschrijft een supply-chain aanval door een statelijke actor, waarbij een cloudserver wordt uitgeschakeld. Hierdoor vallen diensten van organisaties in diverse sectoren uit, inclusief vitale processen. Het herstel duurt tussen de 2 en 6 dagen.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	D	De gebeurtenissen zijn voorstelbaar en gezien de geopolitieke ontwikkelingen zijn er ook steeds meer redenen om aan te nemen dat de hoeveelheid aanvallen toeneemt. Het is daarom niet ondenkbaar dat een aanval gericht op Nederland zal gebeuren en het is lastig om hier effectieve maatregelen tegen te treffen.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	B	Dit criterium is van toepassing vanwege de vierde categorie: Gewelddadige en/of ondermijnende acties door buitenlandse actoren in Nederland. Het gaat hier namelijk om een cyberaanval van grote omvang en omvangrijke schaal. Hierbij is Nederland onvoldoende snel en effectief met deze crisis omgegaan.
	1.3 Informatie en digitale ruimte	E	In het scenario wordt beschreven hoe een groot aantal organisaties, waaronder vitale aanbieders en overheidsinstanties, wordt getroffen. De verstoring is omvangrijk en wordt toegeschreven aan een statelijke actor met als doel spionage en sabotage voor geopolitiek gewin. Er is enige grip op de storing, gezien de relatief snelle duiding van de situatie. Gezien de catastrofale schending, valt het in klasse E.
	1.4 Grondgebied EU en NAVO lidstaten	0	Niet van toepassing.
Fysiek	2.1 Doden	A	Het is niet ondenkbaar dat er doden vallen door verstoring van het Cloud netwerk. Denk aan patiëntendossiers die tijdelijk niet beschikbaar

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			zijn en patiënten die onvoldoende/verkeerde medicatie innemen.
	2.2 Ernstig gewonden en chronisch zieken	A	Hier geldt dezelfde redenering als bij bovenstaand criterium: Het is niet ondenkbaar dat er ernstig gewonden en chronisch zieken ontstaan door verstoring van het Cloud netwerk wanneer specifieke organisaties worden geraakt. Denk aan patiëntendossiers die tijdelijk niet beschikbaar zijn en patiënten die onvoldoende/verkeerde medicatie innemen.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing. De duur van de verstoring is voor de meeste gebruikers relatief kort.
Economisch	3.1 Kosten	B	Door de aanval op de CSP worden veel bedrijven, onderwijs-, zorg- en overheidsinstellingen getroffen. Ziekenhuizen hebben geen toegang meer tot patiëntendossiers, wat leidt tot gezondheidsschade. Bedrijven kunnen niet meer inloggen, communiceren of toegang krijgen tot hun bestanden. Dit leidt tot verlies aan productiviteit en dus tot financiële schade. De kosten van het bestrijden van een volgende cyberaanval zullen vooral bij Cirrocumulus Networks liggen. Doordat veel instanties hierdoor getroffen worden en de duur tot 6 dagen kan duren, kunnen de kosten oplopen tot 500 miljoen.
	3.2 Aantasting vitaliteit	0	Niet van toepassing. Er is geen sprake van correctiefactor omdat het aandeel van bbp <10% en de tijdsduur kleiner is dan een maand.
Ecologisch	4.1 Aantasting beschermwaardige natuur	0	Niet van toepassing
	4.2 Aantasting milieu en natuur in algemene zin	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	Het is voorstelbaar dat meerdere indicatoren worden geraakt: 1. Onderwijs wordt deels geraakt. Niet alle instellingen zullen gebruik maken van deze CSP, maar wel een aanzienlijk deel. 2. Werk wordt deels geraakt. 3. Maatschappelijke voorzieningen/bereikbaarheid: In de zorg kunnen mogelijk bepaalde activiteiten tijdelijk geen doorgang vinden. Ook andere maatschappelijke voorzieningen kunnen hier mee te maken krijgen maar dit zal niet op zeer grote schaal leiden tot het niet gebruik kunnen maken van maatschappelijke voorzieningen.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			4. Het eigen sociale netwerk zal beperkt geraakt worden maar niet dusdanig dat het gescoord wordt. 5. Virtuele bereikbaarheid: kan ook worden geraakt (bepaalde systemen), maar dat zal zich waarschijnlijk beperken tot een kleine schaal. 6. Noodzakelijke aankopen: er zullen effecten zijn bij winkels, maar het is de verwachting dat dit niet of nauwelijks leidt tot het niet kunnen doen van noodzakelijke aankopen.
	5.2 Aantasting democratische rechtsstaat	C	Er is sprake van een aanzienlijke aantasting van het openbaar bestuur omdat vele digitale overheidsdiensten stilvallen en soms voor langere tijd worden verstoord. Dit belemmert ook de werkzaamheden van het ambtenarenapparaat. Een groot deel van de processen en diensten is na enkele dagen weer hersteld, echter diverse diensten kunnen niet simpelweg gereset worden vanwege de complexiteit van het herstelproces en resulteren in een langer durend herstelproces. Dit heeft ook effect op het vertrouwen van burgers in de overheid. Omdat dit effect veroorzaakt wordt door het moedwillig handelen van een andere staat wordt de initiële impactscore B verhoogd tot C.
	5.3 Sociaal-maatschappelijke impact	0	Niet van toepassing
Internationale rechtsorde	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	A	Het betreft hier een aanval van een statelijke actor (infiltratie, spionage en sabotage) waarbij er sprake is van normschending.
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Multilaterale instituties en internationale regimes	0	Niet van toepassing
	6.4 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.2.2 Het scenario 'Misconfiguratie bij groot technologiebedrijf'

Er bestaan grote afhankelijkheden van IT-diensten die geleverd worden door een klein aantal grote technologiebedrijven. Deze afhankelijkheid strekt zich uit tot essentiële infrastructuur in zowel publieke als private domeinen. Wanneer deze diensten uitvallen, heeft dat directe en verstrekkende gevolgen (Kasteleijn, 2024; NOS, augustus 2025; Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2024). Een voorbeeld is de NAFIN-storing in 2024, een softwarefout in het standaard netwerkonderdeel van het Defensienetwerk zorgde voor een

grootschalige storing van allerlei overheidsinstanties (Algemene Rekenkamer, 2024). Een tweede voorbeeld is de CrowdStrike storing in juli 2024, een software update zorgde ervoor dat wereldwijd Windows-systemen offline gingen waardoor de systemen van verschillende (vitale) organisaties (deels) niet beschikbaar waren (Nationaal Cyber Security Centrum, 2024). Een derde voorbeeld is de storing op 25 januari 2023 bij Microsoft, waarbij diensten zoals Outlook, Teams, SharePoint en OneDrive tijdelijk niet beschikbaar waren. De storing werd veroorzaakt door een misconfiguratie in een netwerkcomponent tijdens een geplande update. Deze fout leidde tot een authenticatieprobleem en had een domino-effect op andere systemen binnen de Microsoft-Cloud omgeving (AD Techredactie, 2023).

Incidenten zoals misconfiguraties bij grote technologiebedrijven komen regelmatig voor. Tot nu toe is de impact vaak beheersbaar, maar het risico op ernstigere en langdurige verstoringen neemt toe. Dit wordt onder meer veroorzaakt door de snelle ontwikkeling van geavanceerde technologieën waaronder artificiële intelligentie, de inzet van digitale middelen als geopolitiek machtsmiddel en de toenemende afhankelijkheid van een select aantal dominante technologieleveranciers. Naast incidenten door technische fouten worden incidenten steeds vaker veroorzaakt door doelbewuste aanvallen, zoals sabotage of spionage door statelijke actoren.

Dat Nederland kwetsbaar is, blijkt ook uit de eerdere berichtgeving, zoals Schellevis (2024), waaruit naar voren komt dat ongeveer 63 procent van de circa 3800 grootste Nederlandse bedrijven, waarvan de website achterhaald kon worden, gebruik maakt van clouddiensten van Microsoft of Google. Uit latere berichtgeving blijkt eveneens dat de afhankelijkheid van Nederlandse bedrijven van Amerikaanse Cloud infrastructuur steeds verder toeneemt (Schellevis, 2026). Het rapport ‘Van Kwetsbaar naar weerbaar’ van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2025) gebruikt hierbij de woorden ‘analoog onbekwaam’. Ook hier wordt benadrukt dat structurele aandacht in digitale weerbaarheid nodig is. Doordat een steeds groter deel van de organisaties afhankelijk is van deze (cloud)diensten, kan één fout of storing bij een Amerikaanse aanbieder in één keer miljoenen organisaties ontwrichten.

Ook in de samenleving lieten de eerdergenoemde incidenten duidelijk de afhankelijkheid van digitale dienstverleners zien. Overheidsinstellingen zoals de Tweede Kamer en diverse gemeenten konden hun digitale dienstverlening niet goed uitvoeren. Burgers konden in verschillende gemeenten geen afspraken maken of documenten aanvragen en het storingsnummer van bijvoorbeeld drinkwaterbedrijf Vitens was moeilijk bereikbaar. Cloud-gebaseerde applicaties en diensten op Micorsoft Azure (de clouddienst van Microsoft) waren tijdelijk onbereikbaar (AD Techredactie, 2023).

Grote technologiebedrijven zoals Microsoft leveren uiteenlopende diensten en componenten die verweven zitten in allerlei systemen en netwerken wereldwijd. Ook leunen dergelijke technologiebedrijven sterk op hun eigen technologie en interne backbone voor het leveren van diensten. De kwaliteit en expertise van deze organisaties is enorm en

over het algemeen willen zij zo min mogelijk afhankelijk zijn van andere partijen, maar dit kan ook betekenen dat er steeds meer onbekende afhankelijkheden in hun systemen zitten, waardoor de storing zich verder kan verspreiden én herstel bemoeilijkt kan worden (Rathenau Instituut, 2024).

Bovenstaande was, in afstemming met experts, dan ook de aanleiding voor de keuze van het scenario dat voor deze analyse is uitgewerkt: een misconfiguratie bij een groot technologiebedrijf. In het scenario wordt geschetst wat voor type systemen allemaal geraakt kunnen worden: slimme apparaten, *Internet of Things*-systemen, toegangssystemen, gebouwbeheersystemen, kantoor-automatiseringsdiensten, en clouddiensten.

In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario Misconfiguratie bij groot technologiebedrijf gebouwd is.

Tabel 8 Bepalende bouwstenen voor het scenario 'Misconfiguratie bij groot technologiebedrijf'

Oorzaak	Actor	Element	Middelen	Aard van de aantasting	Getroffenen (direct)	Getroffenen (ketenefecten)	Doordringingsgraad
Technisch falen	Interne actoren	Een fout in de software update	Misconfiguratie	Aantasting van beschikbaarheid	Digitale Dienstverleners	Rijksoverheid	Aanzienlijk deel van de betreffende categorieën is getroffen (30%)
						Digitale Dienstverleners Topsectoren Overige organisaties (incl. gemeenten, veiligheidsregio's, MKB) Burgers Vitale infrastructuur Vitaal (kleine mate)	

3.2.2.1 Scenario: Misconfiguratie bij groot technologiebedrijf

Bij een groot internationaal technologiebedrijf waar miljarden organisaties en gebruikers op zijn aangewezen, genaamd Futurion, wordt tijdens routineonderhoud aan de interne systemen een configuratiefout gemaakt. Diensten zoals e-mail, online vergaderen, cloudopslag en tekstverwerken zijn tijdelijk niet beschikbaar in delen van Europa. In verschillende sectoren zijn direct veel mensen en organisaties getroffen, waaronder Nederlandse overheden, publieke diensten, onderwijs, zorg, bedrijfsleven en consumenten. Iedereen die rechtstreeks diensten afneemt van Futurion, of indirect afhankelijk is van dienstverleners die hierop bouwen, ondervindt de gevolgen. De impact voor vitale sectoren blijft beperkt doordat er noodprocedures zijn en essentiële diensten voorrang krijgen op toegang tot noodzakelijke systemen en middelen.

Medewerkers van Futurion merken het direct en doen er alles aan om te achterhalen wat er mis is gegaan. Het blijkt dat de configuratiefout is ontstaan door een software update. Binnen tien uur wordt dit achterhaald. Vervolgens wordt alles op alles gezet om de fout te herstellen.

De hoge mate van automatisering en onderliggende afhankelijkheden in de systemen van het bedrijf zorgen ervoor dat de configuratiefout onmiddellijk aan andere systemen wordt doorgegeven, wat tot een opeenstapeling van problemen leidt voor de dienstverlening. Naast directe afnemers worden ook veel bedrijven geraakt die hun dienstverlening op dit platform hebben gebouwd. Voor de overheid geldt bijvoorbeeld dat essentiële voorzieningen, zoals DigiD, niet meer toegankelijk zijn. Voor de zorg geldt dat patiëntendossiers tijdelijk niet beschikbaar zijn en voor het onderwijs ontstaan problemen met online lesmateriaal. Ook allerlei commerciële bedrijven ervaren problemen omdat zij hun hele dienstverlening gebaseerd hebben op de systemen van Futurion.

Futurion levert ook veel componenten die gebruikt worden in allerlei slimme apparaten met een internetverbinding, zoals koelkasten, thermostaten, slimme horloges en deurbellen. Veel organisaties in deze sector hebben hun centrale dienst gebaseerd op Futurion diensten en verliezen hun verbinding en gaan in '*fallback* modus', waardoor ze niet meer op afstand bestuurd en uitgelezen kunnen worden.

Na het achterhalen van de fout in de eerste tien uur van het incident, kost het nog ongeveer 10 uur om de misconfiguratie te herstellen. Het duurt vervolgens nog een aantal uur om alle systemen langzaam weer op te starten en de verschillende diensten weer online te brengen. Omdat er bij het opstarten een enorme hoeveelheid dataverkeer zal ontstaan moet dit gefaseerd gedaan worden, want anders zal overbelasting ervoor zorgen dat systemen direct weer uit vallen. De meeste functionaliteiten zijn voor Futurion en diens klanten snel hersteld, al duurt het nog dagen om de systemen geheel te herstellen. Klanten die hun eigen dienstverlening hebben gebouwd op de Futurion-diensten kunnen mogelijk nog meerdere dagen nodig hebben om volledig herstel naar hun klanten te organiseren.

3.2.2.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario 'Misconfiguratie bij groot technologiebedrijf'.

Tabel 9 Beoordelingstabel scenario 'Misconfiguratie bij groot technologiebedrijf'

Thema	**Cyberdreigingen**
Dreigingscategorie	Verstoring functioneren internet
Scenario	Misconfiguratie bij groot technologiebedrijf
Scenariotoelichting	Door een interne misconfiguratiefout bij een groot technologiebedrijf (Futurion), veroorzaakt door een software update, waren de diensten tijdelijk verstoord. Het duurde ca. 10 uur om de fout te achterhalen en nog eens 10 uur om de fout te herstellen. Veel organisaties hadden hier last van.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	D	Het is waarschijnlijk dat dit kan gebeuren. Recente verstoringen laten dit ook zien. De afhankelijkheid van enkele specifieke buitenlandse grote technologiebedrijven is een bekende kwetsbaarheid, maar er zijn weinig mitigerende maatregelen om de afhankelijkheden minder risicovol te laten zijn.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	0	Niet van toepassing
	1.3 Informatie en digitale ruimte	0	Niet van toepassing omdat er geen sprake is van ongewenste toegang en daarom wordt de digitale ruimte niet geschaad.
	1.4 Grondgebied EU en NAVO lidstaten	0	Niet van toepassing
Fysiek	2.1 Doden	A	Het is niet ondenkbaar dat er doden vallen door het tijdelijk niet werken van de digitale systemen van zorgorganisaties. Denk aan patiëntendossiers die tijdelijk niet beschikbaar zijn en patiënten die onvoldoende/verkeerde medicatie innemen.
	2.2 Ernstig gewonden en chronisch zieken	A	Hier geldt dezelfde bovenstaande redenering.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing want de verstoring duurt niet langer dan 2 dagen (ondergrens).
Economisch	3.1 Kosten	B	De herstelkosten liggen vooral bij Futurion en zijn als onderdeel van de gebruikelijke IT-bedrijfsvoering minimaal, zowel voor dienstverlener als afnemer. De uitval raakt de werkzaamheden van veel (semi)publieke organisaties en bedrijven, wat leidt tot financiële schade. Ook de zorg wordt aangetast omdat

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			patiëntendossiers tijdelijk niet beschikbaar zijn, al zal de gezondheidsschade beperkt blijven. De impact is groot, maar door de korte duur niet erg intensief. Doordat er veel organisaties getroffen worden, lopen de kosten op tot meer dan 100 miljoen Euro.
	3.2 Aantasting vitaliteit	0	Niet van toepassing. Er zijn geen lange termijneffecten.
Ecologisch	4.1 Aantasting beschermwaardige natuur	0	Niet van toepassing
	4.2 Aantasting milieu en natuur in algemene zin	0	Niet van toepassing
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	Het is voorstelbaar dat meerdere indicatoren worden geraakt: 1. Onderwijs wordt deels geraakt want mogelijk zijn lesmaterialen of leeromgevingen niet beschikbaar, omdat veel onderwijsinstellingen aangesloten zijn op Futurion diensten. 2. Werk: een grote hoeveelheid organisaties en bedrijven zijn aangeslotenop Futurion, impact van korte duur. 3. Maatschappelijke voorzieningen worden niet geraakt. 4. Sociale netwerk: Dit wordt onvoldoende geraakt om bij te dragen in de score. 5. Sociale bereikbaarheid: Er zal een verminderde virtuele en sociale bereikbaarheid zijn. 6. Noodzakelijke aankopen: Dit wordt niet geraakt. Gezien de duur van 1 tot 2 dagen en het aantal getroffenen (meer dan 1 miljoen), klasse B.
	5.2 Aantasting democratische rechtsstaat	0	Niet van toepassing. Het gaat hier om kortdurend technisch falen en daarom is er geen sprake van aantasting van de democratische rechtsstaat.
	5.3 Sociaal-maatschappelijke impact	0	Niet van toepassing. In het scenario wordt niet gesproken over sociaal-maatschappelijke onrust.
Internationale rechtsorde & stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	0	Niet van toepassing
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Multilaterale instituties en internationale regimes	0	Niet van toepassing
	6.4 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.2.3 *Beschouwing Verstoren functioneren internet*

De scenario's in deze dreigingscategorie illustreren de risico's die samengaan met een sterke afhankelijkheid van dominante technologiebedrijven, onder meer wanneer deze afhankelijkheid wordt geëxploiteerd door een moedwillige aanval.

Beide scenario's scoren hoog op waarschijnlijkheid. Dit hangt samen met de vergelijkbare incidenten die de afgelopen jaren hebben plaatsgevonden van een gelijkaardige aard en omvang zoals beschreven in de inleiding van het scenario. Daarnaast benadrukt deze beoordeling ook een duidelijke verstoring in het dagelijks leven. Digitale diensten zijn diep verweven in de dagelijkse werkzaamheden van organisaties in allerlei sectoren; overheden, zorginstellingen en onderwijsorganisaties vertrouwen op deze infrastructuur voor communicatie, gegevensopslag en dienstverlening. Een (gerichte) verstoring kan verstrekkende gevolgen hebben zoals beperkte toegang tot DigiD, patiëntendossiers die niet beschikbaar zijn of beperkte toegang tot online lesmateriaal. Tevens kan een (gerichte) verstoring ook leiden tot datalekken, en problemen met dienstverlening voor vitale infrastructuur.

In het eerste scenario betreft de oorzaak een moedwillige aanval van een statelijke actor. Internationale spanningen vergroten de bereidheid van landen om cyberaanvallen als instrument in te zetten. Deze aanvallen zijn vaak relatief goedkoop en schaalbaar en betrokkenheid kan worden ontkend. Hierbij zetten landen ook steeds vaker niet-statelijke actoren of private organisaties in om cyberaanvallen uit te voeren (CSBN, 2025). Deze ontwikkeling heeft bijgedragen aan een hoge waarschijnlijkheid in bovenstaande analyse waarin een statelijke actor digitale spionage pleegt via een Cloud leverancier. Dit kan het herstel complexer en langduriger maken. Wanneer Nederland te maken krijgt met een geavanceerde aanval op vitale processen of andere kritieke entiteiten, heeft dat grote gevolgen. Dit scenario maakt duidelijk dat geopolitieke motieven en technologische kwetsbaarheden samen het risico vergroten op een grootschalige impact.

De kosten voor beide scenario's vallen in categorie B omdat een breed scala aan organisaties afhankelijk is van werkende IT-systemen, clouddiensten en internet. Daardoor ontstaan niet alleen hoge herstelkosten, maar ook aanzienlijke financiële schade wanneer de bedrijfsvoering uitvalt. Zelfs bij een relatief korte verstoring lopen de totale kosten al op tot ruim boven de 100 miljoen Euro. De verwevenheid tussen (publieke) diensten en digitale infrastructuur is daarmee een grote kwetsbaarheid. Wanneer de schade toeneemt, worden herstelwerkzaamheden complexer of wellicht deels onmogelijk met aanzienlijke kosten als gevolg.

Het feit dat deze scenario's heel waarschijnlijk worden geacht, en dat het hierbij gaat om een dusdanige verstoring van het dagelijks leven, aanzienlijke kosten en een aantasting van de rechtsstaat wanneer het gaat om een moedwillige aanval, maakt dat dit een risico is voor de nationale veiligheid en daarom maatregelen vereist om de weerbaarheid te vergroten voor de digitale zelfstandigheid van Nederland.

3.3 Dreigingscategorie verstoren cyber-fysieke systemen

Deze dreigingscategorie richt zich op de potentiële gevolgen van incidenten met zogenaamde cyber-fysieke systemen. Het gaat hierbij om digitale systemen die worden gebruikt om fysieke processen aan te sturen (Lee, 2008), zogenoemde Industriële Controle Systemen (ICS). ICS zijn onderdeel van de operationele technologie (OT) en worden in veel sectoren gebruikt om uiteenlopende processen aan te sturen, zoals energiesystemen, drinkwaterdistributie, het bedienen van pompen, bruggen en sluizen, beveiligingssystemen of chemische industrieprocessen. Omdat ICS een grote rol spelen in veel vitale processen, bestaat binnen deze dreigingscategorie een sterke samenhang met bedreigingen tegen de vitale infrastructuur. Ook is het belangrijk om de verwevenheid met andere fenomenen te erkennen. Kwetsbaarheden in ICS worden namelijk steeds vaker benut door zowel statelijke actoren als criminele groeperingen, niet alleen om systemen te saboteren, maar ook om politieke druk uit te oefenen, *crime as a service* (geldelijk gewin) of voorbereiding te treffen om tot actie over te kunnen gaan als dat opportuun is. In deze dreigingscategorie is het scenario 'Cyberincident Regionale Energievoorziening' uitgewerkt.

3.3.1 Het scenario 'Cyberincident Regionale Energievoorziening - op aanvraag

Het scenario is gebaseerd op twee bestaande scenario's uit de Rijksbrede Risicoanalyse Nationale Veiligheid 2022 (ANV, 2022) ("cyberaanval ICS – chemische sector" en "landelijke black-out"). Daarnaast is in het scenario gebruik gemaakt van ervaringen uit de praktijk zoals de landelijke stroomuitval in Spanje en Portugal en de toenemende zorgen van de Inspectie Justitie en Veiligheid over de weerbaarheid van Nederlandse veiligheidsregio's tegen langdurige stroomuitval (Cybercrimeinfo, 2025; NOS, augustus 2025; NOS, april 2025; Inspectie Justitie en Veiligheid, 2025).

In de trendanalyse van 2024 is benoemd waarom de bedreiging van vitale infrastructuur voor de energiesector specifiek zorgwekkend is. Nederland kampt met een beperkte capaciteit van het elektriciteitsnetwerk, dat onder druk staat door de energietransitie. Steeds meer huishoudens stappen over naar elektriciteit als energiebron. Dit zorgt ervoor dat de vraag groter is dan het aanbod en in sommige gevallen huishoudens niet kunnen worden aangesloten. In het Caribische deel van het Koninkrijk zorgt de instabiliteit van het netwerk al regelmatig tot stroomuitval.

Het scenario betreft daarom een cyberaanval door een buitenlandse staatsgelieerde extremistische groepering op een regionale energievoorziening in Nederland. Via social engineering weten de aanvallers toegang te verschaffen tot de informatie- en operationele technologie (hierna IT en OT) omgeving van de netbeheerder. De hackersgroep installeert malware op het netwerk met als gevolg dat tussenstations uitvallen en delen van de Randstedelijke regio zonder stroom komen te zitten. Uiteindelijk ontstaat er een langdurige stroomuitval met grote gevolgen voor de vitale sectoren en de bredere samenleving.

3.3.1.1 Scenario: Cyberincident Regionale Energievoorziening

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

3.3.2 Beschouwing verstoren cyber-fysieke systemen

Dit scenario gaat specifiek in op de kwetsbaarheid van een netbeheerder door de toenemende interactie van IT-en OT-systemen. Waar IT zich richt op data en communicatie, is OT verantwoordelijk voor het aansturen van fysieke processen. Naarmate deze systemen meer op elkaar aansluiten, ontstaan nieuwe kwetsbaarheden. Een aanval op IT-systemen kan onder bepaalde omstandigheden overslaan naar OT en daar mogelijk fysieke schade veroorzaken.

Deze verwevenheid is niet beperkt tot één sector, dit is zichtbaar in vrijwel alle vitale sectoren zoals energie en water. In deze sectoren kan een verstoring grote maatschappelijke gevolgen hebben zoals een landelijke black-out of problemen met het beheer van water (CSBN, 2025).

De beoordeling laat zien dat de impact op de toegang tot primaire levensbehoeften groot is en dat het zorgt voor een grote verstoring op het dagelijks leven. Het scenario laat zien dat veel onderdelen van het dagelijks leven uitvallen of verstoord raken zoals straatverlichting, verwarming, het wegpompen van afval- en rioolwater, en ook mobiele netwerken en openbaar vervoer worden getroffen. Wanneer mensen twee dagen geen beschikking hebben tot warmte, koeling en sanitair heeft dat verstrekkende gevolgen en komt ook de acute zorg in gevaar. Het niet beschikbaar zijn van het 112-noodnummer zal de hulpverlening vertragen, terwijl uitval van verkeerssystemen verkeerschaos veroorzaakt en risico op ongevallen vergroot. De onzekerheid kan ook leiden tot gevoelens van angst en paniek onder de bevolking. Daarnaast heeft het incident als gevolg dat men tijdelijk geen onderwijs meer kan volgen, werk verminderd kan worden uitgevoerd en de virtuele en sociale bereikbaarheid beperkt wordt.

Geopolitieke motieven en statelijke actoren spelen een steeds grotere rol in dit onderwerp. Internationale spanningen en botsende strategische belangen vergroten niet alleen de kans dat vitale infrastructuur doelwit wordt van cyberaanvallen maar maken het dreigingslandschap ook complexer door onder andere het gebruik van proxies, criminele groeperingen of ingehuurde hackers om doelen te bereiken. Juist vanwege de kritieke functie van vitale sectoren in de samenleving, is het aanvallen van digitale systemen van deze kritieke entiteiten een steeds belangrijker instrument geworden voor staten in een geopolitiek volatiel systeem.

Al met al laat het scenario zien dat een cyberaanval niet beperkt blijft tot het digitale domein, maar ook fysieke processen kan ontwrichten met verstrekkende gevolgen voor het dagelijks leven en daarmee hoge kosten. Geopolitieke motieven vergroten het risico op een cyberaanval en maken deze kwetsbaarheid steeds zichtbaarder. Daarom is het noodzakelijk aandacht te blijven houden voor de beveiliging van cyber-fysieke systemen.

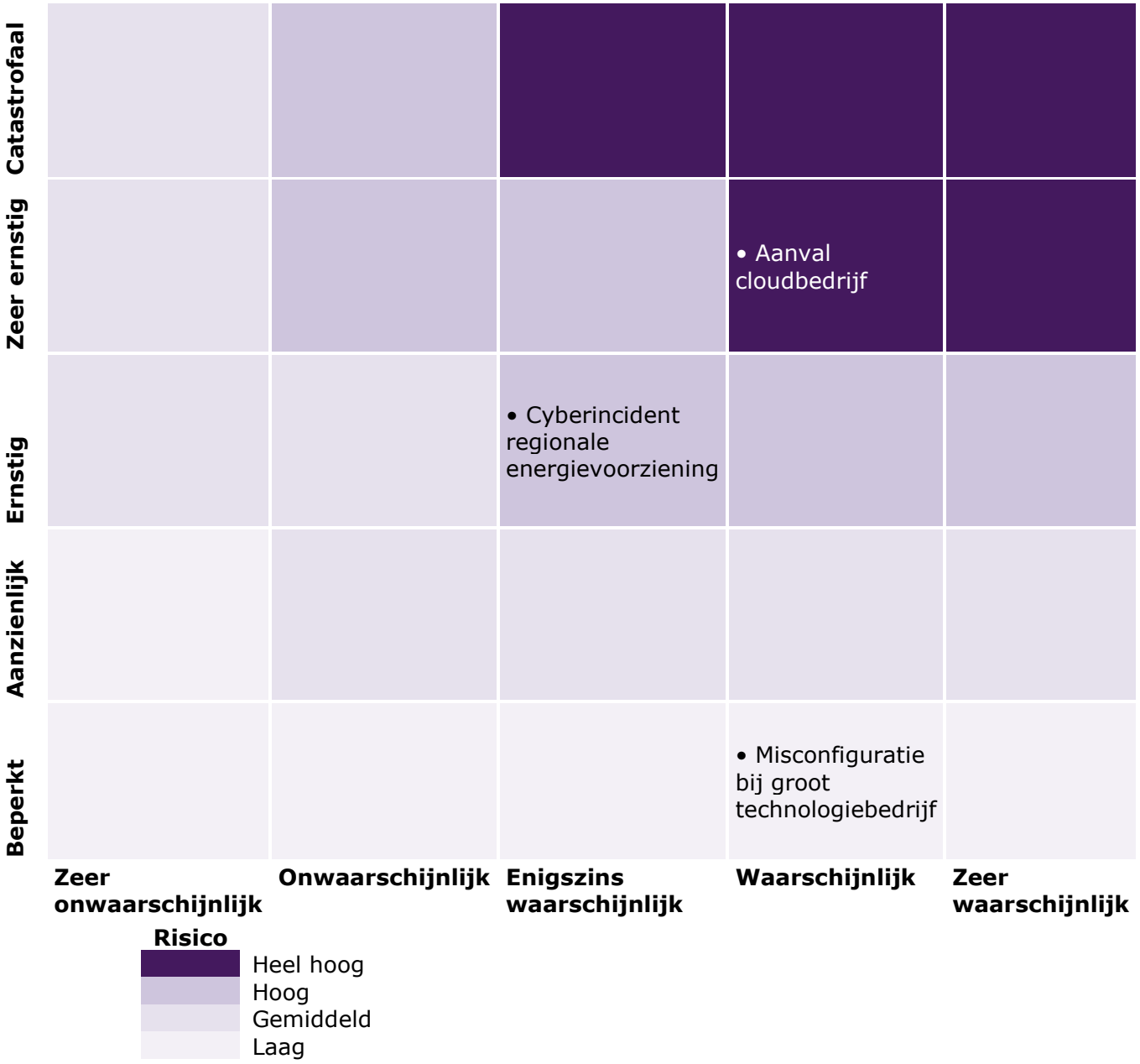
3.4 Slotbeschouwing thema cyberdreigingen

Binnen het thema Cyberdreigingen worden dreigingen voor de nationale veiligheid beschreven die samenhangen met de digitalisering van de samenleving. Binnen dit thema zijn twee verschillende dreigingscategorieën in kaart gebracht, namelijk 'verstoren functioneren internet' en 'verstoren cyber-fysieke systemen'. In totaal zijn er drie scenario's uitgewerkt waarvoor de impact en waarschijnlijkheid in kaart zijn gebracht (zie Figuur 1).

3.4.1 De impact en waarschijnlijkheid van Cyberdreigingen

In onderstaande figuur worden de drie uitgewerkte scenario's in vergelijkend perspectief weergegeven.

Figuur 1 Risicodiagram thema Cyberdreigingen



In het risicodiagram is te zien dat alle uitgewerkte scenario's binnen het thema cyberdreigingen hoog scoren op waarschijnlijkheid. De twee scenario's binnen de dreigingscategorie 'verstoren functioneren internet' worden waarschijnlijk geacht, het scenario binnen de dreigingscategorie 'verstoren cyber-fysieke systemen' enigszins waarschijnlijk. Cyberaanvallen en andere digitale incidenten zijn aan de orde van de dag, waarbij tot nu toe de impact en schade beperkt blijven. Gezien het huidige geopolitieke klimaat en de toenemende technische mogelijkheden zal de hoeveelheid digitale incidenten toenemen en mogelijk de impact van dergelijke incidenten evenzo.

De impact van de uitgewerkte scenario's loopt meer uiteen, voor het scenario 'misconfiguratie bij groot technologiebedrijf' is de algehele impact een stuk lager dan bij de overige twee scenario's. Dit heeft voornamelijk te maken met het verschil in oorzaak. Bij zowel het scenario 'aanval op cloudbedrijf' als 'cyberincident regionale energievoorziening' is er sprake van ondermijnende acties door actoren en een schending van de digitale ruimte. Ook zijn er bij de scenario's, zeker bij het scenario in de dreiging categorie cyber-fysieke systemen, relatief veel kosten gemoeid met het verhelpen van het incident.

Bovendien is er hoog gescoord op het impactcriterium 'aantasting van de democratische rechtsstaat'. De verwevenheid van toenemende digitalisering en de veranderende geopolitieke verhoudingen leiden ook tot andere vormen van schade met maatschappelijke impact. Zo kan er een angstcultuur ontstaan doordat berichtgeving over cyberaanvallen en desinformatie het beeld versterken dat systemen en instituties kwetsbaar zijn, hierdoor kan wantrouwen toenemen. Daarnaast kan het weglekken van informatie of desinformatie het vertrouwen van de burger in de overheid en instituties ondermijnen.

Zoals hierboven wordt beschreven, zijn cyberdreigingen niet meer weg te denken uit de samenleving. Dit wordt versterkt door verschillende ontwikkelingen: de toenemende digitalisering, de vervaging van attributie van cyberaanvallen en de schaalvergroting van digitale systemen. Daarboven komt de toenemende afhankelijkheid van een beperkt aantal niet-Europese technologiebedrijven, de opkomst van cyberaanvallen in de ruimte en het risico op keteneffecten bij verstoringen. Dit speelt allemaal een rol bij de onzekerheid over de weerbaarheid van Nederland. Hieronder volgt een toelichting op de genoemde aspecten.

3.4.2 Impact ontwikkelingen

3.4.2.1 Digitalisering van de samenleving

De samenleving wordt in toenemende mate afhankelijk van digitale technologieën, wat nieuwe kwetsbaarheden introduceert. Een belangrijke ontwikkeling die niet genoemd is in de scenario's, maar die wel nieuwe uitdagingen met zich meebrengt voor nationale veiligheid, is de verdere ontwikkeling van *Artificial Intelligence* (AI) en in het bijzonder generatieve AI. Deze technologie kan onder meer worden ingezet om cyberaanvallen te ontwikkelen en te automatiseren, kwetsbaarheden sneller te identificeren, phisingcampagnes te verfijnen en malware te genereren (ANV, 2024). In de beschreven scenario's zou het toepassen van generatieve AI ervoor kunnen zorgen dat

cyberaanvallen nog geavanceerder zijn en dat het nog moeilijker wordt spam en phishingteksten te detecteren.

Naast moedwillige aanvallen moeten organisaties ook rekening blijven houden met interne systeemfouten. Dit vraagt om kritische reflectie op het onderhoud en de robuustheid van digitale systemen. Kortom, digitalisering van de samenleving maakt dat (kleine) technische en menselijke fouten een groot effect kunnen hebben.

3.4.2.2 Cyberaanvallen als machtsmiddel

De selectie van de scenario's is een reflectie van het feit dat cyberaanvallen steeds vaker moedwillig worden ingezet door (statelijke) actoren. De geopolitieke spanningen nemen in rap tempo toe en cyberaanvallen worden steeds vaker gebruikt als instrument voor spionage, sabotage en beïnvloeding (DBSA, 2025). De machtsbalans in de wereld is aan het veranderen en die verschuivingen hebben een steeds grotere impact op de wereldorde, zie ook het themarapport Internationale en Militaire Dreigingen. Zo laten staten in toenemende mate de bereidheid zien om actief druk uit te oefenen met (de dreiging van) economische en militaire drukmiddelen (DBSA, 2025; Rutten, 2026). Deze dynamiek kan aanzienlijke impact hebben op het Koninkrijk der Nederlanden en de nationale veiligheid.

Naast de toename in cyberaanvallen, is het ook steeds vaker onduidelijk wie een cyberaanval uitvoert. Staten maken gebruik van proxies en criminele netwerken om sporen te verhullen. Hierdoor is het onderscheid tussen actoren en statelijke en niet-statelijke doelwitten verdwenen wat attributie en respons bemoeilijkt omdat onduidelijk is wie iets doet en tegen wie het gericht is (AIVD, 2024).

Eén van de middelen die door criminelen wordt gebruikt en is benoemd in de trendanalyse van 2024 is de inzet van ransomware (ANV, 2024). Ransomware kan bedrijfsprocessen volledig stilleggen door systemen te blokkeren totdat losgeld wordt betaald. Steeds vaker combineren aanvallers dit met het stelen van gevoelige data en dreigen ze deze openbaar te maken. Hoewel ransomware en andere vormen van cybercrime niet zijn uitgewerkt in scenario's, zijn deze thema's nog steeds actueel. Zo werd telecomprovider Odido in februari 2026 getroffen door een hack waarbij klantgegevens van minstens 6,5 miljoen mensen openbaar werden gemaakt, nadat aanvallers losgeld hadden geëist om publicatie te voorkomen (Schellevis & Mouissie, 2026). Deze activiteiten hebben ook een duidelijke link met de dreigingscategorie georganiseerde criminaliteit in het dreigingsthema 'Ongewenste inmenging en beïnvloeding democratische rechtsstaat'.

3.4.2.3 Afhankelijkheid van een beperkt aantal niet-Europese technologiebedrijven

Een volgende belangrijke ontwikkeling betreft de groeiende afhankelijkheid van grote technologiebedrijven, die cruciale digitale infrastructuur beheren**.** De dreigingscategorie 'verstoren van functioneren internet' heeft laten zien hoe kwetsbaar deze afhankelijkheid ons maakt; uitval door technisch falen of gerichte aanvallen kan vitale processen zoals betalingsverkeer, zorg en energievoorziening ontwrichten en digitale autonomie van Nederland

ondermijnen. Deze autonomie staat onder druk door de dominantie van grote internationale technologiebedrijven. Het ontbreken van redundantie betekent dat een storing bij één aanbieder grote delen van onze infrastructuur stillegt. Dit gebrek aan alternatieven voor publieke diensten maakt Nederland kwetsbaar (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2025). Daarnaast maakt het de politieke positie van Nederland lastiger: het beperkt het handelingsperspectief van Nederland op politiek-strategische dossiers en vergroot het gevaar van digitale verstoringen wanneer die worden ingezet als machtsmiddel. Het hebben van Europese (publieke) alternatieven is daardoor niet alleen belangrijk voor de digitale autonomie, maar ook een strategische noodzaak.

3.4.2.4 Cyber in de ruimte

Naast de eerder besproken ontwikkelingen is het belangrijk om ook stil te staan bij een minder tastbare, maar groeiende uitdaging: cyberdreigingen in de ruimtevaart. Het gebruik van satellieten is de afgelopen jaren sterk toegenomen, maar er is gebrekkig aandacht voor de digitale veiligheid van ruimte infrastructuur. Dit zorgt voor kwetsbaarheden in militaire en civiele systemen zoals GPS, aardobservatie en telecommunicatie (ANV, 2022; ANV, 2024; NIST, 2024).

3.4.2.5 Keteneffecten

Het scenario in de dreigingscategorie ‘cyber-fysieke systemen’ illustreert hoe cyberaanvallen steeds vaker vitale infrastructuur als doelwit hebben en niet langer als geïsoleerde incidenten kunnen worden beschouwd. De aanvallen veroorzaken vaak keteneffecten die zowel digitale als fysieke processen ontwrichten (NCTV, 2025). Een aanval op een waterbeheersysteem kan bijvoorbeeld leiden tot verstoringen in drinkwatervoorziening, die vervolgens gevolgen hebben voor de landbouw en de volksgezondheid. Een aanval op het elektriciteitsnet kan niet alleen stroomuitval veroorzaken, maar ook acute zorgprocessen stilleggen en logistieke ketens ontregelen. De verwevenheid van IT- en OT-systemen vergroot deze kwetsbaarheid aanzienlijk doordat een digitale inbreuk zich snel kan vertalen naar fysieke schade en maatschappelijke ontwrichting.

3.4.3 Kwetsbaarheden

Bovenstaande ontwikkelingen roepen de vraag op hoe weerbaar sectoren zoals overheden, onderwijsinstellingen, zorgorganisaties, het bedrijfsleven en overige zijn wanneer digitale incidenten niet binnen korte tijd worden opgelost. De afhankelijkheid van digitale systemen neemt voortdurend toe en deze systemen blijven zich in hoog tempo ontwikkelen. Dit is ook herhaaldelijk benoemd in diverse rapporten (zoals het rapport ‘Van Kwetsbaar naar weerbaar’ van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2025)) en benadrukt dat structurele aandacht voor digitale weerbaarheid nodig is. Een voorbeeld waaruit duidelijk wordt dat er ook allerlei maatregelen in ontwikkeling zijn, is de Cyberbeveilingswet (Cbw). Het wetsvoorstel dient om de Europese NIS2-richtlijn om te zetten in Nederlandse wetgeving om daarmee de digitale weerbaarheid te versterken door normen en verplichtingen vast te leggen voor organisaties (NCSC, 2025).

De beschreven kwetsbaarheden vormen een dynamisch en groeiend risico voor nationale veiligheid (ANV, 2022, 2024). Een combinatie van toenemende digitalisering, geopolitieke spanningen en technologische innovaties maakt dat Nederland zich proactief moet voorbereiden. Hoewel de scenario's binnen dit thema zo zijn geschetst dat het gaat om incidenten die uiteindelijk zijn verholpen, is het belangrijk te onderkennen dat dit niet vanzelfsprekend is. Het is realistisch dat zich incidenten voordoen waarbij de schade niet volledig kan worden hersteld. Het versterken van digitale weerbaarheid, het verminderen van afhankelijkheden en het verder ontwikkelen van crisisplannen zijn daarom een noodzaak.

Eén van de manieren om kwetsbaarheden te verminderen is het zoeken naar aanvullende of alternatieve digitale leveranciers. Ook het opbouwen van redundantie kan behulpzaam zijn op dit vlak. Bijvoorbeeld redundantie gericht op het uit kunnen blijven voeren van vitale processen wanneer verstoring niet voorkomen kan worden. Tot slot is het in zijn algemeen van belang om een beeld te krijgen en te onderhouden van waar in de (digitale) keten zich risico's dan wel kwetsbaarheden bevinden.

4 Literatuur

AD Techredactie. (2023, januari 25). Uren geen Teams, Outlook en Office 365 door storing Microsoft: ook problemen bij Nederlandse overheden. https://www.ad.nl/tech/uren-geen-teams-outlook-en-office-365-door-storing-microsoft-ook-problemen-bij-nederlandse-overheden~ae92b7119/

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2024). Jaarverslag 2024. Beschikbaar via: https://www.aivd.nl/documenten/jaarverslagen/2025/04/24/jaarverslag-2024

Algemene Rekenkamer. (2024, november 7). *Cruciaal defensienetwerk NAFIN goed opgezet, maar beveiliging in de praktijk onvoldoende*. https://www.rekenkamer.nl/actueel/nieuws/2024/11/07/cruciaal-defensienetwerk-nafin-goed-opgezet-maar-beveiliging-in-de-praktijk-onvoldoende

Algemene Rekenkamer. (2025, 15 januari). *Het Rijk in de cloud*. Https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud

Analistennetwerk Nationale Veiligheid (2026, maart). *Leidraad Risicobeoordeling Rijksbrede risicoanalyse Nationale Veiligheid.*

Analistennetwerk Nationale Veiligheid (ANV) (2024). *Trendanalyse Nationale Veiligheid 2024. Verdieping op de Trendanalyse.*

Analistennetwerk Nationale Veiligheid (ANV) (2022). *Rijksbrede Risicoanalyse Nationale Veiligheid.*

Centraal Bureau voor de Statistiek. (2025, april 30). *4. Cloudaanbieders*. In *Verkenning mogelijkheden beschikbaarheid statistieken over data delen, Internet of Things en clouddiensten*. Geraadpleegd op 20 augustus 2025, van https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/verkenning-mogelijkheden-beschikbaarheid-statistieken-over-data-delen-internet-of-things-en-clouddiensten/4-cloudaanbieders

Cybercrimeinfo. (2025).beschikbaar via: De stroomstoring in Spanje en Portugal: gevolgen en lessen voor Nederland / Cyber Commando / Bibliotheek | Cybercrimeinfo.nl

Cybersecuritybeeld Nederland (CSBN). 2025, NCTV, 26-11-2025, https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/11/26/cybersecuritybeeld-nederland-2025/cybersecuritybeeld-nederland-2025.pdf.

Digitale Overheid. *Prioriteit 1 – Cloud*. Nederlandse Digitaliseringsstrategie. Geraadpleegd op 20 augustus 2025, van https://www.digitaleoverheid.nl/nederlandse-digitaliseringsstrategie-nds/6-prioriteiten-voor-een-overheid/prioriteit-1-cloud/)

Dreigingsbeeld Statelijke Actoren (DBSA) 2025, AIVD, MIVD, NCTV, 17-07-2025, https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025.

ENGIE. (zonder datum). Beschikbaar via: Piekbelasting: hoe kan het voorkomen worden? | ENGIE

European Union Agency for the Space Programme (EUSPA). *Galileo*. EU Space Programme. https://www.euspa.europa.eu/eu-space-programme/galileo

Inspectie Justitie en Veiligheid. (2025). *Brief - Toezicht preparatie op (langdurige) stroomuitval*. Beschikbaar via: https://www.inspectie-jenv.nl/site/binaries/site-content/collections/documents/2025/08/07/brief-toezicht-preparatie-op-stroomuitval/brief-toezicht-preparatie-op-stroomuitval.pdf

Kasteleijn, N. (2024, juli 19). *Wat is CrowdStrike en hoe kon het zo misgaan? Dit is wat we nu weten*. NOS. https://nos.nl/artikel/2529477-wat-is-crowdstrike-en-hoe-kon-het-zo-misgaan-dit-is-wat-we-nu-weten

Koning, M. de. (2025, 12 februari). *Onze afhankelijkheid van Big Tech is gevaarlijk, waarschuwen techneuten – de oplossing: een Nederlandse Cloud*. NRC. Geraadpleegd op 28 juli 2025, van https://www.nrc.nl/nieuws/2025/02/12/onze-afhankelijkheid-van-big-tech-is-gevaarlijk-waarschuwen-techneuten-de-oplossing-een-nederlandse-cloud-a4882880

Edward A. Lee, "Cyber physical systems: Design challenges," *11th IEEE international symposium on object and component-oriented real-time distributed computing* (ISORC) (mei 2008): 363-369, 10.1109/ ISORC.2008.25.

Ministerie van Algemene Zaken, Directie Risicobeheersing & Rampenbeleid (2027, december). *Risicoprofiel Curaçao 2017-2022*.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2011, 20 april). *Reactie op de motie van het lid Van der Burg c.s. (26643, nr. 157) over mogelijkheden voor de inrichting van de overheidscloud* (Kamerstuk 26643, nr. 179). Tweede Kamer der Staten-Generaal. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2011D21372&did=2011D21372

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2025, september 12). *Rapport Van kwetsbaar naar weerbaar: Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties*. Rijksoverheid. Https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar [rijksoverheid.nl]

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025). *Dreigingslandschap Vitale Infrastructuur*. Inzicht in de stapeling van toenemende en veranderende dreigingen. https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2024). *Cybersecuritybeeld Nederland 2024*. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024

Nationaal Cyber Security Centrum. (2024, juli 19). *Update wereldwijde storing CrowdStrike*. NCSC. https://www.ncsc.nl/actueel/nieuws/2024/juli/19/wereldwijde-storing

Nationaal Cyber Security Centrum. (2025, juni 7). *Wetsvoorstel Cbw ingediend bij Tweede Kamer*. https://www.ncsc.nl/nieuws/wetsvoorstel-cbw-ingediend-bij-tweede-kamer

Nationaal Cyber Security Centrum. *Cloud uitgelegd*. https://www.ncsc.nl/cloud/cloud-uitgelegd

National Institute of standards and Technology (NIST). (2024*). Cybersecurity for the Space Domain*. Via: *https://www.nccoe.nist.gov/cybersecurity-space-domain*

NOS. (2025, oktober 20). *Apps en games weer bereikbaar na urenlange storing bij Amazon*. NOS. https://nos.nl/artikel/2587142-apps-en-games-weer-bereikbaar-na-urenlange-storing-bij-amazon

NOS. (2025, augustus 7). *Inspectie: veiligheidsregio's moeten zich voorbereiden op landelijke stroomuitval*. NOS. https://nos.nl/artikel/2577840-inspectie-veiligheidsregio-s-moeten-zich-voorbereiden-op-landelijke-stroomuitval

NOS. (2025, april 28). *Landelijke stroomstoring treft miljoenen mensen in Spanje en Portugal.* NOS. https://nos.nl/artikel/2565295-landelijke-stroomstoring-treft-miljoenen-mensen-in-spanje-en-portugal

Rathenau Instituut. (2024). *Digitale afhankelijkheid en autonomie*. Rathenau.nl

Rijksoverheid (2023). *Veiligheidsstrategie voor het Koninkrijk der Nederlanden*

Rutten, R. (2026, 18 januari). *Trumps dreigementen rond Groenland zijn voor Europese politici een rode lijn*. NRC. https://www.nrc.nl/nieuws/2026/01/18/trumps-dreigementen-rond-groenland-zijn-voor-europese-politici-een-rode-lijn-a4918010

Schellevis, J. (2024, 1 maart). *Amerikaanse overheid kan bij e-mail van Nederlandse overheden en kritieke bedrijven*. NOS. Geraadpleegd op 23 juli 2025, van https://nos.nl/artikel/2510923-amerikaanse-overheid-kan-bij-e-mail-van-nederlandse-overheden-en-kritieke-bedrijven

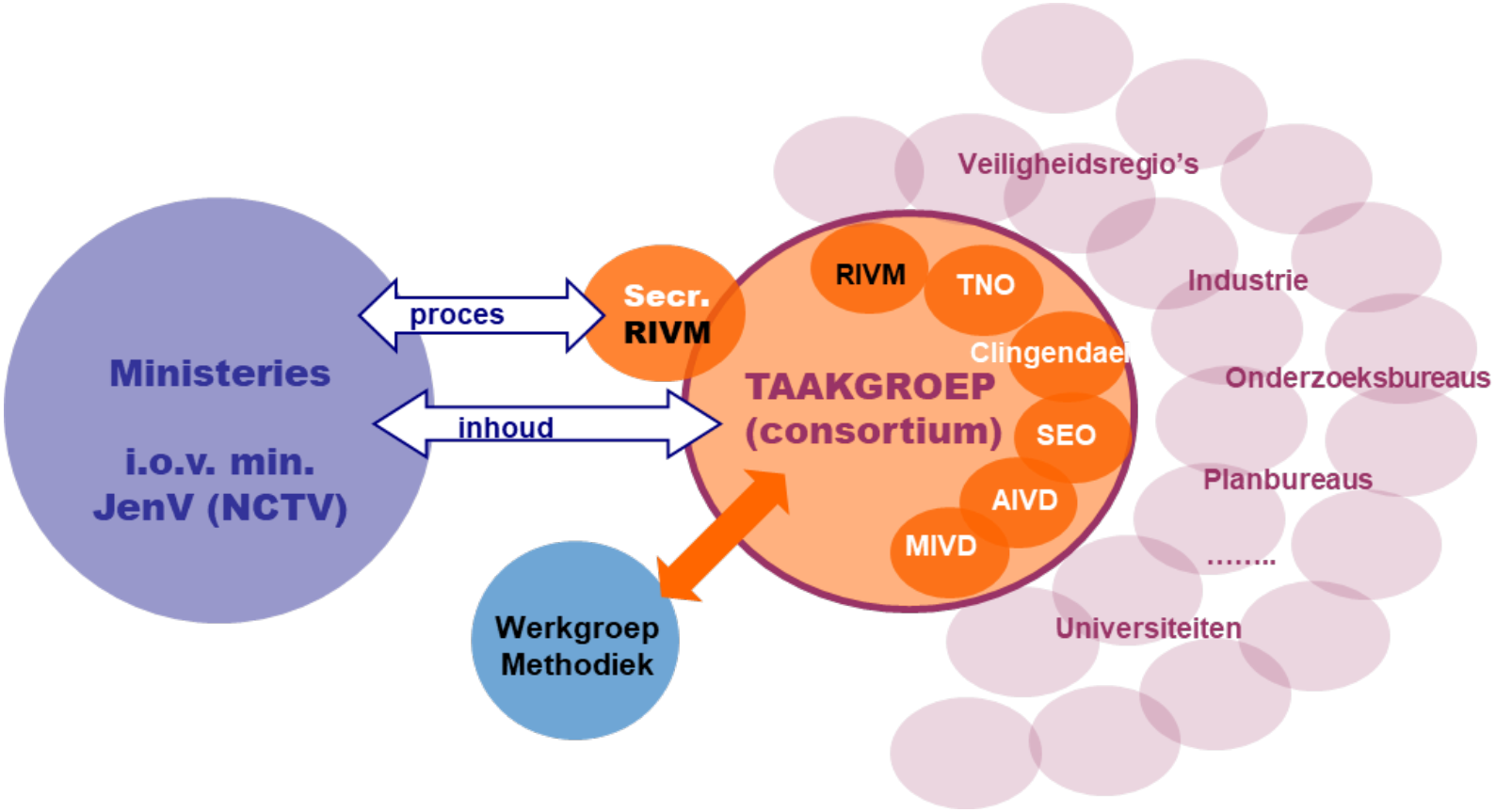
Schellevis, J. (2024, 31 mei). Overheid leunt veel meer op Amerikaanse clouds dan bekend: 'Meelezen is makkelijk'. NOS. Geraadpleegd op 28 juli 2025, van https://nos.nl/artikel/2569392

Schellevis, J. (2026, 25 januari). *Nederland hangt aan Amerikaans tech-infuus: 'We zitten in de houdgreep'*. NOS. https://nos.nl/artikel/2599601-nederland-hangt-aan-amerikaans-tech-infuus-we-zitten-in-de-houdgreep

Schellevis, J., & Mouissie, S. (2026, 1 maart). *Odido-hackers publiceren resterende klantdata, ook miljoenen ID-nummers*. NOS. https://nos.nl/artikel/2604461-odido-hackers-publiceren-resterende-klantdata-ook-miljoenen-id-nummers

Veiligheidsregio ZHZ (2024). *Regionaal Risicoprofiel.*

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