Rijksbrede Risicoanalyse Nationale Veiligheid 2026

Themarapport Ongewenste inmenging en beïnvloeding democratische rechtsstaat



Rijksbrede Risicoanalyse
Nationale Veiligheid 2026

Themarapport Ongewenste inmenging en beïnvloeding democratische rechtsstaat

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 Ongewenste inmenging en beïnvloeding democratische rechtsstaat.

Contact:
anv@rivm.nl

De Rijksbrede Risicoanalyse Nationale Veiligheid 2026, Themarapport Ongewenste inmenging en beïnvloeding democratische rechtsstaat 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 Ongewenste inmenging en beïnvloeding democratische rechtsstaat — 17
3.1 Inleiding — 18
3.2 Dreigingscategorie Ongewenste buitenlandse beïnvloeding (hybride dreigingen) — 18
3.2.1 Bouwstenen — 19
3.2.2 Het scenario 'Heimelijke beïnvloeding via een privaat bedrijf' – op aanvraag — 21
3.2.3 Beschouwing Ongewenste buitenlandse beïnvloeding (hybride dreigingen) — 22
3.3 Dreigingscategorie Spionage — 23
3.3.1 Bouwstenen — 26
3.3.2 Het scenario 'Klassieke Statelijke Spionage' — 27
3.3.3 Het scenario 'Cyberspionage Rijksoverheid' — 31
3.3.4 Het scenario 'Sabotage zeekabels Caribisch gebied voorbereid met spionage' — 36
3.3.5 Beschouwing spionage — 40
3.4 Dreigingscategorie Ongewenste buitenlandse inmenging — 42
3.4.1 Bouwstenen — 43
3.4.2 Het scenario 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland' — 44
3.4.3 Beschouwing Ongewenste buitenlandse inmenging — 48
3.5 Dreigingscategorie Georganiseerde criminaliteit — 49
3.5.1 Bouwstenen — 50
3.5.2 Het scenario 'Georganiseerde criminaliteit door heel Nederland' — 52
3.5.3 Beschouwing Georganiseerde criminaliteit — 58
3.6 Slotbeschouwing thema Ongewenste inmenging en beïnvloeding democratische rechtsstaat — 60
3.6.1 De impact en waarschijnlijkheid van ongewenste inmenging en beïnvloeding democratische rechtsstaat — 61
3.6.2 Impact ontwikkelingen — 62
3.6.3 Kwetsbaarheden — 64

4 Literatuur — 67

Bijlage 1 Samenstelling Analistennetwerk Nationale Veiligheid — 73

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 thema Ongewenste inmenging en beïnvloeding democratische rechtsstaat 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

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

besproken; de bouwstenen 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 Ongewenste inmenging en beïnvloeding democratische rechtsstaat

3.1 Inleiding

Het dreigingsthema *Ongewenste inmenging en beïnvloeding democratische rechtsstaat* beschouwt verschillende moedwillige dreigingen tegen de democratische rechtsstaat door toedoen van inmenging en beïnvloeding vanuit statelijke actoren, evenals criminelen en andere niet-statelijke actoren. In dit thema wordt onderscheid gemaakt tussen vier dreigingscategorieën. Deze categorieën zijn gelijk aan de categorieën uit de Rijksbrede Risicoanalyse 2022, te weten:

- Ongewenste buitenlandse beïnvloeding (hybride dreigingen);
- Spionage;
- Ongewenste buitenlandse inmenging;
- Georganiseerde criminaliteit.

3.2 Dreigingscategorie Ongewenste buitenlandse beïnvloeding (hybride dreigingen)

Statelijke en niet-statelijke actoren ontplooien diverse activiteiten die op verschillende manieren kunnen leiden tot beïnvloeding van andere staten. Ook Nederland en bondgenoten van Nederland zijn veelal doelwit, maar dat hoeft niet tot aantasting van de nationale veiligheid te leiden. Deze buitenlandse beïnvloeding is ongewenst, omdat op deze manier uiteenlopende nationale veiligheidsbelangen kunnen worden geschaad (AIVD, MIVD & NCTV, 2025, p. 10, 11). Buitenlandse beïnvloeding wordt vaak gevat onder de noemer hybride dreigingen. Hybride dreigingen hebben over het algemeen een aantal kenmerken (AIVD et al., 2021, p. 16-17; Hybrid CoE, 2022, AIVD, MIVD & NCTV, 2025, p. 10):

- De dreiging wordt gevormd door gecoördineerde acties die bewust inspelen op kwetsbaarheden van democratische staten en instituties;
- Deze gecoördineerde acties hebben als doel besluitvorming van het doelwit te beïnvloeden (en daarmee het doelwit te ondermijnen), terwijl de acties bijdragen aan de strategische doelen van de actor die ze uitoefent;
- Een actor zal veelal detectie en attributie van hybride activiteiten willen vermijden (onder meer door gebruik te maken van andere actoren zoals criminele organisaties);
- Een actor zal verschillende machtsinstrumenten (diplomatiek/politiek, economisch, militair, informatie) en methoden (militair, spionage, sabotage, statelijke inmenging, economie, diplomatie en politiek) inzetten teneinde de strategische doelen te bereiken;
- Hybride dreigingen zijn ambigu in de zin dat bewust de grenzen tussen oorlog en vrede, legaal en illegaal, conventioneel en onconventioneel worden vervaagd; ook om zo de drempel van gewapend conflict steeds wat verder op te schuiven.

Hybride activiteiten worden veelal toegepast door statelijke actoren – al dan niet ondersteund of uitgevoerd door niet-statelijke actoren zoals criminele organisaties. Tegelijkertijd is het voorstelbaar dat niet-statelijke actoren ook een hybride dreiging tegen de nationale veiligheid vormen, bijvoorbeeld in het geval van terroristische groeperingen of grote bedrijven. Statelijke dreigingen worden interdepartementaal gedefinieerd als: "dwingende, ondermijnende, misleidende of heimelijke

activiteiten van of namens statelijke actoren, onder de drempel van gewapend conflict, die de nationale veiligheidsbelangen van Nederland kunnen schaden door een combinatie van nagestreefde doelen, gebruikte middelen en ressorterende effecten" (AIVD, MIVD, NCTV, 2025, p. 9). Onder hybride activiteiten wordt ook wel verstaan: "beïnvloedingsactiviteiten in zowel het fysieke als digitale domein, waaronder cyberaanvallen, heimelijke beïnvloedingsactiviteiten en sabotageacties" (AIVD & MIVD, 2026).

In de Trendanalyse Nationale Veiligheid uit 2024 is geschetst dat de afgelopen jaren de hybride dreiging vergroot is als gevolg van toegenomen grootmachtcompetitie. Deze trend heeft zich nu verder voortgezet. De schaal en frequentie waarmee steeds assertiever en agressiever wordende staten gebruik maken van hybride instrumenten is de afgelopen jaren sterk toegenomen. Bovendien schetsen de AIVD & MIVD (2026: 13) dat sprake is van een toegenomen risicobereidheid bij de Russische Federatie. Het korte dreigingsbeeld hybride en militaire dreigingen uit december 2024 vat de situatie als volgt samen: "In deze context kan Rusland als de grootste dreiging en China als de grootste uitdaging gezien worden" (AIVD & MIVD, 2024). Ook in het Dreigingsbeeld Statelijke Actoren 2025 wordt een soortgelijke conclusie getrokken: "Ten opzichte van het vorige DBSA uit 2022 is de dreiging op veel vlakken onverminderd sterk aanwezig gebleven en is de sabotagedreiging toegenomen. Geen enkele dreiging is afgenomen" (p. 9).

3.2.1 Bouwstenen

Hybride dreigingen zijn (per definitie) zeer divers van aard, omdat actoren op verschillende manieren gebruik maken van het hybride instrumentarium, met verschillende doeleinden voor ogen. Voor deze categorie is dan ook een overzicht van mogelijke actoren en factoren opgesteld die deze verscheidenheid reflecteert (zie onderstaande tabel). Deze dienen als 'bouwstenen' aan de hand waarvan scenario's binnen de categorie kunnen worden opgesteld.

Tabel 5 Bouwstenen 'Ongewenste buitenlandse beïnvloeding (hybride dreigingen)'[4]

Actor	Motief	Middel	Doelwit
Rusland	Beïnvloeden van beleid en standpunten (bijvoorbeeld over eigen systeem/beleid)	Diplomatie/Politiek Bijv. bevriezen dialoog; diplomatieke sancties; infiltratie; invloed via personen in politiek; ondermijnen internationale samenwerkingsverbanden; verdeel-en-heers tactieken.	Politiek Overheden, democratische instituties en processen, bondgenoot-schappen en internationale organisaties (bijv. EU/NAVO), politiek leiderschap
China	Vertrouwen in de overheid/politieke instituties aantasten	Informatie Bijv. publieksdiplomatie; digitale beïnvloeding; desinformatiecampagnes en propaganda; angst en	Militair Bijv. militaire bases, defensie-medewerkers, defensie industrie.

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

Actor	Motief	Middel	Doelwit
		vijandbeelden verspreiden; intimidatie of in diskrediet brengen van media, wetenschappers, diaspora, politici (*hack & leak* activiteiten); invloed uitoefenen via o.a. diaspora-gemeenschappen, sympathisanten en anderen.	
Iran	Alternatieve politiek-economische systemen populariseren/ liberale orde ondergraven	Militair Bijv. militaire intimidatie d.m.v. troepenopbouw; oefeningen aan de grens; schendingen luchtruim/territoriale wateren; inzet proxies/niet statelijke actoren; (digitale) sabotage.	Economisch bijvoorbeeld bedrijven, onderzoeks-instellingen, kennisinstituten, topsectoren
Noord-Korea	EU/NAVO uiteen drijven	Economisch Bijv. financiële steun; economische boycot; gerichte investeringen; geconditioneerde markttoegang; prijsmanipulatie; controle toegang tot (schaarse) resources; controle over vitale infrastructuur of strategische locaties; (digitale) (bedrijfs)spionage, opzetten van onderzoeksnetwerken/-instituten.	Sociaal Bijv. Nederlandse burgers/publieke opinie, wetenschappers, diaspora, geloofs-gemeenschappen, maatschappelijk middenveld
	Aanscherpen kwetsbaarheden tegenstander		Informatie Bijv. media, digitale dienstverleners
	Publieke opinie voor zich winnen/beïnvloeden beeldvorming/ kritiek snoeren op eigen systeem/beleid		Infrastructuur Bijv. nutsbedrijven, (lucht)havens, transportnetwerken, andere vitale infrastructuur.
	Behouden van een zekere mate van interne (binnenlandse) stabiliteit		
	Vergroten van onrust		

Allereerst proberen meerdere **actoren** andere staten te beïnvloeden. De voor Nederland belangrijkste actoren zijn Rusland en China, maar de lijst landen die zich in Nederland bedient van ondermijnende beïnvloeding is langer (AIVD, MIVD & NCTV, 2025: p. 31 e.v.). Het gaat daarbij om transnationale repressie tegen diaspora en ondermijnende beïnvloeding om beeldvorming te veranderen. Ook niet-statelijke actoren kunnen gebruik maken van verschillende instrumenten om hun doelen te bereiken, maar vallen voor de doeleinden van deze analyse buiten scope. In deze categorie bouwsteen wordt uitgegaan van een niet-uitputtende lijst statelijke actoren waar hybride dreiging vanuit kan gaan.

Daarnaast kunnen hybride actoren verschillende **motieven** hebben, waarmee de strategische doelen worden bedoeld. Kenmerkend aan hybride acties is dat ze vaak onderdeel zijn van een groter geheel, een overkoepelende operatie of campagne. De doelstelling van een specifieke actie kan dus anders zijn dan de strategische doelstelling van een actor, maar wel bijdragen aan deze strategische doelstelling. Belangrijk om te vermelden is dat het hier gaat om de intentie, het gewenste doeleinde. Een actie kan immers ook niet het beoogde effect blijken te hebben. In deze set bouwstenen zijn *gewenste* strategische doeleinden opgenomen. Ook is het niet zo dat hybride acties altijd als zodanig worden georkestreerd vanuit een campagne - en worden gepland in de tijd. Juist een hybride actor als Rusland ontplooit ook beïnvloedingsactiviteiten op basis van opportunisme en pragmatisme en speelt daarmee in op de situatie van het moment. Dat wil niet zeggen dat dergelijke opportunistische beïnvloedingsactiviteiten lukraak worden ingezet, de strategische doelstellingen blijven leidend.

Zoals gezegd kan een hybride actor een scala aan **middelen** inzetten om de doelen te bereiken. De lijst van middelen kan daarmee veel langer worden (en is dus niet uitputtend in de bouwstenentabel). De verschillende middelen kunnen wel ingedeeld worden in categorieën van middelen: diplomatiek en politiek, informatie, militair en economisch[5].

Tot slot worden de middelen ingezet tegen een specifiek **doelwit**. Ook hier geldt dat de lijst van mogelijke doelwitten erg lang kan zijn, vandaar dat ook de doelwitten per categorie zijn opgesomd in de tabel, met enkele voorbeelden: politiek, militair, economisch, sociaal, informatie en infrastructuur. Belangrijk om hierbij op te merken is dat een informatiemiddel niet per definitie ingezet hoeft te worden tegen een informatiedoelwit. Propaganda is bijvoorbeeld veelal bedoeld voor de bevolking en grijpt dus aan op een sociaal doelwit.

3.2.2 Het scenario 'Heimelijke beïnvloeding via een privaat bedrijf' – op aanvraag

In deze dreigingscategorie wordt één scenario beschreven waarin ongewenste buitenlandse beïnvloeding speelt. Daarnaast spelen op de

[5] Deze indeling wordt vaak gebruikt. In de literatuur worden allerlei verschillende indelingen in categorieën gehanteerd. Het door het JRC opgestelde conceptual framework betreffende hybride dreigingen hanteert bijvoorbeeld een gedetailleerdere indeling in Infrastructuur, Cyber, Space, Economy, Military/Defence, Culture, Social/Societal, Public administration, Legal, Intelligence, Diplomacy, Political, Information (Giannopoulos et al., 2021).

achtergrond van het combinatiescenario Oorlog in Europa ook beïnvloedingsactiviteiten die onderdeel zijn van de dreigingscategorie Ongewenste buitenlandse beïnvloeding. Ook in verschillende enkelvoudige scenario's spelen dreigingen die onderdeel kunnen zijn van een hybride dreiging, waaronder cyberspionage, georganiseerde criminaliteit en militaire intimidatie.

Het scenario vindt plaats in een veranderde geopolitieke situatie. China heeft tot doel de wereldorde aan te passen in lijn met de eigen antiwesterse en antidemocratische ideeën (AIVD, 2025a: 31). Het land ziet zichzelf ook in die nieuwe wereldorde als grootmacht. Verder is China voornemens om Taiwan volledig onderdeel van China te maken (MIVD, 2025: 16). Ook speelt in het scenario een rol dat de Verenigde Staten een voortgaande agressieve handelspolitiek voeren. Zo zijn invoerheffingen hoog en worden uiteenlopende andere handelsbeperkingen ingesteld. De Europese Unie heeft in het scenario een gedeeltelijk antwoord weten te formuleren op deze agressieve handelspolitiek – onderdeel daarvan is een uitgebreide handelsrelatie met China evenals een toename van samenwerking bij de ontwikkeling van innovatieve technologie.
Er wordt in het scenario nog steeds vertrouwd op de impliciete veiligheidsgaranties vanuit de VS inherent aan het NAVO-verdrag, tegelijkertijd wordt de Europese defensie stap-voor-stap versterkt. Door de aandacht voor economische veiligheid en voor het weglekken van hoogwaardige kennis zijn verschillende wetten in werking getreden in Nederland, waaronder de Wet Veiligheidstoets Investering, Fusies en Overnames (Wettenbank, 2025) en de Wet Screening Kennisveiligheid (Rijksoverheid, 2025).

3.2.2.1 Scenario: Heimelijke beïnvloeding via een privaat bedrijf

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

3.2.3 Beschouwing Ongewenste buitenlandse beïnvloeding (hybride dreigingen)

In het bovenstaande scenario worden de implicaties van het doorzetten van de reeds in gang gezette veranderingen in de geopolitieke verhoudingen tussen de Europese Unie, de Verenigde Staten en China geschetst. In dit specifieke geval speelt in feite dat Nederland van beide zijden onder druk wordt gezet. Zeker middelgrote en kleine landen zijn kwetsbaar voor het ondervinden van de effecten van grote geopolitieke dynamieken. Verder geldt dat het Koninkrijk op verschillende manieren last zou kunnen ondervinden van deze dynamiek. Daarbij kunnen incidenten in uiteenlopende sectoren aanleiding zijn voor een verslechtering van politieke en economische betrekkingen en kan ook de situatie in het Caribisch deel van het Koninkrijk een rol spelen. Zo zijn Chinese bedrijven actief in de Cariben en speelt het een rol dat de Verenigde Staten in zijn directe omgeving probeert Chinese (en Russische) invloed sterk te verminderen. Dit wordt als één van de achterliggende redenen genoemd voor de acties van de Verenigde Staten gericht op het Venezolaanse regime aan het begin van 2026.
In het scenario is daarnaast sprake van de inzet van een dekmantelbedrijf of een proxyorganisatie. Dit is karakteristiek voor hybride dreigingen, omdat deze modus operandi plausibele ontkenning

mogelijk maakt en het zo voor de statelijke actor mogelijk wordt van meer capaciteiten gebruik te maken. Specifiek voor China geldt bovendien dat onder de noemer van nationale veiligheid wetgeving is ingevoerd, waardoor alle Chinese organisaties en burgers verplicht zijn informatie over te dragen aan de overheid. Daarnaast zet de Chinese overheid bedrijven in staatseigendom directer in om doelen van de staat te dienen, waaronder het ontvreemden van technologie en andere nuttige informatie. Specifiek voor Rusland gaat het om de inzet van criminele groeperingen, ideologische of terroristische groeperingen en 'nuttige idioten' ten behoeve van observatie, vergaren van informatie, sabotage en meer langdurige inlichtingenoperaties. In het geval van Iran gaat het ook om relaties met criminele netwerken, zowel op het niveau van kopstukken als op het niveau van uitvoerders.

In dit scenario wordt een hybride dreiging primair ingezet als wijze van handelen om politiek, financieel-economisch en geopolitiek gewin te bereiken. In relatie tot militaire dreigingen staan echter vaak andere doelen centraal. Zo kan het creëren van maatschappelijke onrust, frustreren van besluitvorming voor effectieve respons ten tijde van een militaire crisis of fysiek verstoren van militaire mobiliteit of militaire operaties centraal staan. Met dat laatste doel in gedachten kan bijvoorbeeld de doorvoer van militaire goederen richting Oekraïne worden verstoord of ten tijde van grootschalige *host nation support* ten behoeve van NAVO-operaties kan militaire mobiliteit worden verstoord.

Zie het Combinatiescenario 'Oorlog in Europa' in het betreffende themarapport, waarin Rusland digitale en sabotage-aanvallen uitvoert op kritieke knooppunten en infrastructuur in Nederland om de taak als host nation ten aanzien van de doorvoer van (Amerikaans) materieel en personeel richting het front in Oekraïne te frustreren.

Ten slotte is het nuttig enkele observaties te doen die te maken hebben met de frequentie van optreden van componenten van het hierboven geschetste scenario en de waarschijnlijkheid van het gehele scenario. Zoals in het scenario wordt opgemerkt is reeds langere tijd sprake van grootschalige en langdurige inlichtingenoperaties en beïnvloedingscampagnes vanuit zowel China en Rusland. Het Dreigingsbeeld Statelijke Actoren 2025 spreekt[6] in relatie tot de spionagedreiging van een toename van het aantal landen dat spioneert in Nederland. Deze toename kan komen door verschuivingen in de wereldorde, maar ook door een verbeterd zicht van de inlichtingen- en veiligheidsdiensten op statelijke dreigingen. Ook verslechtering van politieke en niet-politieke betrekkingen na diplomatiek getouwtrek komt in werkelijkheid vaker voor en is dus zeer voorstelbaar.

3.3 Dreigingscategorie Spionage

Spionage is het op heimelijke wijze verzamelen van inlichtingen. Het doel kan bijvoorbeeld zijn om de politieke of economische situatie in een land in kaart te brengen, maar ook om bedrijfsgeheimen te stelen of om kennis over technologie te bemachtigen. Het komt tevens voor dat statelijke actoren op grote schaal persoonsgegevens verzamelen, met

[6] DBSA 2025, p. 23.

China als prominent voorbeeld. In het geval van China is deze activiteit onder andere gericht op het creëren van profielen van mensen werkzaam bij voor de Chinese overheid interessante bedrijven of instellingen, met als uiteindelijk doel het faciliteren van een (digitale) inbraak in de systemen van deze organisaties (AIVD, 2021). Zo heeft China zeer geavanceerde cyberaanvallen uitgevoerd op hoogtechnologische bedrijven (AIVD, 2025a). Spionage is iets van alle tijden en vormt een aanzienlijke bedreiging. Tegelijkertijd is spionage haast onzichtbaar en zijn weinig mensen zich bewust van de gevaren.

Het Koninkrijk der Nederlanden is een aantrekkelijk spionagedoelwit voor andere landen. Nederland is lid van de NAVO en van de EU en beschikt in die hoedanigheid over interessante informatie. Daarnaast is Nederland gastland van tal van internationale organisaties, zoals de Organisatie voor het Verbod op Chemische Wapens (OPCW), Europol, het Internationaal Gerechtshof (ICJ) en het Internationaal Strafhof (ICC). Ook de kennis en hoogwaardige technologie die Nederland als 'kenniseconomie' bezit, maken het land extra aantrekkelijk voor spionage. Om de dreiging die uit spionage voortkomt beter het hoofd te kunnen bieden, is in 2025 de Wet uitbreiding strafbaarheid spionageactiviteiten in werking getreden. Met deze wet is het strafrecht zo aangepast dat ook vormen van digitale spionage en 'diasporaspionage' voor een buitenlandse mogendheid expliciet strafbaar zijn (Rijksoverheid, 2025).

Allerlei actoren spioneren in en tegen Nederland om informatie of objecten te bemachtigen waarmee zij hun voordeel kunnen doen. Sommige landen spioneren op grote schaal en beschikken ook over geavanceerde inlichtingendiensten om dit werk uit te voeren. Deze buitenlandse inlichtingendiensten spioneren op verschillende manieren. Spionage kan plaatsvinden op de klassieke manier, door het benaderen van personen om via hen toegang te krijgen tot informatie – ook wel *human intelligence* of HUMINT genoemd. Medewerkers van geheime diensten zoeken continu naar interessante gesprekspartners (bronnen), zoals ambtenaren, militairen, wetenschappers, topfunctionarissen en journalisten. Zo werd in 2023 een Marokkaans-Nederlandse medewerker van de NCTV aangehouden op verdenking van het schenden van staatsgeheimen, al dan niet in opdracht van de Marokkaanse inlichtingendienst (AIVD, 2025a). Naast statelijke actoren proberen ook criminele netwerken, met hun eigen inlichtingenteams, doelbewust te infiltreren in onderdelen van de overheid om aan informatie te komen (AIVD, 2025a).

HUMINT blijft belangrijk binnen het spionagewerk. Wanneer iemand beschikt over interessante informatie en daarom opvalt bij een inlichtingendienst, proberen zij via een medewerker in contact te komen. Deze persoon zal proberen een vertrouwensrelatie op te bouwen. Hij of zij doet zich bijvoorbeeld voor als diplomaat, journalist of ondernemer om zo op een natuurlijke manier in contact te komen. Soms kan een glimp worden opvangen van dergelijke activiteiten: afgelopen jaren zijn tientallen Russische diplomaten officieel uitgezet omdat zij inlichtingenwerk verrichtten (NOS, 2023).

Er wordt ook veel digitaal gespioneerd. Digitale spionage, ook wel cyberspionage genoemd, is het (ongezien) stelen van informatie door binnen te dringen in geautomatiseerde systemen (AIVD, 2022a). Hierbij worden informatiesystemen gecompromitteerd, wat de integriteit van de digitale ruimte aantast. Staten zoals Rusland, China en Iran hebben een offensief cyberprogramma, onder andere gericht op het voor strategische doeleinden verwerven van gevoelige of vertrouwelijke informatie van andere staten, waaronder Nederland (AIVD, 2022a). De afgelopen jaren ontwikkelen steeds meer landen een offensief cyberprogramma, waarmee zij in staat zijn om cyberaanvallen uit te voeren (AIVD, 2025a). Via (cyber)spionage verkregen informatie kan, afhankelijk van de aard hiervan, door spionerende partijen onder andere worden ingezet voor het verbeteren van de concurrentiepositie van de eigen economie, het versterken van de eigen krijgsmacht of het beïnvloeden van processen en besluitvorming binnen internationale gremia. Dit gaat ten koste van de Nederlandse belangen. Cyberspionage kan als onderdeel van het hybride instrumentarium worden ingezet voor diverse doelen, zoals het verkrijgen van pressiemiddelen ten aanzien van andere statelijke actoren. Ook kan cyberspionage worden ingezet om waardevolle informatie te stelen, bijvoorbeeld over technologie of bedrijfsgeheimen. Klassieke en digitale vormen van spionage zijn verschillend in aard, maar kunnen ook in samenhang worden ingezet.

Onderzeese en vitale infrastructuur is een belangrijk spionagedoelwit. De inlichtingen- en veiligheidsdiensten wijzen al enkele jaren op het feit dat onderzoeksschepen van de Russische marine, maar ook schepen die op het eerste oog economische activiteiten ondernemen, spionageactiviteiten uitvoeren (Braw, 2024). Zo bouwt de Russische Federatie een situatiebeeld op van de positie van onderzeese infrastructuur, waarmee risico’s op sabotage van bijvoorbeeld energie- en internetnetwerken gepaard gaan. In veel gevallen is het echter juridisch uitdagend om dergelijke spionageactiviteiten af te schrikken (Sari, 2025).

Net als veel andere landen krijgt Nederland geregeld te maken met cyberspionage. Zo zijn er meerdere kritieke organisaties binnen Nederland succesvol aangevallen via een kwetsbaarheid in Citrix NetScaler (NCSC, 2025b). In 2020 probeerden statelijke actoren ook al gebruik te maken van een kwetsbaarheid in Citrix-VPN servers, die ook worden gebruikt door ambtenaren om vanuit huis op afstand in te loggen op het bedrijfsnetwerk van hun organisatie (AIVD & MIVD, 2021). In 2024 schreven de AIVD en de MIVD voor het eerst direct en in het openbaar een cyberaanval toe aan de Chinese staat. Uit deze aanval, onder andere gericht op een Nederlands defensienetwerk, blijkt de intentie om te spioneren bij de Nederlandse overheid en politieke doelwitten (AIVD, 2025a; NCSC, 2024). Sindsdien is nog een andere casus naar buiten gekomen waarbij een Chinese hackorganisatie, genaamd Salt Typhoon, betrokken was. Zij hebben, naast andere doelwitten binnen de wereldwijde telecomsector, toegang verkregen tot routers van Nederlandse doelwitten (AIVD, 2025b).

Actoren kunnen bij (cyber)spionage ook samenwerken met commerciële bedrijven. Aanbieders van cybermiddelen zijn in opkomst en de capaciteiten zijn inmiddels zeer geavanceerd (NCTV, 2024). Hierdoor

kunnen steeds meer actoren op relatief laagdrempelige wijze, capaciteiten opbouwen om te spioneren. Ook maken statelijke actoren in toenemende mate gebruik van zogenaamde "ORBnetwerken", een soort proxy-netwerk van gecompromitteerde apparaten, waarvan de infrastructuur door onafhankelijke partijen wordt verhuurd, waardoor digitale spionagecampagnes nog moeilijker te attribueren zijn (NCSC, 2025a).

De dreiging van cyberspionage wordt ook in toenemende mate gelinkt aan de afhankelijkheid van buitenlandse leveranciers voor hard- en software. Ook bijvoorbeeld applicaties uit landen met een offensief cyberprogramma tegen Nederland vormen een inherent spionagerisico (AIVD, 2023). Daarnaast groeien de maatschappelijke en politieke zorgen over de afhankelijkheid van buitenlandse technologiebedrijven die clouddiensten leveren. Een groot deel van de Europese data worden opgeslagen en verwerkt in de infrastructuur van enkele grote Amerikaanse aanbieders. Daardoor ontstaat een risico dat gevoelige of strategische informatie onder buitenlandse jurisdictie valt en dat daarmee mogelijkheden worden verschaft voor buitenlandse actoren om Europese staten onder druk te zetten (Gomes & Okano-Heijmans, 2024).

3.3.1 *Bouwstenen*

Binnen de dreigingscategorie 'Spionage' zijn er verschillende factoren die van invloed zijn op de ernst van de dreiging. Deze bouwstenen zijn in onderstaande tabel weergegeven.

Tabel 6 Bouwstenen 'Spionage'[7]

Actor	Motief	Middel	Doelwit
Rusland	Versterken van de (geopolitieke) machtspositie	Omkoping	Overheid (excl. Defensie)
China	Economisch gewin	Chantage	Defensie
Overige of niet gedefinieerde statelijke actor	Ideologische doelstelling	Infiltratie (fysiek)	Bedrijfsleven
Criminele actoren		Observatie (fysiek)	NAVO- of EU-bondgenoten
Statelijke proxy's		Malware-infectie	Internationale organisaties
Bedrijven		Social engineering (incl. phishing)	Kennis- of onderwijsinstellingen
Overig		Benutten ingebouwde achterdeuren in software of hardware	(Vitale) infrastructuur
		Misbruik van kwetsbaarheden	Overig
		Overig	

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

De **actor** beschrijft hierbij welke partij de spionageactiviteiten uitvoert. Spionage wordt vaak door statelijke actoren uitgevoerd, maar ook criminele groeperingen kunnen op heimelijke manier informatie vergaren voor hun activiteiten. In toenemende mate werken criminele groeperingen ook in opdracht van statelijke actoren of verkopen zij informatie die zij bij bijvoorbeeld een cyberaanval bemachtigen door aan staten. Ook bedrijven kunnen spionage plegen om informatie van concurrenten te stelen (al dan niet gesteund door een staat). Het **doel** betreft wat de actor wil bereiken. Hoewel het vaak niet direct duidelijk is wat het motief is van een actor, wordt spionage ingezet vanuit strategische doelen om bijvoorbeeld de economische en/of politieke positie te versterken. Het **middel**: geeft aan hoe de actor van plan is de doelen te verwezenlijken en het **doelwit** laat zien tegen wie of wat de middelen worden ingezet.

Voor de dreigingscategorie spionage zijn er drie scenario's uitgewerkt. Deze scenario's betreffen 'Klassieke Statelijke Spionage,' 'Cyberspionage' en 'Sabotage zeekabels Caribisch gebied voorbereid met spionage.'

3.3.2 Het scenario 'Klassieke Statelijke Spionage'

In het scenario 'Klassieke Statelijke Spionage' komt een Nederlandse majoor tijdens een internationale defensiebeurs in contact met een vertegenwoordiger van een Nederlands technologiebedrijf. Na enkele gesprekken krijgt de majoor het vooruitzicht aangeboden om als consultant bij het bedrijf aan de slag te gaan. Wat eerst onschuldig advieswerk leek, ontwikkelt zich echter geleidelijk tot een situatie waarin de majoor onder druk wordt gezet om staatsgeheimen prijs te geven. Later blijkt de vertegenwoordiger een buitenlandse inlichtingenofficier te zijn, waarna de majoor wordt gearresteerd op verdenking van spionage. In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario anti-institutionele enclaves gebouwd is.

Tabel 7 Bepalende bouwstenen voor het scenario 'Klassieke Statelijke Spionage'

Actor	Motief	Middel	Doelwit
Statelijke actor	Versterken van de (geopolitieke) machtspositie	Omkoping	Defensie
		Chantage	NAVO- of EU-bondgenoten

3.3.2.1 Scenario: Klassieke Statelijke Spionage

Een Nederlandse jachtvlieger wordt na een veelbelovende start van zijn militaire carrière geplaatst bij het 312 squadron op de vliegbasis Volkel. Hier dient de majoor "slechts" als wapeninstructeur en operatieofficier, waarbij hij verbonden is aan verschillende NAVO-initiatieven. Hoewel hij onder collega's bekend staat als vakbekwaam, leeft bij de majoor bitter ongenoegen over promoties die uitblijven. Innovaties waar hij aan werkt worden volgens hem onterecht tegengehouden, en zijn inbreng in NAVO-overleggen lijkt nauwelijks te landen.

Tijdens een bezoek aan een internationale defensiebeurs raakt de majoor in gesprek met een vertegenwoordiger van een Nederlandse technologiebedrijf. Het bedrijf, dat onder andere geavanceerde sensoren

en dronecomponenten ontwikkelt, is actief in meerdere NAVO-landen en levert aan zowel civiele als militaire afnemers. De vertegenwoordiger stelt zich voor als strategisch adviseur op het snijvlak van dronetechnologie en de militaire toepassingen daarvan.

De twee raken aan de praat over de interoperabiliteit van NAVO-systemen en de soms stroperige innovatiecultuur binnen Defensie. De twee voeren een geanimeerd gesprek over *'Loyal Wingman'*-drones en de kansen van de F-35 om met succes geïntegreerde luchtverdedigingssysteem binnen te dringen. De strategisch adviseur toont zich onder de indruk van de technische en tactische kennis van de majoor en vraagt of hij misschien vaker kort met hem wilt sparren voor een internationaal R&D-project.

De majoor gaat akkoord. Aanvankelijk betreft het louter theoretisch advieswerk onder het genot van een biertje en uitgebreide diners: de gesprekken gaan over de integratie van sensordata en verschillende technische aspecten van het Link 16-communicatiesysteem. Ook komen ze te spreken over de verschillende collega's die hij kent bij de MIVD, die potentieel ook wat voor het bedrijf zouden kunnen betekenen. Voor het eerst in lange tijd voelt de majoor zich gehoord en gewaardeerd om zijn kennis. De strategisch adviseur geeft aan dat hij bereid is om een rol open te stellen voor hem als consultant. Daarvoor moet hij echter wel een paar opdrachten op papier inleveren, zodat ook de CEO zijn mening kan vormen. Deze opdrachten worden 'via-via' geregeld en contact verloopt via versleutelde berichtenapps.

In de weken die volgen groeit het ongemak. De opdrachten worden technischer, gevoeliger. De informatie die de strategisch adviseur en zijn collega's opvragen raken aan geheime NAVO-procedures en -doctrines voor dronegebruik. Echter, omdat vergelijkbare documenten volgens hen ook op het internet te vinden zijn, gaat hij overstag. In de laatste opdracht wordt gevraagd naar gedetailleerde eigenschappen van de F-35A. Wanneer de majoor in eerste instantie voorzichtig weigert, insinueert de strategisch adviseur dat hij al in de problemen zit door zijn medewerking en dat hij maar beter kan blijven gehoorzamen als hij niet in de cel wil belanden. De majoor voelt zich in een hoek gedreven en geeft zich gewonnen.

Ruim een jaar na de internationale defensiebeurs krijgen de Nederlandse veiligheidsdiensten een bericht vanuit een buitenlandse collegadienst. Een buitenlandse inlichtingenofficier zou waarschijnlijk in Nederland actief zijn onder commerciële dekmantel. Onderzoek naar aanleiding van dit bericht brengt hen op het spoor van een 'strategisch adviseur' bij een Nederlands technologiebedrijf. Uiteindelijk blijkt dat de strategisch adviseur in werkelijkheid een officier is van een buitenlandse militaire inlichtingendienst, die zich jarenlang onder valse identiteit heeft weten te bewegen binnen westerse defensiekringen.

Tijdens het onderzoek naar het technologiebedrijf stuiten de diensten op enkele verdachte financiële transacties naar de majoor. Verdere analyse van logboekbestanden toont dat de majoor op onregelmatige momenten gevoelige documenten heeft geopend die buiten zijn directe taakgebied vallen, waaronder gedetailleerde specificaties van de F-35A. De majoor

wordt aangehouden op verdenking van spionage, maar van de strategisch adviseur ontbreekt ieder spoor.

Hoewel het technologiebedrijf geen kennis had van de ware identiteit van de strategisch adviseur en niet betrokken was bij de spionage, wordt het bedrijf na het uitlekken van het incident door media en publieke opinie met de zaak in verband gebracht. De suggestie dat het mogelijk betrokken was bij sanctieontwijking en export van dual-use-technologie naar statelijke rivalen leidt tot een diepe vertrouwenscrisis. Binnen enkele dagen verliest het beursgenoteerde bedrijf een fors deel van zijn marktwaarde en worden samenwerkingen met NAVO-partners tijdelijk stilgelegd.

Binnen Defensie leidt de onthulling tot grote onrust. Het feit dat een operationeel officier jarenlang ongezien toegang had tot gevoelige informatie en deze wist door te spelen legt pijnlijke kwetsbaarheden bloot. Er ontstaat een sfeer van wantrouwen onder personeel: collega's worden onder een streng toezichtsregime geplaatst en bestaande onderzoeksdossiers worden opnieuw tegen het licht gehouden. Binnen Defensie wordt een interne commissie opgetuigd die nog striktere richtlijnen opstelt, maar het gevoel van controleverlies blijft hangen. In de gangen van het ministerie klinkt de vraag die niemand hardop wil stellen: als dit zo lang onopgemerkt kon blijven—wat hebben we dan nog meer gemist? Ook binnen de NAVO laat het incident sporen na. De vertrouwensrelatie met Nederland komt onder druk te staan. Bepaalde werkzaamheden rondom de F35 mogen niet langer in Woensdrecht worden uitgevoerd, en bij gezamenlijke operaties groeit de aarzeling om gevoelige informatie te delen.

Wanneer officieren in andere NAVO-landen – waar het technologiebedrijf eveneens actief is – worden gearresteerd op verdenking van betrokkenheid bij soortgelijke spionagepogingen, is het duidelijk dat de strategisch adviseur slechts één pion was in een breder netwerk. De commerciële structuur rond het technologiebedrijf blijkt door buitenlandse inlichtingendiensten op meerdere fronten te zijn misbruikt als dekmantel. Wat begon als een individueel lek binnen de Nederlandse krijgsmacht, escaleert tot een internationale vertrouwenscrisis die de onderlinge samenwerking binnen NAVO op scherp zet.

3.3.2.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario 'Klassieke statelijke spionage'.

Tabel 8 Beoordelingstabel scenario 'Klassieke statelijke spionage'

Thema	Internationale en militaire dreigingen
Dreigingscategorie	Spionage
Scenario	Klassieke statelijke spionage
Scenariotoelichting	Een Nederlandse majoor gaat advieswerk leveren aan de strategisch adviseur van een Nederlands technologiebedrijf. Wat eerst onschuldig advieswerk leek, ontwikkelt zich geleidelijk tot een situatie waarin de majoor onder druk wordt gezet om staatsgeheimen prijs te geven.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		Toelichting
Waarschijnlijkheid:	E	Het scenario is zeer voorstelbaar en er zijn concrete aanwijzingen dat een dergelijk scenario geeffectueerd zou kunnen worden (zie bijvoorbeeld de uitzetting van Russische spionnen zowel in maart 2022 als in februari 2023) (Koster, 2023; Van Rosenthal & Van Rosenthal, 2022).

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	A	Er is sprake van een lichte aantasting van het Nederlandse imago omdat samenwerking op de F35 wordt ingeperkt binnen NAVO-verband. Aangezien verschillende landen eveneens een lek hebben gekend, is er echter geen grond om te stellen dat Nederland systematisch faalt in de bescherming van zijn informatie.
	1.3 Informatie en digitale ruimte	C	Ongewenste toegang tot informatie van een vitale aanbieder (Defensie) middels een *insider threat*, met een geopolitiek motief. Wel is er grip gekregen op de duur van de ongewenste toegang, wat de impact beperkt.
	1.4 Grondgebied EU en NAVO lidstaten	B	Er is sprake van heimelijk inzet van middelen, waaronder infiltratie in politiek-strategische functies en chantage van een functionaris van een vitale aanbieder (Defensie). De betreffende functionaris is zelf Nederlands, maar ook werkzaam binnen NAVO-verband en met toegang tot informatie van belang voor zowel Nederland als haar bondgenoten.
Fysiek	2.1 Doden	0	Niet van toepassing
	2.2 Ernstig gewonden en chronisch zieken	0	Niet van toepassing
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing
Economisch	3.1 Kosten	A	Door imagoschade van het bedrijf dat als commerciële cover diende zullen zij enig economisch verlies leiden
	3.2 Aantasting vitaliteit	0	Niet van toepassing
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	0	Niet van toepassing

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
	5.2 Aantasting democratische rechtsstaat	B	Beperkte aantasting van het functioneren van het openbaar bestuur (incl. ambtenaren) en het veiligheidssysteem via moedwillige chantage vanuit een buitenlandse mogendheid. De verwachting is dat de aantasting langer dan een half jaar duurt.
	5.3 Sociaal-maatschappelijke impact	A	Beperkte gevolgen merkbaar voor wat betreft de sociaal-maatschappelijke impact. Dit kan onder meer tot uitdrukking komen door negatieve media-aandacht, onrust op sociale media en maatschappelijke verontwaardiging.
Internationale rechtsorde	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	B	Het scenario kan leiden tot inperking van het gezag van een soevereine staat (bijvoorbeeld door middel van infiltratie). Aangezien in dit scenario de normbreker een permanent lid van de VN-Veiligheidsraad is wordt de score verhoogd van A naar B.
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Multilaterale instituties en internationale regimes	0	De interne werking en effectiviteit van de NAVO wordt niet direct aangetast, al is voorstelbaar dat het lekken van gevoelige technologische gegevens op termijn de afschrikwekkende werking van de NAVO richting Rusland kan aantasten.
	6.4 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.3.3 Het scenario 'Cyberspionage Rijksoverheid'

In dit scenario verkrijgt een staatsgelieerde hackersgroep via een kwetsbaarheid van het thuisnetwerk van een medewerker toegang tot het dataverkeer van het ministerie van Economische Zaken. Na de ontdekking wordt een groot onderzoek ingesteld, uit voorzorg worden systemen (tijdelijk) platgelegd en vervangen. Er ontstaat veel onrust bij de medewerkers van het ministerie, de burgers en ketenpartners. Het duurt uiteindelijk 6 maanden voordat de systemen van het ministerie volledig zijn opgeschoond.
In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario cyberspionage Rijksoverheid gebouwd is.

Tabel 9 Bepalende bouwstenen voor het scenario 'Cyberspionage Rijksoverheid'

Actor	Motief	Middel	Doelwit
Statelijke actor	Versterken van de (geopolitieke) machtspositie	Malware	Overheid (excl. Defensie)
	Economisch gewin	Social engineering (incl. phishing)	Defensie

Actor	Motief	Middel	Doelwit
		Misbruik van kwetsbaarheden	Bedrijfsleven
			NAVO- of EU-bondgenoten

3.3.3.1 Scenario: Cyberspionage Rijksoverheid

Op de laptops van meerdere medewerkers van het ministerie van Economische Zaken draait een Citrix-applicatie met een onbekende kwetsbaarheid. Door het hybride werken zijn deze systemen vaak verbonden met zowel het thuisnetwerk van de medewerkers als het interne netwerk van het ministerie. Via de kwetsbaarheid in de Citrix-applicatie weet de actor toegang te krijgen tot het netwerk. Na het verkrijgen van toegang installeert de actor malware op het netwerk, die zich verspreidt van het thuisnetwerk naar het interne netwerk van het ministerie zodra een medewerker verbinding maakt via Citrix. De geïnstalleerde malware is in staat om soft- en firmware-updates te overleven waardoor de actor langdurig en onopgemerkt toegang behoudt tot het netwerk van het ministerie.

Verschillende medewerkers van het ministerie rapporteren prestatieproblemen, zoals een tragere computer en vastlopende programma's. Als gevolg van deze toenemende meldingen start het incidentresponsteam een diepgaand onderzoek, waarbij de niet eerder bekende malware wordt ontdekt. Het ministerie schakelt direct diverse interne en externe experts in om een uitgebreid forensisch onderzoek op te starten. Om verdere verspreiding van de malware te voorkomen worden direct kritieke systemen platgelegd en vervangen. Dit leidt tot verstoring in de dienstverlening en verhoogde werkdruk voor de medewerkers van het ministerie. Al gauw na de detectie wordt vastgesteld dat het gaat om een buitenlandse staatsgelieerde hackersgroep, waardoor blijkt dat de aanval deel uitmaakt van een bredere trend van buitenlandse politieke spionage tegen het Koninkrijk en zijn bondgenoten.

Enkele uren na de ontdekking van de malware komt het incident in de media. Door de link met de zeer geavanceerd opererende buitenlandse hackersgroep ontstaat er veel onzekerheid over de aard en omvang van het incident onder burgers en ketenpartners. Het is onduidelijk wat de daders met de informatie van plan zijn en om welke informatie het precies gaat. Dit leidt tot speculatie, geruchten en desinformatie, vooral op sociale media.

Kort daarna blijkt dat de aanvallers de buitgemaakte informatie gebruiken om hun pogingen toegang te krijgen tot systemen van ketenpartners effectiever te maken, waaronder andere ministeries, vitale aanbieders, internationale organisaties en private bedrijven die samenwerken met het ministerie. Meerdere bedrijven uit de halfgeleider- en quantumindustrie melden (pogingen van) het plaatsen van malware en later ook datadiefstal en het verstoren van bedrijfsprocessen. Financiële schade treedt op bij de ketenpartners, doordat zij moeten investeren in herstel en forensisch onderzoek. Ketenpartners verliezen het vertrouwen in de beveiliging van het

ministerie en worden terughoudend in het delen van gevoelige informatie, toekomstige samenwerking komt onder druk te staan.

Niet alleen de ketenpartners verliezen langzamerhand hun vertrouwen in het ministerie. Enkele weken na de eerste mediaberichten verschijnen er op sociale media en in buitenlandse nieuwsmedia geruchten en (mogelijk gemanipuleerde) documenten die lijken te zijn gebaseerd op de gestolen informatie. De documenten suggereren dat militaire, diplomatieke en economische informatie is gelekt, wat leidt tot diplomatieke spanningen met andere landen, die hun samenwerking tijdelijk opschorten of extra eisen stellen aan informatie-uitwisseling. De reputatie van het ministerie en de Rijksoverheid als geheel komen onder druk te staan. Er ontstaat maatschappelijke onrust over de betrouwbaarheid van de overheid in het beschermen van vertrouwelijke informatie. Politieke druk wordt opgevoerd om verantwoording af te leggen en structurele verbeteringen door te voeren, dit wordt ook ervaren op de werkvloer door de medewerkers van de Rijksoverheid. Het duurt tot 6 maanden voordat de systemen van het ministerie volledig zijn hersteld en opgeschoond. In deze periode treft het ministerie meerdere maatregelen om het vertrouwen intern en extern te herstellen. Er wordt openlijk gecommuniceerd over de oorzaak, impact en de genomen maatregelen tijdens het incident. Daarnaast worden er structurele maatregelen verkondigd op technisch en beleidsmatig vlak die bijdragen aan het verhogen van de digitale weerbaarheid van het ministerie.

3.3.3.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario 'Cyberspionage Rijksoverheid'.

Tabel 10 Beoordelingstabel scenario 'Cyberspionage Rijksoverheid'

Thema	**Ongewenste inmenging en beïnvloeding democratische rechtsstaat**
Dreigingscategorie	Spionage
Scenario	Cyberspionage Rijksoverheid
Scenariotoelichting	Het scenario beschrijft een cyberspionage-incident als gevolg van een kwetsbaarheid van het thuisnetwerk van een medewerker van het ministerie van Economische Zaken.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	D	Er zijn aanwijzingen, zoals bestaande kwetsbaarheden in IT-systemen en spionage door statelijke actoren, die maken dat het zeer voorstelbaar is dat het scenario zal plaatsvinden.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing.
	1.2 Internationale positie	B	Twee categorieën binnen dit impactcriterium worden geraakt; spanning op diplomatieke samenwerking en gecoördineerde cyberaanvallen met spionagedoeleinde.
	1.3 Informatie en digitale ruimte	E	De zwaarste categorie organisaties wordt geraakt (overheid), daarbij worden ook vitale aanbieders getroffen waar het ministerie mee samenwerkt wat de schaal omvangrijk maakt. Tot slot is er sprake van een moedwillig motief.
	1.4 Grondgebied EU en NAVO lidstaten	0	Niet van toepassing.
Fysiek	2.1 Doden	0	Niet van toepassing.
	2.2 Ernstig gewonden en chronisch zieken	B	Het is voorstelbaar dat een deel van de medewerkers (enkele tientallen) van het ministerie behoefte heeft aan psychische zorg, door de ervaring van diplomatieke spanning, politieke druk om verantwoording af te leggen en de lange tijdsduur voordat de kwetsbaarheid volledig is verwijderd en de onzekerheid die dit met zich meebrengt.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing.
Economisch	3.1 Kosten	B	Naast materiële schade en herstelkosten door ongewenste toegang tot de ministeriële IT-systemen, is er enige financiële schade voor

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			ketenpartners door het lekken van vertrouwelijke informatie.
	3.2 Aantasting vitaliteit	0	Niet van toepassing.
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	A	Honderden mensen werkzaam binnen het ministerie en de getroffen ketenpartners kunnen tijdelijk hun werk niet uitvoeren.
	5.2 Aantasting democratische rechtsstaat	C	Medewerkers van het ministerie worden beperkt in hun werk waardoor het functioneren van het openbaar bestuur en daaraan verbonden ambtenaren in gevaar komt. Daarbij duurt het tot 6 maanden totdat de kwetsbaarheid volledig uit de systemen van het ministerie is verwijderd waarmee institutionele processen verstoord zullen worden. Daarbij is er sprake van moedwillige heimelijke beïnvloeding.
	5.3 Sociaal-maatschappelijke impact	A	Het is denkbaar dat er enige vorm van polarisatie ontstaat door het verlies van vertrouwen bij een deel van de bevolking in de overheid in het omgaan met cyberspionage. Het lekken van economische informatie kan ervoor zorgen dat enige onrust ontstaat tussen burgers en specifieke bedrijven.
Internationale rechtsorde & stabiliteit	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	B	Er is sprake van een beperkte schending van de staatssoevereiniteit door het saboteren/infiltreren van de digitale systemen van het ministerie. Daarbij is er sprake van moedwillig handelen door een statelijke actor waardoor de correctiefactor van +1 is toegewezen.
	6.2 Mensenrechten	0	Niet van toepassing.
	6.3 Multilaterale instituties en internationale regimes	0	In dit scenario is sprake van niet naleven van afspraken over de interactie tussen staten (het binnentreden van elkaars digitale systemen) door één van de permanente leden van de VN-Veiligheidsraad. Echter, cyberspionage gebeurt zo regelmatig dat het niet voorstelbaar is dat hierdoor multilaterale instituties worden ondermijnd.
	6.4 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing.

3.3.4 *Het scenario 'Sabotage zeekabels Caribisch gebied voorbereid met spionage'*

In dit scenario wordt besproken wat de gevolgen zijn van een spionagescenario in de Caribische zee, waarbij aantasting van de nationale veiligheid optreedt in zowel de landen in het Koninkrijk der Nederlanden als een bijzondere gemeente van Nederland in die regio. In de beschouwing wordt besproken wat de gevolgen zouden zijn van kleine of meer ontwrichtende sabotageacties uitgevoerd op basis van de verzamelde informatie.

In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerde, fictieve scenario sabotage zeekabels Caribisch gebied voorbereid met spionage gebouwd is.

Tabel 11 Bepalende bouwstenen voor het scenario 'Sabotage zeekabels Caribisch gebied voorbereid met spionage'

Actor	Motief	Middel	Doelwit
Venezuela	Voorbereiding militaire actie	Observatie (fysiek)	(Vitale) infrastructuur
Rusland	Versterken van de (geopolitieke) machtspositie	Infiltratie (fysiek)	Bedrijfsleven
		Misbruik van kwetsbaarheden	Overheid (excl. Defensie)
			Defensie

3.3.4.1 Scenario: Sabotage zeekabels Caribisch gebied voorbereid met spionage

Venezuela en de Russische Federatie werken nauw samen: ze zijn geopolitieke partners. De marines van beide landen ondernemen gezamenlijke oefeningen en de Russische marine gebruikt zowel Venezuela als Nicaragua en Cuba als steunpunten voor reisbewegingen door het Caribisch gebied. Venezuela heeft de afgelopen jaren ingezet op de doorontwikkeling van oceanografisch onderzoek in de Caribische Zee, waaronder ook in het Bonaire Bassin. Er worden bathymetrische[8] en oceaanstroming-metingen uitgevoerd.

Het onderzoek wordt uitgevoerd met een nieuw oceanografisch schip genaamd 'Guaiquerí III'. Venezuela geeft aan dat het belangrijk is de ecosystemen en biologie van de Caribische Zee te begrijpen – en dat het land daarom heeft geïnvesteerd in een nieuw schip. Voor de aanschaf en verdere ontwikkeling van het schip werkt het Venezolaanse oceanografisch instituut samen met een Russisch oceanografisch instituut.

De Venezolaanse 'Guaiquerí III' wordt gedurende enkele weken gezien in de wateren rond Curaçao en Bonaire. Het schip is actief in verschillende gebieden en voert daar uiteenlopende metingen uit. Echter worden ook op verschillende plekken verdachte bewegingen gezien via AIS- en radarobservatie door de Nederlandse marine. Het schip bevindt zich enkele uren direct boven de datakabel die van Curaçao via Aruba naar onder andere Puerto Rico loopt en dagen later ook enkele uren boven een datakabel tussen Curaçao en Trinidad & Tobago. Op basis

[8] Bathymetrie is het opmeten van de topografische hoogte van de zeebodem.

van deze eerste verdachte bewegingen wordt besloten tot nadere observatie van het schip. Aan boord van het schip blijken enkele Russische onderzoekers te zijn, waarvan het de vraag is of zij echt civiele onderzoekers zijn, of dat het Russische militairen of inlichtingenmedewerkers zijn.

Weer enkele dagen later vallen vrijwel tegelijkertijd de twee datakabels uit waar eerder observatie op is uitgevoerd. Eerst lijkt het mogelijk om internetverkeer om te leiden. Echter, wanneer toevallig op Curaçao ook uitval van elektriciteit optreedt, ontstaat gedeeltelijke uitval van verschillende telecommunicatiesystemen, waaronder telefoon- en vast en mobiele internetverkeer, zowel op Curaçao als op Puerto Rico en Trinidad & Tobago. Het lijkt er op dat bij de aanlandpunten van de zeekabels op het strand van Curaçao moedwillig grote beschadigingen zijn aangebracht, waardoor de datakabels zo zijn beschadigd dat deze niet meer functioneren. Bovendien wordt bij het aanlandpunt van de zeekabel van Curaçao naar Venezuela ook schade aangetroffen, echter functioneert die kabel nog wel naar behoren. In dezelfde periode blijkt een onderzeese explosie te hebben plaatsgevonden voor de kust van Curaçao; hier lijkt geen verdere schade aan infrastructuur bij te zijn ontstaan. Het Venezolaanse schip is echter al enige tijd vertrokken richting een Nicaraguaanse haven. Er is mogelijk ter afleiding gebruik gemaakt van eerder in stelling gebrachte explosieven. Na enkele uren, nadat de elektriciteitslevering weer is hersteld, lichten de autoriteiten het publiek toe hoe het incident naar verwachting is ontstaan.

3.3.4.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario ‘Sabotage zeekabels Caribisch gebied voorbereid met spionage’.

Tabel 12 Beoordelingstabel scenario 'Sabotage zeekabels Caribisch gebied voorbereid met spionage'

Thema	**Ongewenste inmenging en beïnvloeding democratische rechtsstaat**
Dreigingscategorie	Ongewenste buitenlandse beïnvloeding (hybride dreigingen)
Scenario	Sabotage zeekabels Caribisch gebied voorbereid met spionage
Scenariotoelichting	Dit scenario beschrijft spionage- en sabotagehandelingen gericht op enkele datakabels tussen verschillende eilanden in de Caribische zee uitgevoerd door Rusland en Venezuela.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	B	Het scenario wordt gezien als onwaarschijnlijk: er zijn eenvoudiger manieren om een soortgelijk effect te bereiken, gelijktijdige uitval van data en elektra maakt het minder waarschijnlijk, en er is op dit moment een gebrek aan directe intentie. Het is overigens wel voorstelbaar dat de intentie toeneemt wanneer bijvoorbeeld oorlog in Europa plaatsvindt, omdat dan ter afleiding een incident in de Cariben wordt veroorzaakt.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	A	Er worden geen diplomatieke acties verwacht, ook al ondervinden Puerto Rico en Trinidad & Tobago effect van elektriciteitsuitval binnen het Koninkrijk der Nederlanden. Er vindt een sabotageactiviteit plaats, waardoor het aanzien van het Koninkrijk in het buitenland wordt aangetast, dus wordt op de vierde categorie van de indicatoren een beperkte aantasting gezien.
	1.3 Informatie en digitale ruimte	0	Omdat er geen oneigenlijk toegang tot informatie noch de digitale ruimte ontstaat, er is ten slotte sprake van uitval, wordt geen aantasting verwacht. Digitale toegang is ten slotte niet mogelijk want de digitale ruimte is niet toegankelijk.
	1.4 Grondgebied EU en NAVO lidstaten	B	Er wordt heimelijke inzet van middelen in ieder geval onder militaire aansturing gezien, waarbij de aanlandpunten die worden beschadigd zich binnen het territorium van het Koninkrijk bevinden.
Fysiek	2.1 Doden	0	Onder sommige omstandigheden zijn enkele doden voorstelbaar – met name daar waar geen noodaggregaten voorhanden zijn en het weer toevallig bovengemiddeld warm is. De uitval van elektriciteit komt echter vaker voor en is geen specifiek uitvloeisel van dit scenario.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
	2.2 Ernstig gewonden en chronisch zieken	0	Onder sommige omstandigheden zijn enkele gewonden voorstelbaar – met name daar waar geen noodaggregaten voorhanden zijn en het weer toevallig bovengemiddeld warm is. De uitval van elektriciteit komt echter vaker voor en is geen specifiek uitvloeisel van dit scenario.
	2.3 Gebrek primaire levensbehoeften	0	Door uitval van elektriciteit zijn uitvallen van gezondheidszorg, voeding- en medicijnenimport enzovoort voorstelbaar. Echter zal de duur beperkt zijn.
Economisch	3.1 Kosten	A	Door materiële schade aan de kabels dienen reparatiekosten te worden gemaakt. Deze kosten zijn naar verwachting beperkt, omdat de schade primair op het strand is opgetreden, maar ook omdat doorgaans een verzekering wordt afgesloten. Verder treden economische kosten op door uitval van elektra en telefoon- en internetverkeer. Ten slotte worden bestrijdingskosten gemaakt door de inzet van observatiemiddelen, waaronder een marineschip. Het is niet plausibel dat deze kosten boven € 100 miljoen uitkomen.
	3.2 Aantasting vitaliteit	0	Niet van toepassing
Ecologisch	4.1 Aantasting beschermwaardige natuur	0	De onderzeese explosie is zeer lokaal, waardoor geen substantieel effect op milieu en natuur plaatsvindt.
	4.2 Aantasting milieu en natuur in algemene zin	0	De onderzeese explosie is zeer lokaal, waardoor geen substantieel effect op milieu en natuur plaatsvindt.
Sociaal-politiek	5.1 Verstoring dagelijks leven	0	Uitval van elektriciteit en telecom veroorzaakt enige verstoring van het dagelijks leven. Het is echter te verwachten dat de elektriciteitsuitval na vier tot acht uur weer gemitigeerd is. Vanaf dat moment kan de telecommunicatie omgeleid worden. De verstoring van het dagelijks leven door de telecomuitval zal dus naar verwachting minder dan een halve dag duren. Daardoor geldt geen aantasting van de nationale veiligheid.
	5.2 Aantasting democratische rechtsstaat	0	Niet van toepassing
	5.3 Sociaal-maatschappelijke impact	A	Enige boosheid over de kwetsbaarheid van vitale processen wordt verwacht. Drijfveer voor deze boosheid is bovendien initiële onduidelijkheid over wie de sabotageactie heeft uitgevoerd, onzekerheid over voorkomen van kabelsabotage in de toekomst, evenals het feit dat statelijke actoren zich richten op sabotage op Curaçao.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Internationale rechtsorde	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	B	Het gezag van een soevereine staat wordt ingeperkt, en wel door een P5-staat te weten de Russische Federatie (+1).
	6.2 Mensenrechten	0	Niet van toepassing
	6.3 Multilaterale instituties en internationale regimes	C	De Russische Federatie ondermijnt in het scenario de basisbeginselen van de internationale rechtsorde, meer specifiek het UNCLOS-regime.
	6.4 Instabiliteit rondom Koninkrijk/EU	0	Niet van toepassing

3.3.5 Beschouwing spionage

Alhoewel het binnen de dreigingscategorie spionage veelal gaat om relatief kleinschalige gebeurtenissen, zoals bijvoorbeeld het omkopen van een enkele medewerker van Defensie, kunnen de gevolgen wel degelijk groot zijn met implicaties voor de nationale veiligheid. Welke veiligheidsbelangen het meest worden geraakt, hangt sterk af van het type informatie dat wordt verkregen en het doel van de operatie. Maar het hangt ook af van de actor die deze informatie in handen krijgt. De AIVD en MIVD vragen al langere tijd aandacht voor digitale spionagepogingen van onder andere statelijke actoren bij Nederlandse ministeries (AIVD & MIVD, 2021). Tegelijkertijd ontwikkelen ook commerciële partijen steeds geavanceerdere spionagemiddelen, waardoor er steeds meer actoren achter spionageactiviteiten kunnen zitten. Risico's rond (cyber)spionage voedt ook de maatschappelijke en politieke discussie over strategische (digitale) autonomie. Opvallend is dat de waarschijnlijkheid van zowel cyberspionage als klassieke spionage relatief hoog wordt ingeschat – respectievelijk met scores D en E (waarschijnlijk tot zeer waarschijnlijk). De ontwikkelingen binnen deze dreigingscategorie en de analyse van de scenario's tonen dan ook de prangende actualiteit aan van (cyber)spionage.

Tegelijkertijd is het niet eenvoudig om de impact van (cyber)spionage op de nationale veiligheid te duiden. Zo is het meestal onzeker welke informatie er door welke actor is buitgemaakt en waarvoor de actor deze informatie wil inzetten. De economische waarde van specialistische kennis, die buit kan worden gemaakt uit kennisinstellingen zoals (technische) universiteiten, is moeilijk in te schatten. Ook kunnen situaties lang onder de radar blijven. Daardoor is het bijvoorbeeld lastig om de economische impact van spionage in te schatten: want wat heeft een spionerende actor precies gehad aan buitgemaakte informatie bij het ontwikkelen van een nieuw product? Ook kan een spionerende actor belangrijke buitgemaakte informatie achter de hand houden, om op een voor de actor in kwestie opportuun moment in te zetten. Op deze wijze kunnen bijvoorbeeld internationale onderhandelingsprocessen worden beïnvloed. Spionage kan ook grote maatschappelijke gevolgen hebben.

Zo zou bijvoorbeeld het vertrouwen van de samenleving in de overheid kunnen worden geschaad door een omvangrijk informatielek.

Niet enkel het vertrouwen van de samenleving in de overheid, maar ook het vertrouwen binnen en tussen departementen kan worden geschaad door spionage. Wanneer er sprake is van (cyber)spionage, kan er bijvoorbeeld (uit voorzorg) minder informatie worden gedeeld tussen verschillende afdelingen of departementen. Ook kunnen er onnodig veel extra obstakels worden gecreëerd voor gegevenstoegang, wat op de lange termijn samenwerking beperkt, maar nog altijd een *'insider threat'* niet volledig kan uitsluiten. Zeker in de aanpak van interdepartementale problematiek, waaronder inmenging en beïnvloeding in de democratische rechtsorde, zou dit een obstakel kunnen vormen voor een effectieve aanpak.

Verder is spionage en sabotage van onderzeese infrastructuur tegenwoordig aan de orde van de dag en is het van belang hier blijvend aandacht op te vestigen. Enkele incidenten die in de afgelopen jaren zijn waargenomen, zijn de internetkabelbreuk bij Spitsbergen (2021), het Nordstream-II-incident (2022) en het Newnew Polar Bear-incident (2023) in de Oostzee waarbij gasinfrastructuur beschadigd raakte en het Eagle S-incident bij Finland waarbij internetinfrastructuur beschadigd raakte (Braw, 2024). De waarschijnlijkheid van dit scenario is echter laag om enkele redenen: er zijn eenvoudigere manieren om een maatschappij-ontwrichtend effect te bereiken (zoals sabotage van infrastructuur op land), er is op dit moment geen heldere intentie te verbinden aan een actie gericht op het Caribisch deel van het Koninkrijk en gelijktijdige uitval van data en elektriciteit treedt nu eenmaal minder snel op. De waarschijnlijkheid van het optreden van dit scenario zou hoger zijn, wanneer het oorlog is in Europa, omdat het dan in het belang van de dreigingsactor is militaire eenheden aan het Caribisch deel van het Koninkrijk te binden. De impact van een dergelijk scenario in het Caribisch deel van het Koninkrijk is relatief groot, omdat de eilanden met een kleiner aantal datakabels zijn verbonden dan Europees Nederland.

Twee andere variaties op het scenario zijn van belang. Ten eerste, het soort sabotageacties dat hier is opgenomen, heeft in Europa plaatsgevonden op de Oostzee, maar zou ook op de Noordzee voorstelbaar zijn. Als dit type incident op de Noordzee optreedt, is de verwachting dat daadwerkelijke uitval van vitale processen beperkt kan blijven. Daarbij spelen zowel redundantie van telecominfrastructuur als het zeer lage uitvalpercentage van elektriciteitsinfrastructuur in Nederland een rol. Een laatste mogelijke variatie is dat in plaats van een relatief beperkte uitval, een kritiek kruispunt in onderzeese infrastructuur wordt aangegrepen en reparatie ook niet op korte termijn haalbaar is. In dit geval is het voorstelbaar dat (veel) grotere en meer langdurige uitval van vitale processen optreedt – en dus ook verstoring van het dagelijks leven, grootschalige maatschappelijke onrust door zowel onduidelijkheid omtrent attributie als door de uitval. Dus treedt significante impact op de nationale veiligheid op.

Ten slotte heeft de reactie vanuit de Nederlandse overheid in dit type scenario's belangrijke implicaties voor de algemene afschrikking wat

betreft sabotageacties op zee. Door te reageren, te observeren en eventueel actie te ondernemen wordt enerzijds getoond dat toereikend wordt gehandeld om actie voorkomen, terwijl anderzijds ook essentiële informatie voor een tegenstander beschikbaar komt waarmee een volgende actie effectiever kan worden.

3.4 Dreigingscategorie Ongewenste buitenlandse inmenging

In deze tijd van voortschrijdende internationalisering raken interne en externe veiligheid steeds meer met elkaar verknoopt. De thematiek rondom ongewenste buitenlandse inmenging in brede zin is hiervan een duidelijk voorbeeld. Onder ongewenste buitenlandse inmenging verstaat men de inmenging van statelijke actoren die zich specifiek richt op het functioneren van de democratische rechtsorde en open samenleving (NCTV, 2025b). Ongewenste buitenlandse inmenging kan schade toebrengen aan de integriteit van het Nederlands bestuur als deze de onafhankelijke volksvertegenwoordiging of rechtsspraak compromitteert, of als deze twijfel doet ontstaan over de vrijheid en eerlijkheid van verkiezingen. Wanneer ongewenste buitenlandse inmenging zich richt op het creëren van tegenstellingen of vijandelijkheden tussen bevolkingsgroepen, heeft dit de potentie om de maatschappelijke stabiliteit te ondermijnen. De meest prominente recente voorbeelden van ongewenste buitenlandse inmenging zijn:

- Desinformatiecampagnes, met name rondom verkiezingen en grote internationale kwesties;
- Deelname in of overname van vitale sectoren van de economie;
- Inmenging in diasporagemeenschappen.

Terwijl voorgaande dreigingscategorieën zich hebben gebogen over hybride (desinformatie)campagnes en economische inmenging, richt de huidige dreigingscategorie zich op inmenging in diasporagemeenschappen. Inmenging in diasporagemeenschappen is een vorm van ongewenste buitenlandse inmenging die in Nederland al diverse keren in het middelpunt van de belangstelling heeft gestaan. In Nederland gaat het in ieder geval om de volgende groepen:

- De Turks-Nederlandse gemeenschap. Onder ander het ronselen van stemmen rondom verkiezingen in Turkije en de intimidatie van politieke tegenstanders (met name na de couppoging in Turkije in 2016) (Houtkamp et al., 2024a).
- De Marokkaans-Nederlandse gemeenschap. Onder andere de intimidatie van politieke tegenstanders en de beïnvloeding van prominente leden van de Marokkaans-Nederlandse bestuurlijke elites om de belangen van Marokko te behartigen (Kahmann & Bellaart, 2025);
- De Russisch-Nederlandse gemeenschap. Onder andere door intimidatie of stevige beïnvloeding vanuit door het Kremlin gefinancierde instellingen (Houtkamp & Drost, 2023).
- De Eritrees-Nederlandse gemeenschap. Onder andere de gedwongen afdracht van financiële middelen naar Eritrea, de zogenaamde ‘diaspora-taks’ (Bellaart & Kahmann, 2024);
- De Chinees-Nederlandse gemeenschap. Onder andere de monitoring van Chinese studenten in Nederland (D’Hooghe en Dekker, 2020; Pieke, 2021);

- De Iraans-Nederlandse gemeenschap. Gericht maar zeer gewelddadig, soms dodelijk, optreden tegen politieke tegenstanders (AIVD, 2019; Ministerie van Buitenlandse Zaken, 2023).

3.4.1 *Bouwstenen*

Binnen de dreigingscategorie 'Ongewenste buitenlandse inmenging' zijn er verschillende factoren die van invloed zijn op de ernst van de dreiging. Deze bouwstenen zijn in onderstaande tabel weergegeven.

Tabel 13 Bouwstenen 'Ongewenste buitenlandse inmenging'[9]

Doelen	Middelen	Doelwit
Controle op eigen etnische of religieuze gemeenschap verkrijgen en uitoefenen	Angst en vijandsbeelden verspreiden	Eigen etnische of religieuze gemeenschap
Financieel/economisch gewin	Bevolkingsgroepen tegen elkaar opzetten/ bewust polarisatie veroorzaken	Diasporagemeenschappen
Politieke of maatschappelijke gunsten/voordelen verkrijgen	Legitimiteit van de overheid ter discussie stellen en in de praktijk ondergraven	Overheden (landelijk of lokaal)
Politieke invloed verkrijgen	Chantage	Minderheden
	Intimidatie	Media
	(Heimelijke) beïnvloeding	Westerse wereld/EU
	Vertrouwen in de overheid van ontvangend land aantasten; legitimiteit van overheid in ontvangend land ondergraven	
	Propaganda via klassieke en sociale media	
	Desinformatie via klassieke en sociale media	
	Rekruteren van personen	
	Intredepolitiek/met verborgen agenda lidmaatschap verkrijgen van politieke partijen, gemeenteraden, overlegorganen van de overheid, e.d.	

Bij **doelen** gaat het er hierbij om wat de actor wil bereiken met de ongewenste buitenlandse inmenging. De **middelen** geven aan hoe de actor van plan is de doelen te verwezenlijken en het **doelwit** geeft aan tegen wie de middelen worden ingezet.

Binnen deze dreigingscategorie is er één scenario uitgewerkt: 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland.'

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

3.4.2 *Het scenario 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland'*

De Nederlandse overheid heeft vanaf 2019 stappen gezet om ongewenste buitenlandse inmenging in diaspora-gemeenschappen effectief te monitoren en aan te pakken (NCTV, 2025a). Het dossier blijft vanwege de complexe interactie tussen de binnenlandse situatie en geopolitieke belangen echter ingewikkeld. Nederlanders die in opiniepeilingen zeggen zich sterk verbonden te voelen met lokale gemeenschappen ('*somewheres*'; ongeveer de helft van de bevolking) zien buitenlandse inmenging inmiddels als de belangrijkste internationale bedreiging voor de nationale veiligheid en brede welvaart (Sie Dhian Ho et al., 2025). Binnen diasporagemeenschappen reageert men vaak verdeeld op de bemoeienis vanuit het voormalige moederland (Houtkamp en Drost 2023; Houtkamp et al., 2024a). Tegelijkertijd hecht Nederland vanwege geopolitieke redenen groot belang aan de relatie met sommige 'afzendende landen' van inmenging.

In onderstaande tabel zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland gebouwd is.

Tabel 14 Bepalende bouwstenen voor het scenario 'ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland'

Doelen	Middelen	Doelwit
Controle op eigen etnische of religieuze gemeenschap verkrijgen en uitoefenen	Angst en vijandsbeelden verspreiden	Eigen etnische of religieuze gemeenschap
Politieke of maatschappelijke gunsten/voordelen verkrijgen	Bevolkingsgroepen tegen elkaar opzetten/ bewust polarisatie veroorzaken	Diasporagemeenschappen
Politieke invloed verkrijgen	Legitimiteit van de overheid ter discussie stellen en in de praktijk ondergraven	Minderheden
	Intimidatie	
	(Heimelijke) beïnvloeding	
	Vertrouwen in de overheid van ontvangend land aantasten; legitimiteit van overheid in ontvangend land ondergraven	

3.4.2.1 Scenario: Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland

Al tijden groeit in Nederland het ongemak over buitenlandse inmenging in diasporagemeenschappen. De Tweede Kamer tracht het toezicht op verschillende instituten die onderdeel uitmaken van het 'diasporalandschap' te versterken. De controle op weekendscholen en ander informeel onderwijs is inmiddels behoorlijk aangescherpt, na jaren van stevige politieke discussie. Sommige politieke partijen pleiten ervoor om een stap verder te gaan, en ook diaspora-gerelateerde culturele evenementen en gebedshuizen aan soortgelijke wetgeving te onderwerpen.

Ondertussen groeit de onrust in een land in de ring rond Europa. Politieke tegenstanders van de huidige regering zien de, in hun ogen, verdere ontmanteling van hun democratie met lede ogen aan. Velen vertrekken naar Europa, waaronder naar Nederland. Het land, dat als vanouds intensieve relaties onderhoudt met zijn gemeenschap in Nederland, ziet het massale vertrek van opponenten (inmiddels meer dan 20.000 in één jaar tijd) naar Nederland als een bedreiging. Er gaan hardnekkige geruchten dat het land de monitoring van politieke tegenstanders in de diaspora behoorlijk intensiveert, om broeinesten van oppositie in de kiem te smoren. Binnen de gemeenschappen nemen paranoïde gevoelens sterk toe. De klassieke kloof tussen aanhangers van regering, oppositie en niet-stemmers verscherpt: mensen durven steeds minder over politiek te spreken, uit angst voor represailles vanuit het moederland.

De Nederlandse regering wordt vanuit de politiek en maatschappij steeds meer onder druk gezet om te handelen, maar ziet nog onvoldoende aanleiding om in te grijpen. Die situatie verandert wanneer het land wordt opgeschrikt door een ingelaste tv-toespraak van de president aldaar. Hij kondigt aan dat er, net als meerdere keren in het verleden, een couppoging tegen de regering is verijdeld. Om het land te 'zuiveren van verraders' geeft hij opdracht prominente oppositiepolitici, journalisten, wetenschappers en activisten te laten oppakken en berechten. Europese experts tonen zich sceptisch. Zij duiden het 'nieuws' als een volgende aanval van de president op de democratische rechtsstaat.

Het nieuws slaat in als een bom in de diasporagemeenschap in Nederland: men denkt terug aan eerdere jaren, toen oppositie-aanhangers op de korrel werden genomen door andere leden van de diaspora. Cruciaal verschil is nu dat de oppositie, die nu een stuk omvangrijker is, in Nederland zich veel luider verzet. Volgende op de demonstraties ontstaan talrijke opstootjes en gewelddadige incidenten binnen de gemeenschap. Het wordt steeds duidelijker dat het moederland zich met deze opstootjes bemoeit: vanuit de ambassade worden opruiende teksten verspreid om de eigen aanhang op te hitsen en er zijn berichten dat het land infiltreert in de gemeenschappen om oppositieleden op het spoor te komen. De ambassade beschuldigt Nederland er openlijk van terrorisme te faciliteren, omdat Den Haag niet wil meewerken aan het monitoren en uitleveren van prominente oppositieleden.

Voor de Nederlandse overheid is de maat nu vol: zij reageert met stevige binnenlandse en diplomatieke maatregelen. De monitoring van de aan het andere land gelieerde culturele en religieuze instellingen wordt met onmiddellijke ingang geïntensiveerd. Demonstraties worden hardhandig opgebroken door de politie. Buitenlandse Zaken ontbiedt de ambassadeur. Binnenskamers wordt de Nederlandse regering gerustgesteld maar in een interview enkele dagen na de ontmoeting beschuldigt de ambassadeur Den Haag van het faciliteren van terrorisme. De ambassadeur eist de uitlevering van honderden oppositieleden die recent naar Nederland zijn gevlucht. De Europese bondgenoten roepen ondertussen achter de schermen de Nederlandse overheid op tot kalmte: het andere land is immers een cruciale speler in

de Europese veiligheidsarchitectuur. Sommige bondgenoten pleiten er zelfs voor om de meest vocale oppositieleden misschien tóch uit te leveren, als diplomatiek gebaar.

De onrust bereikt een kookpunt wanneer een prominent oppositielid in Nederland wordt ontvoerd. Het is niet hard te maken of het moederland hier de hand in heeft: wel is duidelijk dat de operatie is uitgevoerd door een criminele organisatie. Er ontstaat een mediastorm: de roep om nog stevigere maatregelen tegen buitenlandse inmenging om de bedreigde gemeenschap te beschermen neemt hand over hand toe. De demonstraties tegen de regering van het andere land worden ook steeds drukker bezocht, zowel door leden van de diaspora als andere Nederlanders. Overheid en politiek staan voor een moeilijke balanceer-act: hoe kunnen zij de onrust in Nederland beheersen zonder het andere land als bondgenoot en ook de Europese partners van zich te vervreemden?

3.4.2.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland'.

Tabel 15 Beoordelingstabel scenario 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland'

Thema	**Ongewenste inmenging en beïnvloeding democratische rechtsstaat**
Dreigingscategorie	Ongewenste buitenlandse inmenging
Scenario	Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland
Scenariotoelichting	Wanneer de onrust in een land in de ring rond Europa groeit, vertrekken veel politieke tegenstanders naar Nederland. Het moederland ziet dit al bedreiging en versterkt de beïnvloeding op de diasporagemeenschap in Nederland. Deze beïnvloeding en de gevolgen hiervan lopen dusdanig ver op dat er spanning ontstaan tussen de Nederlandse regering en de regering van het andere land.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)	**Score**	**Toelichting**
Waarschijnlijkheid:	D	Nederland heeft diverse diasporagemeenschappen, die intern politiek divers zijn. Deze zijn verbonden met potentieel instabiele landen. Daarmee zijn de bouwblokken aanwezig om dit scenario in gang te zetten als de situatie in een van die landen destabiliseert.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	0	Niet van toepassing
	1.2 Internationale positie	A	De internationale positie wordt geschaad vanwege gewelddadige operationele activiteiten van proxy-organisaties van statelijke actoren op Nederlandse bodem

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
	1.3 Informatie en digitale ruimte	0	Niet van toepassing
	1.4 Grondgebied EU en NAVO lidstaten	0	Niet van toepassing
Fysiek	2.1 Doden	0	Niet van toepassing
	2.2 Ernstig gewonden en chronisch zieken	A	Gewelddadige incidenten leiden tot gewonden
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing
Economisch	3.1 Kosten	0	Voorstelbare maar niet onvermijdelijke kosten voor de monitoring en beveiliging van gebedshuizen en culturele centra.
	3.2 Aantasting vitaliteit	0	Niet van toepassing
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	A	Een beperkte groep mensen durft geen gebruik meer te maken van culturele en religieuze voorzieningen omdat zij zich bedreigd voelen door buitenlandse monitoring.
	5.2 Aantasting democratische rechtsstaat	B	Burgers voelen zich beperkt in hun vrijheid van meningsuiting en geloofsbelijdenis doordat zij gemonitord worden door aanhangers van de buitenlandse regeringspartij. Omdat een buitenlandse mogendheid hier moedwillig op aanstuurt (+1 van de score: A wordt een B).
	5.3 Sociaal-maatschappelijke impact	B	Structurele spanning tussen rivaliserende groepen binnen de diaspora. Het effect zit nog op groepsniveau daarom score B. Er is enige ontwikkeling op bevolkingsniveau, omdat de bevolking één groep meer lijkt te steunen. Echter heeft dat nog geen structureel effect van uitsluiting.
Internationale rechtsorde	6.1 Staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting	0	Niet van toepassing
	6.2 Mensenrechten	C	Burger- en politieke rechten worden aangetast. Door de scherpe autoritaire wending wordt op grote schaal de oppositie onderdrukt.
	6.3 Multilaterale instituties en internationale regimes	0	Niet van toepassing

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
	6.4 Instabiliteit rondom Koninkrijk/EU	A	Persvrijheid en oppositie worden op aanzienlijke schaal beperkt. De sociale en politieke onrust die dat tot gevolg heeft, leidt tot enige instabiliteit in een land rondom de EU.

3.4.3 Beschouwing Ongewenste buitenlandse inmenging

Ongewenste buitenlandse inmenging is een complex, politiek gevoelig fenomeen omdat hier bij uitstek buitenlandse en binnenlandse spanningen samenkomen. Het is in dat licht niet verwonderlijk dat incidenten gerelateerd aan ongewenste buitenlandse inmenging vaak leiden tot een stevig maatschappelijk debat. Voorbeelden zijn er te over: de vanuit Teheran georganiseerde moorden op Iraanse oppositieleden in de jaren 2010, het incident met de Turkse minister in Rotterdam in 2017, de intimidatie vanuit Moskou tegen de Russisch-orthodoxe kerk in Amsterdam in 2022, de rellen in Den Haag tussen vertegenwoordigers van de Eritrese gemeenschap in 2024 en mogelijk ook de aanslag op een Iraanse politieagent in 2026. Deze lijst is verre van uitputtend.

Een effectieve beleidsreactie houdt voortdurend rekening met de perspectieven van vier grote partijen: de betreffende diasporagemeenschap (die vaak intern ook zeer verdeeld is), de (voormalige) moederlanden die ongewenste buitenlandse inmenging 'afzenden', het overig deel van Nederland dat niet tot de diasporagemeenschap hoort, en de Nederlandse overheid en veiligheidsautoriteiten.

De wensen van deze vier partijen lopen geregeld uiteen. Het overgrote deel van de Nederlandse bevolking ziet buitenlandse inmenging als een belangrijke bedreiging voor de Nederlandse veiligheid (Sie Dhian Ho et al., 2025). Men pleit daarom doorgaans voor harde maatregelen om ongewenste buitenlandse inmenging te adresseren. Diasporagemeenschappen hebben soms behoefte aan bescherming tegen inmenging, soms aan het verhogen van hun maatschappelijke weerbaarheid om de impact van ongewenste buitenlandse inmenging te verzachten. Een deel van de gemeenschappen zal de inmenging ook niet afwijzen, en zien als welkome steun vanuit het moederland. Die (voormalige) moederlanden voeren vanuit hun eigen perspectief noodzakelijk beleid om hun relatie met de diaspora te onderhouden, of zien het monitoren van de gemeenschappen als essentieel voor hun nationale veiligheid.

De Nederlandse overheid staat als vierde partij voor de ingewikkelde taak de juiste balans te vinden tussen de verschillende belangen: het beschermen en weerbaar maken van de gemeenschappen, het vertrouwen vasthouden bij het overig deel van Nederland dat de beleidsstrategie effectief is, het voorkomen van (de perceptie van) discriminatie door onnodig in te grijpen bij buitenlandse gemeenschappen in het Koninkrijk der Nederlanden, en het onderhouden van vruchtbare diplomatieke betrekkingen met de OBI afzendende landen.

Ter afsluiting zijn twee reflectiepunten van belang voor de toekomstige beleidsvorming rondom het dossier over ongewenste buitenlandse inmenging. Ten eerste is de impact van ongewenste buitenlandse inmenging op de nationale veiligheid niet altijd meteen evident is. De NCTV en AIVD stellen dat de impact van statelijke inmenging in diasporagemeenschappen waarschijnlijk aanzienlijk is, maar moeilijk te kwantificeren (NCTV, 2025). Niet elk geval van ongewenste buitenlandse inmenging wordt immers gemeld bij de autoriteiten. Bovendien vindt de inmenging geregeld plaats via subtiele handelingen, zoals (online)intimidatie, die niet altijd aan een dader zijn toe te schrijven. De grotere incidenten, zoals de ongeregeldheden binnen de Eritrese gemeenschap in Den Haag in 2024, zijn niet altijd direct te relateren aan een statelijke actor.

Ten tweede zijn niet alle onderdelen van de democratische rechtsstaat even goed geëquipeerd om goed met het dossier van ongewenste buitenlandse inmenging om te gaan. Met name gemeenten en lokale politieafdelingen worstelen hier geregeld mee, omdat zij niet altijd beschikken over de benodigde (geo)politieke kennis om buitenlandse inmenging in de juiste context te plaatsen. Bovendien is hun handelingsperspectief niet altijd evident. Kennisdeling tussen de Rijksoverheid en andere overheden, al dan niet in samenwerking met kennisinstellingen, is van groot belang om het dossier ongewenste buitenlandse inmenging in heel Nederland effectief te adresseren.

3.5 Dreigingscategorie Georganiseerde criminaliteit

Criminaliteit vindt plaats in allerlei verschillende vormen en maten. Alhoewel strafbaar en onwenselijk, is niet elke vorm van criminaliteit een mogelijke dreiging voor de nationale veiligheid. Dit is potentieel wel het geval wanneer criminele activiteiten vallen onder de noemer georganiseerde criminaliteit.[10] We spreken van georganiseerde criminaliteit als wordt voldaan aan een drietal voorwaarden:[11]

- Het gaat om systematisch gepleegde misdaden met ernstige gevolgen zoals grootschalige fraude, cybercrime, ernstige geweldsdelicten en drugscriminaliteit;
- Het gaat om misdaden die worden gepleegd door groepen die primair gericht zijn op illegaal gewin. Misdaden moeten dus voortkomen uit een groepsverband en gericht zijn op het verkrijgen van macht, geld of status. Dit in tegenstelling tot individueel handelen of een misdaad in de relationele sfeer. Binnen Nederland wordt regelmatig de term crimineel samenwerkingsverband (CSV) gebruikt om te refereren naar de groepen criminelen die zich bezighouden met georganiseerde criminaliteit. Deze samenwerkingsverbanden hebben vaak een wisselende

[10] Vaak wordt in plaats van georganiseerde ook wel gesproken van ondermijnende criminaliteit. De term ondermijnende criminaliteit impliceert per definitie dat de criminele daad waar het over gaat op enige wijze het politieke of maatschappelijke systeem van Nederland aantast (ondermijnt). Georganiseerde criminaliteit is daarentegen een neutralere, overkoepelende term. Georganiseerde criminaliteit omvat grotendeels dezelfde criminele activiteiten als ondermijnende criminaliteit, maar duidt het effect op de maatschappij niet. Aangezien er binnen de nationale veiligheid niet alleen wordt gekeken naar de effecten van een dreiging op de democratische rechtsstaat, maar ook op allerlei andere vlakken, is binnen het ANV gekozen voor de term georganiseerde criminaliteit.
[11] Op basis van de definitie uit Fijnaut et al. 1996.

samenstelling en zijn in Nederland vaak niet sterk hiërarchisch georganiseerd;
- Men is in staat om deze misdaden op betrekkelijk effectieve wijze af te schermen. Hiervoor gebruiken criminelen facilitators in de bovenwereld: mensen werkzaam in legale sectoren die vanuit hun positie al dan niet bewust of vrijwillig faciliterende diensten verlenen aan criminelen. Denk aan makelaars en werknemers van autoverhuurbedrijven of de financiële sector die helpen de ware identiteit dan wel oorsprong van de financiële middelen van een koper, huurder of cliënt te verhullen.

Georganiseerde criminaliteit is een bijzonder breed fenomeen. Het fenomeen reikt van grootschalige cybercrime in de vorm van bijvoorbeeld ransomware-aanvallen tot grootschalige fraude en georganiseerde drugscriminaliteit. Er is dus ook een veelvoud aan delicten, werkwijzen en mogelijk betrokken actoren onderdeel van georganiseerde criminaliteit. Georganiseerde criminaliteit bestaat verder vaak uit veel verschillende met elkaar verbonden handelingen. Zo gaat het bij georganiseerde drugscriminaliteit niet alleen om het fysiek produceren dan wel verhandelen van verdovende middelen, maar komen hier ook veel ondersteunende delicten of werkwijzen bij kijken. Bijvoorbeeld het bedreigen of anderszins onder druk zetten van mensen, het witwassen van de opbrengsten en het plegen van geweld in de openbare ruimte. Dit laatste kan de vorm aannemen van liquidaties, maar de afgelopen jaren is er ook een sterke toename in het plaatsen van explosieven en zwaar vuurwerk bij huizen en bedrijfspanden. De gevolgen van georganiseerde criminaliteit voor de nationale veiligheid komen ook voort uit deze werkwijzen.[12] De effecten van georganiseerde criminaliteit op de nationale veiligheid hangen uiteraard af van het (type) delict en de werkwijze die centraal wordt gesteld. Het is goed om te benadrukken dat uitingen van georganiseerde criminaliteit niet per definitie de nationale veiligheid raken. Dit kan uiteraard wel, afhankelijk van de specifieke uitingen en de ernst hiervan.

3.5.1 *Bouwstenen*

Binnen de dreigingscategorie 'Georganiseerde criminaliteit' zijn er verschillende factoren die van invloed zijn op de ernst van de dreiging. Deze bouwstenen zijn in onderstaande tabel weergegeven.

Tabel 16 Bouwstenen 'Georganiseerde criminaliteit'[13]

Delicten	Doelwit	Gebruik van Facilitators	Reikwijdte	Duur
Liquidatie(s)	N.v.t.	Nee	N.v.t.	< 1 maand
Infiltratie (intredepolitiek)	Criminelen	Openbaar bestuur	1 stad, gemeente of bedrijf	< 6 maanden

[12] In de ANV-themastudie georganiseerde criminaliteit (2021) wordt nader ingegaan op verschillende delicten en werkwijzen. Voor een overzicht van trends en ontwikkelingen rond georganiseerde criminaliteit kunnen de Rijksbrede Risicoanalyse 2022 (ANV, 2022) en de Trendanalyse 2024 (ANV, 2024) worden geraadpleegd.
[13] Vanuit de verschillende mogelijkheden uit de kolommen zijn verschillende scenario's denkbaar. De mogelijkheden uit een rij horen niet noodzakelijkerwijs bij elkaar.

Delicten	Doelwit	Gebruik van Facilitators	Reikwijdte	Duur
Bedreiging en/of intimidatie	Eigen sociale kring en familie	Openbare orde en veiligheids-systeem	Meerdere steden, gemeenten of bedrijven	< 1 jaar
Productie en/of handel in verdovende middelen	Wijk, gebied of stadsdeel	Politieke vertegen-woordiging		> 1 jaar
Doen van investeringen	Openbaar bestuur	Rechtspraak		
Mensenhandel & uitbuiting	Ambtenaren rechts-handhaving en justitie	Commerciële sectoren		
Afpersing	Kwetsbare groepen			
Handel in vuurwapens en explosieven	(mensen werkzaam in) legale sectoren			
Vermogens-criminaliteit	Willekeurige personen			
Cybercrime	Bedrijfsleven			
Milieudelicten	Politieke vertegen-woordiging			
Witwassen				
Omkoping				
Fraude				

Er zijn vijf verschillende typen bouwsteen. Daarbij is het nuttig eerst op te merken dat de centrale actor in de dreigingscategorie georganiseerde criminaliteit primair een crimineel samenwerkingsverband is (of meerdere). Er wordt verder geen onderscheid gemaakt tussen bijvoorbeeld een hoofdzakelijk Nederlands of niet-Nederlands CSV aangezien dit onderscheid in de praktijk niet altijd hard te maken is. De daadwerkelijke bouwstenen zijn als volgt. Ten eerste gaat het om de **activiteiten** van de actor in kwestie. Anders gezegd, met welke hoofddelicten en criminele werkwijzen houdt de actor zich bezig? Hierbij zijn gezien de relevantie voor nationale veiligheid alleen ernstige misdrijven opgenomen. Het tweede type bouwsteen betreft het **doelwit** van deze activiteiten. Dit kunnen personen of groepen zijn, maar ook een bepaald geografisch gebied. Ten derde wordt de vraag gesteld of er gebruik wordt gemaakt van **facilitators** en, zo ja, welke? Facilitators zijn mensen die werkzaam zijn binnen legale sectoren en vanuit die positie al dan niet bewust of vrijwillig faciliterende diensten verlenen aan criminele samenwerkingsverbanden.[14] Een vierde bouwsteen betreft de geografische **reikwijdte** van de activiteiten in het scenario. Tot slot wordt gekeken naar de **duur** van de situatie. De hier opgenomen bouwstenen vormen een selectie van een veel groter aantal mogelijke activiteiten onder de noemer georganiseerde criminaliteit.

[14] Zie de ANV themastudie georganiseerde criminaliteit (2021) voor meer informatie

3.5.2 *Het scenario 'Georganiseerde criminaliteit door heel Nederland'*

Voor georganiseerde criminaliteit is één scenario uitgewerkt. Er is bewust voor gekozen om dit scenario plaats te laten vinden op verschillende plekken in heel Nederland, met aandacht voor het handelen van verschillende criminele samenwerkingsverbanden. In tegenstelling tot bijvoorbeeld terrorisme, geldt hier dus dat de gevolgen voor de nationale veiligheid niet voortkomen uit het handelen van een enkel netwerk of een groep individuen, maar uit een bredere, meer sluimerende situatie. Het scenario begint met het omschrijven van een korte 'basis' voor georganiseerde criminaliteit door heel Nederland, waarna in een tweede deel een escalatie plaatsvindt. Deze escalatie is vormgegeven rond een geweldstoename richting overheidsbeambten. Het scenario is gebaseerd op twee scenario's rond georganiseerde criminaliteit uit de Rijksbrede Risicoanalyse 2022, namelijk georganiseerde criminaliteit door heel Nederland en crimineel geweld richting media en overheid.
In onderstaande tabellen zijn de bouwstenen genoemd waarop het geselecteerd fictieve scenario georganiseerde criminaliteit door heel Nederland gebouwd is.

Tabel 17 Bepalende bouwstenen voor deel 1 van het scenario 'Georganiseerde criminaliteit door heel Nederland'

Delicten	Doelwit	Gebruik van facilitators	Reikwijdte	Duur
Productie en/of handel in verdovende middelen	Criminelen	Openbaar bestuur	Meerdere steden, gemeenten of bedrijven	> 1 jaar
Infiltratie (intredepolitiek)	Wijk, gebied of stadsdeel	Openbare orde en veiligheids-systeem		
Liquidatie(s)	Openbaar bestuur	Politieke vertegen-woordiging		
Bedreiging en/of intimidatie	Ambtenaren rechts-handhaving en justitie	Commerciële sectoren		
Afpersing	Kwetsbare groepen			
Doen van investeringen	Bedrijfsleven			
Vermogenscrimi-naliteit				
Milieudelicten				
Witwassen				

Tabel 18 Bepalende bouwstenen voor deel 2 van het scenario 'Georganiseerde criminaliteit door heel Nederland'

Actor	Delicten	Doelwit	Gebruik van Facilitators	Reikwijdte
CSV	Liquidatie(s)	Criminelen	Openbaar bestuur	Meerdere steden, gemeenten of bedrijven
	Bedreiging en/of intimidatie	Openbaar bestuur		
	Bedreiging en/of intimidatie	Ambtenaren rechts-handhaving en justitie		
	Afpersing	Politieke vertegen-woordiging		

3.5.2.1 Scenario: Georganiseerde criminaliteit door heel Nederland

Georganiseerde criminaliteit vindt continu plaats door heel Nederland, in veel verschillende vormen. Onder meer rond zeehavens, in steden en op het platteland. In de Nederlandse havens komen regelmatig grote drugszendingen per container aan, waaronder cocaïne uit Midden- en Zuid-Amerika. Voor de doorvoer hiervan naar landen als Duitsland en Denemarken, maken criminele samenwerkingsverbanden onder andere gebruik van facilitators werkzaam bij bedrijven actief in de logistiek en de particuliere beveiliging op de haventerreinen. In enkele gevallen zijn ook medewerkers van de douane betrokken. Sommige van deze facilitators zijn op aanwijzing van criminele samenwerkingsverbanden bewust in de organisatie geïnfiltreerd en anderen kampen bijvoorbeeld met grote (gok)schulden waarmee zij onder druk worden gezet.

De ingevoerde drugs worden veelal verstopt tussen of in legale goederen. De betreffende containers worden vaak al ontdaan van hun clandestiene lading op het haventerrein zelf, maar soms ook pas als ze aan zijn gekomen bij hun legitieme eindbestemming. Bedrijven ontdekken meermaals verdachte pakketten tussen geleverde goederen, waarin grote hoeveelheden cocaïne blijken te zitten. Na melding hiervan bij de politie, worden meerdere medewerkers van de betreffende bedrijven ernstig bedreigd. De inbeslagname van grote hoeveelheden drugs leidt ook tot spanningen binnen het criminele circuit. Meermaals worden explosieven bij zowel bedrijfspanden als woningen geplaatst, sommige daarvan ontploffen daadwerkelijk.

Tegelijkertijd speelt het probleem van georganiseerde criminaliteit niet alleen in de havens, maar ook in veel (grote) steden. Criminele samenwerkingsverbanden weten hier grip te krijgen op kwetsbare wijken. Kwetsbare inwoners worden ingezet als katvanger, uithaler en sekswerker. Als er conflicten zijn, worden steeds vaker kwetsbare jongeren ingezet om zelfgebouwde explosieven, op basis van zwaar vuurwerk, achter te laten in portieken en bij bedrijfspanden. Alhoewel er geen slachtoffers vallen, loopt dit in een aantal gevallen maar net goed af. Sommige jongeren kijken op naar de criminelen en zien in de

criminaliteit een manier om de eigen armoede en sociale positie te ontstijgen. Andere mensen worden gedwongen tot medewerking of hebben niet door dat zij criminaliteit faciliteren. De groeperingen proberen hiertoe actief drugs te verkopen aan de jeugd in de wijk om zo een afhankelijkheidsrelatie te creëren.

Dankzij facilitators in de vastgoedsector worden in veel wijken panden opgekocht. Hierin worden dekmantelbedrijven als kapperszaken en afhaalrestaurants gevestigd. Een aantal bonafide ondernemers wordt weggeconcurreerd. Kamers in de slecht onderhouden panden worden met name aan kwetsbare personen verhuurd of worden gebruikt als locatie voor hennepteelt of prostitutie. Een aantal wijken verloedert in een snel tempo en bewoners voelen zich steeds onveiliger. Alhoewel men steeds meer roept om ingrijpen door gemeenten en politie, krijgen deze organisaties geen grip op de situatie. Veel bewoners durven niet meer vrijuit te praten, helemaal niet nadat enkele van hen ernstig zijn bedreigd. Wanneer handhavers of hulpdiensten de wijken betreden, worden zij veelvuldig geïntimideerd en lastiggevallen door grote groepen jongeren. Het sterke vermoeden heerst dat dit wordt aangestuurd door criminelen. Een aantal wijken komt bij hulpdiensten en handhavers steeds meer bekend te staan als een *'no go area'*. Er ontstaat tegelijkertijd een groot maatschappelijk stigma rond de wijken en de mensen die er wonen.

Tot slot ontplooien criminele samenwerkingsverbanden ook in meer landelijke gebieden hun activiteiten. Criminelen huren op verschillende, meer afgelegen plekken loodsen. Vaak hebben de eigenaren geldproblemen en krijgen ze een vergoeding ver boven de marktwaarde in ruil voor het niet stellen van vragen. In de schuren worden grote hoeveelheden synthetische drugs geproduceerd, primair voor de export. Het drugsafval dat ontstaat, waaronder zware metalen als kwik en industriële oplosmiddelen wordt gedumpt in de omgeving. Boswachters vinden steeds meer vaten met drugsafval in het Natura-2000-gebied en maken zich zorgen om de toenemende sterfte van vissen en andere waterdieren in de verschillende meren. Als twee boswachters tijdens een patrouille in de avond vier mannen tegenkomen die bezig zijn met het uitladen van vaten, worden beiden bedreigd en mishandeld.

Escalatie

De maatschappelijke roep om hard(er) op te treden tegen criminele samenwerkingsverbanden klinkt steeds luider. Ook in internationaal verband wordt Nederland steeds vaker aangesproken op het onderwerp. Een aantal Europese landen gaat over tot een formeel protest in EU-verband over de in hun ogen te beperkte Nederlandse aanpak betreffende de productie en uitvoer van synthetische drugs. Daardoor wordt besloten tot een grote landelijke actie gericht op het verstoren van de georganiseerde drugscriminaliteit in Nederland. Met behulp van de resultaten uit al langer lopende dekmanteltrajecten worden enkele kopstukken in de internationale cocaïnehandel opgepakt. Tegelijkertijd worden in meerdere gemeenten panden gesloten van bedrijven waarvan het vermoeden bestaat dat zij worden gebruikt voor de handel of productie van verdovende middelen. De arrestaties en de hierop volgende rechtszaken kunnen rekenen op veel aandacht. Meerdere

misdaadjournalisten doen uitvoerig verslag van de acties en hieruit voortvloeiende rechtszaken.

Al snel krijgt de politie signalen dat de actie en alle aandacht tot kwaad bloed heeft geleid in het criminele circuit. Na enige tijd treffen een aantal betrokkenen een brief aan op hun huisadres met daarin de namen en adressen van een grote hoeveelheid rechters, officieren van justitie, politiemedewerkers, andere ambtenaren en politici. Onderaan de brief staat de eis dat de opgepakte kopstukken binnen twee weken worden vrijgelaten. Uit onderzoek blijkt al snel dat meerdere medewerkers van personeelszaken bij verschillende organisaties, waaronder bij verschillende gemeenten, onder grote druk zijn gezet om vertrouwelijke gegevens door te spelen aan criminelen.

Enkele weken later worden op meerdere van de adressen explosieven aangetroffen, waarvan het merendeel ook afgaat. Alhoewel de schade vaak materieel van aard is, blijkt één van de explosies dusdanig krachtig dat een deel van een appartementencomplex instort. Vijf mensen komen hierbij om het leven, waaronder de officier van justitie voor wie het pakket bedoeld lijkt te zijn geweest. Dezelfde week wordt één van de misdaadjournalisten vanuit een voorbijrijdende auto met een automatisch vuurwapen op straat doodgeschoten. Een vol terras is getuige van de gebeurtenis en meerdere omstanders raken gewond, waarvan twee dodelijk.

Een groot deel van de in de brief genoemde mensen ziet zich gedwongen om onder te duiken. Het beveiligen van een dusdanig grote groep mensen trekt een zware wissel op de beschikbare (politie)capaciteit, financiële middelen voor persoonsbeveiliging en mogelijkheden voor de beveiligde personen om hun werk uit te kunnen blijven voeren. Veel werk blijft liggen en er ontstaat tegelijkertijd angst onder collega’s die soortgelijk werk doen als de groep bedreigde personen. Veel mensen melden zich ziek. Een aanzienlijk aantal rechtszaken moet worden uitgesteld, waaronder de zaak tegen de opgepakte kopstukken. Na twee weken wordt voor een groot aantal mensen op de lijst de beveiliging afgeschaald. Als kort hierna vlak bij het huis van één van de rechters op de lijst twee mannen met zwaar vuurwerk worden aangehouden, ontstaat er steeds meer discussie over de vraag of het niet beter is om toe te geven aan de eisen.

3.5.2.2 Beoordeling van impact en waarschijnlijkheid

Onderstaande tabel bevat de beoordeling van de waarschijnlijkheid en de impact van het fictieve scenario ‘Georganiseerde criminaliteit door heel Nederland’.

Tabel 19 Beoordelingstabel scenario 'Georganiseerde criminaliteit door heel Nederland'

Thema	**Ongewenste inmenging en beïnvloeding democratische rechtsstaat**
Dreigingscategorie	Georganiseerde criminaliteit
Scenario	Georganiseerde criminaliteit door heel Nederland
Scenariotoelichting	Door heel Nederland zijn criminele samenwerkingsverbanden actief. Wanneer vanuit de overheid de druk op deze CSV'en toeneemt, leidt dit tot een geweldsescalatie.

Waarschijnlijkheidsbeoordeling (binnen 5 jaar)		**Toelichting**
Waarschijnlijkheid:	C hoog	Het eerste deel van het scenario kan als waarschijnlijk (score D) of mogelijk zelfs als zeer waarschijnlijk (score E) worden gezien. Veel van de hier omschreven activiteiten vinden reeds plaats. Het tweede deel vormt echter een significante geweldsescalatie richting onder andere het openbaar bestuur. Deze escalatie is relatief gezien minder waarschijnlijk (score C). Aangezien uit deze escalatie een relatief groot deel van de impact komt, is gekozen voor de overall score C hoog.

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
Territoriaal	1.1 Grondgebied	C	Er zijn 'pockets' waar overheidsgezag op papier wel bestaat, maar niet daadwerkelijk wordt uitgeoefend. Het betreft slechts enkele wijken (<100km2), voor meer dan een half jaar en met een hoge bevolkingsdichtheid. Omdat het oppervlak zeer klein is, valt de score lager uit (van D naar C).
	1.2 Internationale positie	A	Er wordt in een internationaal gremium formeel protest aangekaart tegen het handelen van de Nederlandse regering. Er is sprake van een beperkte aantasting van politieke betrekkingen.
	1.3 Informatie en digitale ruimte	C	In het scenario wordt door criminele actoren ongewenst toegang tot vertrouwelijke informatie verkregen behorende tot onder meer overheidsinstanties actief op het gebied van openbare veiligheid en rechtshandhaving (persoonsgegevens medewerkers).
	1.4 Grondgebied EU en NAVO lidstaten	0	Niet van toepassing
Fysiek	2.1 Doden	B	In het scenario vallen zeven doden. Echter, als direct gevolg van de in het scenario omschreven dynamiek is het aannemelijk dat dit aantal nog met enkelen toeneemt.
	2.2 Ernstig gewonden en chronisch zieken	C	In het scenario worden minder dan tien fysiek gewonden expliciet genoemd. Echter, als direct gevolg van de in het scenario omschreven

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			dynamiek is het aannemelijk dat dit aantal nog met enkelen toeneemt. Verder, gezien de mentale belasting van een groot aantal bedreigde personen en de personen hieromheen, is het aannemelijk dat een grotere groep mensen ook mentale klachten ontwikkelt.
	2.3 Gebrek primaire levensbehoeften	0	Niet van toepassing
Economisch	3.1 Kosten	B	In het scenario is sprake van aanzienlijke kosten in de vorm van onder andere schade aan panden, kosten voor de uitval van personeel, gezondheidskosten en de aanvullende beveiliging van ambtenaren, politici en rechters. Aangezien het hierbij om relatief grote hoeveelheden personen en locaties gaat voor een langere tijd, zijn de kosten van relevante omvang en meer dan 100 miljoen.
	3.2 Aantasting vitaliteit	0	Niet van toepassing. Er gaan in het scenario geen banen verloren. Ook is het zeer onwaarschijnlijk dat het scenario een dergelijke belasting legt op de overheidsfinanciën of Nederlandse economische bedrijvigheid dat de schuldquote wordt aangetast. Wel kan het zijn dat Nederland op termijn als onveilig kan worden gezien, wat kan leiden tot een afname in investeringen. Dit valt qua tijdshorizon echter buiten het scenario
Ecologisch	4.1 Aantasting beschermwaardige natuur	A	Een zeer klein deel van de Nederlandse Natura 2000 raakt vervuild met drugsafval. Het effect op de natuurlijke regeneratie zal echter beperkt zijn.
	4.2 Aantasting milieu en natuur in algemene zin	A	Het is aannemelijk dat er ook buiten het genoemde Natura 2000-gebied sprake is van vervuiling. Het effect op de natuurlijke regeneratie zal echter beperkt zijn.
Sociaal-politiek	5.1 Verstoring dagelijks leven	B	Mensen in wijken waar CSV'en veel macht hebben durven minder gebruik te maken van maatschappelijke voorzieningen en kunnen minder een beroep doen op en/of bijdragen aan het eigen sociale netwerk. De groep getroffenen is klein (<10.000), maar wordt wel voor langere tijd geraakt (>1 maand).
	5.2 Aantasting democratische rechtsstaat	D	Er is sprake van integriteitsschendingen binnen het openbare orde en veiligheidssysteem en binnen het openbaar bestuur. Het functioneren van het openbaar bestuur, de rechtspraak en het openbare orde en veiligheidssysteem wordt ernstig aangetast, onder meer door de (gerealiseerde) bedreigingen en de hierdoor ontstane angst en werkachterstanden.
	5.3 Sociaal-maatschappelijke impact	A	Als gevolg van de activiteiten van CSV’en in de wijken en buurten uit het scenario, ontstaat er

Beoordeling gevolgen (impact)			
Veiligheidsbelang	**Criterium**	**Score**	**Toelichting**
			negatieve beeldvorming over de mensen die hier wonen. Of zij nu zelf verbonden zijn aan criminele activiteiten of niet.
Internationale rechtsorde en 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

3.5.3 Beschouwing Georganiseerde criminaliteit

Het bovenstaande scenario bevat een relatief ernstige geweldsescalatie in het tweede deel. Desalniettemin, kan het scenario als geheel worden geclassificeerd als tenminste enigszins waarschijnlijk. Hierbij geldt zelfs dat het eerste deel van het scenario als (zeer) waarschijnlijk kan worden gezien – ook al is dan nog geen sprake van ontwrichting van de nationale veiligheid. Meerdere van de hier genoemde activiteiten vinden bijvoorbeeld al plaats in Nederland. Een gerichte geweldsescalatie van een omvang en set aan handelingen zoals vermeld in het scenario is echter minder waarschijnlijk – in dat deel ontstaat daadwerkelijk ontwrichting van de nationale veiligheid. Dit neemt echter niet weg dat onderdelen hiervan reeds hebben plaatsgevonden in het verleden, zoals de liquidatie van een advocaat in 2019 en van een misdaadjournalist in 2021. Ook het gebruik van (zelfgemaakte) explosieven in de openbare ruimte heeft reeds tot (dodelijke) slachtoffers geleid.[15]

De gevolgen van georganiseerde criminaliteit uiten zich in het scenario op een relatief breed scala aan veiligheidsbelangen. Alhoewel het zwaartepunt zich bevindt rond het belang sociaal-politieke stabiliteit, worden met uitzondering van het belang internationale rechtsorde en stabiliteit alle andere belangen geraakt. De hoogste score komt specifiek naar voren op het functioneren van de democratische rechtsstaat (5.2). Deze aantasting komt met name voort uit dreigementen richting overheidspersoneel en mensen werkzaam in de media, maar ook ten dele uit integriteitsschendingen en een mogelijk verlies van vertrouwen onder de bevolking in het vermogen van de overheid in brede zin om een halt toe te roepen aan georganiseerde criminaliteit.

[15] In december 2024 heeft bijvoorbeeld een grote explosie plaatsgevonden in Den Haag, waarbij zes doden en vier gewonden vielen. Ook stortten woningen en bedrijfspanden rond het direct getroffen blok in. Het ging hierbij naar verwachting om een incident met oorzaak in de relationele sfeer. Zie OM (2025).

Het scenario richt zich verder primair op de 'fysieke' component van georganiseerde criminaliteit. Cybercrime is voor de nationale veiligheid potentieel ook een relevante vorm van georganiseerde criminaliteit, zoals ransomware-aanvallen op systemen verbonden aan het functioneren van vitale infrastructuur. Zie voor een uitgewerkt ransomware-scenario de Themarapportage Cyberdreigingen onderdeel van de Rijksbrede Risicoanalyse 2022, en zie ook de bespreking van ransomwareaanvallen in het themarapport over Cyberdreigingen binnen deze risicoanalyse en in de Trendanalyse 2024. Ook in relatie tot cyberdreigingen tegen de nationale veiligheid is het van belang op te merken dat de verscheidenheid van actoren die gebruik maken van cybercrime als modus operandi sterk is toegenomen. Zo maken niet alleen criminele maar ook statelijke actoren gebruik van bijvoorbeeld ransomware ten behoeve van spionage en sabotage. Bovendien zijn achterliggende motieven niet altijd goed van elkaar te onderscheiden, zie ook de beschouwingen binnen het themarapport Cyberdreigingen.

Ook kunnen statelijke actoren opdracht geven tot criminele activiteiten, bijvoorbeeld als onderdeel van hybride operaties. Statelijke actoren maken dan in feite gebruik van bestaande 'crime-as-a-service'-structuren, onderdeel van georganiseerde criminaliteit.

Verder is het belangrijk om het sluimerende karakter van georganiseerde criminaliteit te benadrukken. In het scenario zijn een aantal meer publieke en expliciete uitingen van georganiseerde criminaliteit opgenomen om het narratief vorm te geven en het beoordelen van de situatie te faciliteren. Tegelijkertijd geldt dat de gevolgen van georganiseerde criminaliteit juist een verhuld en sluimerend karakter hebben. Het gebruik van dekmantelbedrijven, het geleidelijk infiltreren in overheidsorganisaties of het ontstaan van een zwijgcultuur in bepaalde wijken, zijn veelal geen zaken die direct zichtbaar zijn en leiden tot maatschappelijke ontwrichting. Echter, wanneer deze zich over de tijd verder kunnen ontwikkelen, kan dit leiden tot bijvoorbeeld een uitholling en daarmee ook ondermijning van de democratische rechtsstaat of een aantasting van bonafide economische activiteiten. Juist vanwege het sluimerende karakter worden veel ontwikkelingen niet meteen herkend als een gevaar voor nationale veiligheid. Het ingrijpen door een beperkt aantal instituties die dit als eerste herkennen en daarop acteren zal minder effectief zijn zo lang de rest van de veiligheidsketen het fenomeen van georganiseerde misdaad nog niet als gevaar voor de nationale veiligheid herkend of bestempeld.

Naast interventies gericht op het verzwakken van de criminele netwerken, is het van belang om de weerbaarheid tegen georganiseerde criminaliteit te verhogen door blijvend in te zetten op bewustwording. Voor een breed scala aan zowel publieke als private sectoren als voor individuele burgers geldt dat zij hier mogelijk mee te maken kunnen krijgen. Wat dit betreft is de aanpak van georganiseerde criminaliteit een zaak van de lange adem die samenwerking vereist tussen bovengenoemde actoren.

Tot slot is ontwrichting door georganiseerde criminaliteit in specifiek Caribisch Nederland voorstelbaar, bijvoorbeeld als gevolg van drugssmokkel en geassocieerde criminele activiteiten. De positie van Caribisch Nederland ten opzichte van Midden- en Zuid-Amerika maakt dat de dreiging die van georganiseerde criminaliteit uitgaat groot is.

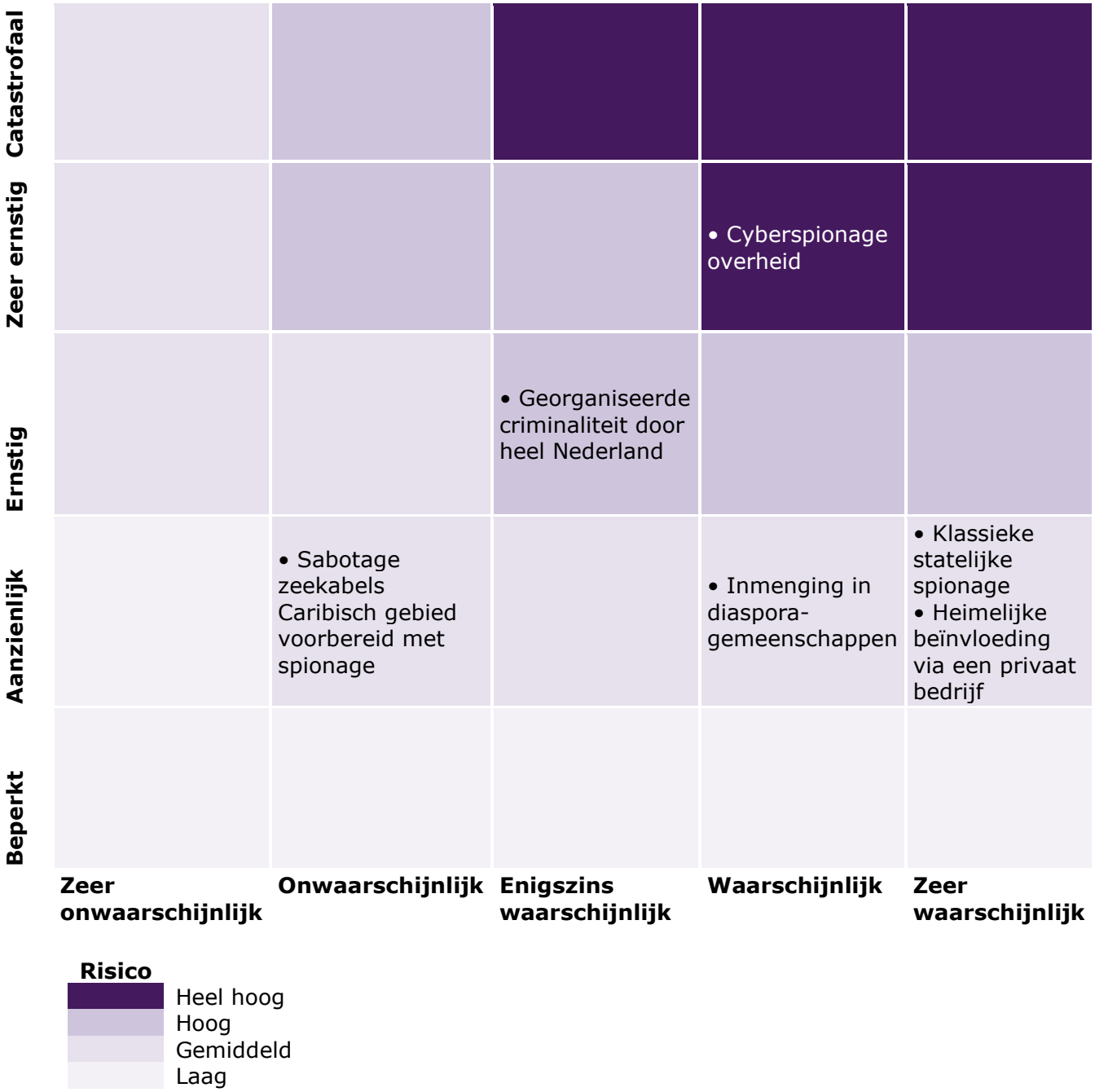
3.6 Slotbeschouwing thema Ongewenste inmenging en beïnvloeding democratische rechtsstaat

Binnen het thema ongewenste inmenging en beïnvloeding van de democratische rechtsstaat worden dreigingen voor de nationale veiligheid beschreven die worden veroorzaakt door activiteiten van statelijke actoren en niet-statelijke actoren, waaronder criminele samenwerkingsverbanden. Binnen dit thema zijn vier verschillende dreigingscategorieën in kaart gebracht, namelijk ongewenste buitenlandse beïnvloeding ofwel hybride dreigingen, spionage, ongewenste buitenlandse inmenging en ten slotte georganiseerde criminaliteit. In totaal zijn er zes scenario's uitgewerkt waarvoor de impact en waarschijnlijkheid in kaart zijn gebracht (zie Figuur 1).

3.6.1 *De impact en waarschijnlijkheid van ongewenste inmenging en beïnvloeding democratische rechtsstaat*

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

Figuur 1 Risicodiagram thema ongewenste inmenging en beïnvloeding democratische rechtsstaat



De dreiging van inmenging en beïnvloeding tegen de democratische rechtsstaat heeft brede en soms ook grote impact op de Nederlandse nationale veiligheid. Zo hebben twee van de beschouwde scenario's een ernstige of zeer ernstige aantasting van de nationale veiligheid tot

gevolg, te weten het scenario over cyberspionage binnen de overheid en het scenario over gewelddadige escalatie van georganiseerde criminaliteit. De scenario's sabotage zeekabels Caribisch gebied voorbereid met spionage, heimelijke beïnvloeding via een privaat bedrijf en klassieke statelijke spionage hebben een aanzienlijke impact op de nationale veiligheid. Daarbij moet worden opgemerkt dat gelijkende scenario's mogelijk een grotere impact hebben, echter betekent dat vaak ook dat de waarschijnlijkheid dat het scenario optreedt lager is. Ten slotte valt op dat de waarschijnlijkheid van een aantal scenario's relatief hoog is: drie van de zes uitgewerkte scenario's worden als waarschijnlijk of zeer waarschijnlijk gezien.

3.6.2 Impact ontwikkelingen

De aard en omvang van de dreiging die uitgaat van ongewenste buitenlandse beïnvloeding of hybride dreigingen is de afgelopen drie tot vijf jaar veranderd. Ten eerste bedient een groter aantal statelijke actoren zich van modus operandi voor beïnvloeding. Daarnaast worden niet alleen politieke, economische, sociale en informatiedoelwitten getroffen, maar juist ook militaire en infrastructurele doelwitten. Reden hiervoor lijkt te zijn dat de Russische Federatie de laatste jaren maatschappelijke ontwrichting in plaats van beperkte beïnvloeding tot doel heeft – en daarbij ook een assertievere houding laat zien. Als ongewenste beïnvloeding wordt ingezet in samenhang met militaire dreigingen staan andere doelen centraal, zoals het creëren van maatschappelijke onrust, frustreren van besluitvorming voor effectieve respons ten tijde van een militaire crisis of fysiek verstoren van militaire mobiliteit of militaire operaties. Er is bijvoorbeeld in West- en Midden-Europa de afgelopen jaren sprake geweest van pogingen om de doorvoer van militaire goederen richting Oekraïne of voor NAVO-operaties in Oost-Europa te verstoren.

Voor wat betreft de spionagedreiging, valt op dat zowel klassieke spionage als cyberspionage als waarschijnlijk of zeer waarschijnlijk worden gezien. In beide gevallen is het voorstelbaar dat grote aantasting van de nationale veiligheid wordt veroorzaakt. Dit is niet alleen zo doordat informatie weglekt, maar ook omdat zo het vertrouwen in de overheid wordt aangetast en de democratische rechtsstaat of andere veiligheidsbelangen worden geraakt. Het Dreigingsbeeld Statelijke Actoren 2025 spreekt[16] van een geziene toename van het aantal landen dat spioneert in Nederland. Die toename kan worden veroorzaakt door verschuivingen in de wereldorde: deze wijzigingen in verhoudingen tussen geopolitieke machtsblokken spelen zich ten slotte ook concreet in Nederland af. Maar de gepercipieerde toename in spionagedreiging tegen Nederland kan ook veroorzaakt worden door een verbeterd zicht van de inlichtingen- en veiligheidsdiensten op statelijke dreigingen.

Zie het scenario 'Klassieke statelijke spionage' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin een militair door een statelijke actor onder druk wordt gezet om staatsgeheimen prijs te geven.

[16] DBSA 2025, p. 23.

Zie het scenario 'Cyberspionage Rijksoverheid' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin een grote hoeveelheid gevoelige overheidsinformatie wordt buitgemaakt. Deze informatie wordt gebruikt om nadere cyberspionage bij ketenpartners te faciliteren. Dit heeft een grote afbreuk van vertrouwen in de Rijksoverheid tot gevolg.

Ook van ongewenste buitenlandse inmenging gaat een dreiging tegen de Nederlandse democratische rechtsstaat uit. Ook al is de precieze impact die van deze inmenging uitgaat niet altijd evident. Hier geldt dat de impact op de nationale veiligheid sluimerend kan zijn en zich op de middellange tot lange termijn pas laat zien. Ook (of juist) wanneer het niet direct wordt herkend, kan de daadwerkelijke impact pas op de lange termijn duidelijk worden. Dit geldt bijvoorbeeld voor spionage ter voorbereiding op sabotage of militaire actie in de toekomst.

Zie het scenario 'Ongewenste buitenlandse inmenging in diasporagemeenschappen in Nederland' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin de inmenging vanuit een statelijke actor in Nederland zo erg toeneemt, dat de verhoudingen tussen de Nederlandse overheid en de statelijke actor onder spanning komen te staan.

Op basis van de dreigingscategorie georganiseerde criminaliteit en het daarin geschetste scenario is duidelijk dat de aanwezigheid en activiteiten van georganiseerde criminaliteit in Nederland zorgelijk blijven. Hoewel de waarschijnlijkheid van grote gewelddadige escalatie beperkt is, blijft dit een punt van aandacht. Gewelddadige escalatie zou kunnen ontstaan uit frictie tussen criminelen en samenwerkingsverbanden onderling, maar ook uit het gericht aanvallen van overheden, de maatschappij en specifieke onderdelen van de democratische rechtsstaat, zoals media, rechtspraak en veiligheidsdiensten.

Ten slotte is sprake van vermenging van dreiging tussen enkele categorieën binnen dit thema, namelijk tussen georganiseerde criminaliteit en statelijke beïnvloeding en statelijke inmenging. Buitenlandse inlichtingendiensten en andere buitenlandse organisaties maken al lange tijd gebruik van criminele uitvoerders omdat zij veelal middelen in positie hebben en in de gelegenheid zijn om operationele activiteiten in Nederland uit te voeren. Zo zijn al in 2015 en 2017 in Nederland door criminelen liquidaties uitgevoerd in opdracht van een buitenlandse mogendheid. De manier waarop criminelen worden ingezet is echter sinds 2022 veranderd en er wordt een sterke toename gezien van de inzet van criminele uitvoerders, maar ook van sympathisanten, en op geldelijk gewin beluste uitvoerders. Hierbij is sprake van het inzetten van meer en minder professionele criminele uitvoerders ten behoeve van het uitvoeren van (onderdelen van) spionage, sabotage, beïnvloeding en inmenging. De goede beschikbaarheid en toegankelijkheid van digitale, versleutelde communicatie evenals cryptografische betaalmiddelen maakt het daarbovenop goed mogelijk voor buitenlandse inlichtingendiensten om anoniem uitvoerders aan te sturen.

3.6.3 Kwetsbaarheden

De hierboven geschetste verbreding van doelwitten van ongewenste buitenlandse beïnvloeding maakt dat een groter aantal maatschappelijke sectoren, waaronder vitale processen, rekening dient te houden met deze dreiging. De Rijksoverheid draagt onder andere bij aan het mitigeren van deze kwetsbaarheid door de aanstaande implementatie van de Wet weerbaarheid kritieke entiteiten.

Zie het scenario 'Heimelijke beïnvloeding via een privaat bedrijf' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin politieke, economische en sociale structuren in de Nederlandse maatschappij worden beïnvloed door een statelijke actor. Hieruit blijkt dat deze vormen van beïnvloeding nog steeds waarschijnlijk zijn.

Zie het combinatiescenario 'Oorlog in Europa' in het betreffende themarapport, waarin ongewenste buitenlandse beïnvloeding wordt ingezet om grootschalige onrust te creëren in de Nederlandse maatschappij en daarmee de eenheid van het NAVO-bondgenootschap te ondergraven evenals de militaire doelen van de Russische Federatie te faciliteren.

Een belangrijke kwetsbaarheid voor cyberspionage hangt samen met de wijze waarop IT-hardware en -software, waaronder cloudopslag, worden ingezet binnen de Rijksoverheid, andere overheden en kritieke entiteiten. Hier ligt een belangrijk raakvlak met ontwikkelingen op het gebied van digitale autonomie en soevereiniteit: hoe meer digitaal autonoom de Rijksoverheid is, hoe meer ook direct zicht gecreëerd kan worden op eventuele IT-kwetsbaarheden. Zie ook de beschouwing op het thema Cyberdreigingen. Daarnaast is er samenhang tussen spionage en vervolgens sabotage ter ontwrichting van de maatschappij. De toegankelijkheid en dus kwetsbaarheid van veel infrastructuur op land en op zee waaronder transportnetwerken, telecomnetwerken en energienetwerken voor spionage en zelfs sabotage komt reeds terug in het in de risicoanalyse opgenomen scenario over zeekabels in het Caribisch deel van het Koninkrijk. Scenario's met een veel grotere aantasting van de nationale veiligheid zijn ook voorstelbaar. Havens en belangrijke knooppunten worden wel beveiligd, maar het is ondoenlijk om alle genoemde netwerken volledig te beveiligen. Spionage gericht op infrastructuur kan tot doel hebben in de toekomst sabotage of anderszins ontwrichting te faciliteren – bijvoorbeeld tijdens een militair conflict. Maar ook meer geavanceerde aanvallen zijn voorstelbaar: zo kan spionage gecombineerd worden met pre-positionering van explosieven om op het juiste moment grote ontwrichting te veroorzaken.

Zie het scenario 'Sabotage zeekabels Caribisch gebied voorbereid met spionage' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin twee aanlandingspunten van telecomkabels op Curaçao worden beschadigd. Door bijkomende elektriciteitsuitval stralen de effecten van dit incident uit naar enkele andere eilanden in de Caribische regio waaronder Trinidad & Tobago en Puerto Rico.

Kwetsbaarheid voor ongewenste buitenlandse inmenging is in veel gevallen inherent aan de gecombineerde achtergrond van bepaalde demografische groepen in de Nederlandse maatschappij. Daarbij komt dat niet elk geval van inmenging bij de overheid wordt gemeld. Bovendien vindt de inmenging geregeld plaats via subtiele handelingen zoals intimidatie die niet altijd aan een actor zijn toe te schrijven. Ook grotere incidenten, zoals de ongeregeldheden binnen de Eritrese gemeenschap in Den Haag in 2024, zijn niet altijd direct te relateren aan een statelijke actor. Verder zijn niet alle onderdelen van de democratische rechtsstaat even goed geëquipeerd om effectief met inmenging om te gaan. Met name gemeenten en politie op districtsniveau worstelen hier geregeld mee, omdat zij niet altijd beschikken over de benodigde geopolitieke kennis om buitenlandse inmenging in de juiste context te plaatsen. Bovendien is hun handelingsperspectief niet altijd evident. Kennisdeling tussen de Rijksoverheid en andere overheden, al dan niet in samenwerking met kennisinstellingen, is van groot belang om inmenging in heel Nederland effectief te adresseren.

De maatschappij en democratische rechtsstaat blijven kwetsbaar voor zowel sluimerende uitbreiding van de invloed van criminelen als voor plotselinge, lokale, grote invloed op bijvoorbeeld een buurt, belangrijke overheidsorganisatie of een essentieel overheidsproces. Daarnaast bedienen criminele netwerken zich van digitale modus operandi – ook op zeer grootschalige of zelfs industriële wijze. Ransomware en andere vormen van cybercriminaliteit leiden ook tot maatschappelijke kosten. De maatschappelijke kwetsbaarheid voor dit soort vormen van cybercrime blijft voor nu wijdverbreid.

Zie het scenario 'Georganiseerde criminaliteit door heel Nederland' (themarapport *Ongewenste inmenging en beïnvloeding democratische rechtsstaat*), waarin de brede maatschappelijke impact van georganiseerde criminaliteit wordt getoond. Daarbovenop ontstaat een gewelddadige escalatie gericht op media, rechtspraak en andere onderdelen van de overheid.

Ten slotte, heeft de hierboven gesignaleerde vermenging van dreigingen zoals inmenging, beïnvloeding en georganiseerde criminaliteit mogelijk een kwetsbaarheid tot gevolg. Er is namelijk samenwerking nodig tussen veiligheidsorganisaties om deze vermenging van dreigingen het hoofd te kunnen bieden. Taakvelden van organisaties zoals politie, inlichtingen- en veiligheidsdiensten en andere bijzondere opsporingsdiensten overlappen immers voor een groot deel. Wanneer deze samenwerking niet genoeg vorm krijgt, zijn monitoring en bestrijding van inmenging, beïnvloeding en criminaliteit niet effectief.

4 Literatuur

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) & Militaire Inlichtingen- en Veiligheidsdienst (MIVD) (2024, 6 december). *Dreigingsbeeld hybride en militaire dreigingen*. Dreigingsbeeld hybride en militaire dreigingen | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD, Militaire Inlichtingen- en Veiligheidsdienst (MIVD) & Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2025, 17 augustus). *Dreigingsbeeld statelijke actoren 2025*. Dreigingsbeeld Statelijke Actoren 2025 - Aanhoudende dreigingen in tijden van groeiende onzekerheid | Rapport | Rijksoverheid.nl.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD, Militaire Inlichtingen- en Veiligheidsdienst (MIVD) & Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2021, 3 februari). *Dreigingsbeeld statelijke actoren*. Dreigingsbeeld statelijke actoren DBSA | AIVD.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) & Militaire Inlichtingen- en Veiligheidsdienst (MIVD). (2025). AIVD. *Jaarverslag 2024.* Jaarverslag 2024 | AIVD.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) & Militaire Inlichtingen- en Veiligheidsdienst (MIVD). (2021). *Brochure cyberaanvallen AIVD en MIVD*. Ministerie van Defensie. https://www.defensie.nl/downloads/publicaties/2021/06/28/ brochure-cyberaanvallen-aivd-en-mivd.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) & Militaire Inlichtingen- en Veiligheidsdienst (MIVD) (2026). *Tussen vrede en oorlog: De oorlog in Oekraïne en de Russische dreiging in Europa.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.aivd.nl/documenten/2026/02/19/tussen-vrede-en-oorlog.-de-oorlog-in-oekraine-en-de-russische-dreiging-in-europa.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2019, 9 januari). *Iran waarschijnlijk betrokken bij liquidaties in Nederland*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.aivd.nl/actueel/nieuws/2019/01/08/iran-waarschijnlijk-betrokken-bij-liquidaties-in-nederland.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2021, 29 april). *AIVD-jaarverslag 2020*. https://www.aivd.nl/documenten/jaarverslagen/2021/04/29/ aivd-jaarverslag-2020.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (z.d.). *Economische veiligheid.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.aivd.nl/onderwerpen/economische-veiligheid.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2023, 23 februari). *Beschouwing risico's gebruik applicaties landen met offensief cyberprogramma gericht tegen Nederland*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.rijksoverheid.nl/documenten/brieven/2023/03/21/aivd-beschouwing-risicos-gebruik-applicaties-landen-met-offensief-cyberprogramma-gericht-tegen-nederland.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2025a). *AIVD Jaarverslag 2024.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2025/04/24/jaarverslag-2024.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). (2025b, 28 augustus). *Nederlandse providers doelwit van Salt Typhoon*. Via https://www.aivd.nl/actueel/nieuws/2025/08/28/nederlandse-providers-doelwit-van-salt-typhoon.

Analistennetwerk Nationale Veilighed (ANV). (2022). *Themarapportage ongewenste inmenging en beïnvloeding democratische rechtsstaat*. Themarapportage ongewenste inmenging en beïnvloeding 2022 | Nationaal Coördinator Terrorismebestrijding en Veiligheid.

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

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

Bellaart, H., & Kahmann, M. (2024). *De ontwikkelingen in de Eritrees-Nederlandse gemeenschap*. Verwey-Jonker Instituut. https://www.verwey-jonker.nl/wp-content/uploads/2025/03/224240_Ontwikkelingen-in-de-Eritrees-Nederlandse-gemeenschap-Informatieblad.pdf.

Braw, E. (2024, 21 november). *Suspected sabotage by a Chinese vessel in the Baltic Sea speaks to a wider threat*. The Atlantic Council. Suspected sabotage by a Chinese vessel in the Baltic Sea speaks to a wider threat - Atlantic Council.

Clark, S. (2025, 4 juni). *Microsoft didn't cut services to International Criminal Court, its president says*. Via https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/.

Computable. (2023). Via Chinese cyberspionage loopt spuigaten uit - Computable.nl.

D'Hooghe, I., & Dekker, B. (2020). *China's invloed op onderwijs in Nederland: een verkenning*. Clingendael. https://www.clingendael.org/sites/default/files/2020-07/Rapport_politieke_beinvloeding_in_het_onderwijs_juni_2020.pdf.

Dorio, C. (2021, 17 april). *Rapport over KPN bevestigt jarenlange geruchten over spionage China*. NOS. Via https://nos.nl/artikel/2377101-rapport-over-kpn-bevestigt jarenlange-geruchten-over-spionage-china.

Fijnaut, C., Bovenkerk, F., Bruinsma, G. & van de Bunt, H. (1996). *Eindrapport Onderzoeksgroep Fijnaut: Georganiseerde Criminaliteit in Nederland*.

Giannopoulos, G., Smith, H., Theocharidou, M. (2021). *The landscape of hybrid threats: A conceptual model*. The landscape of hybrid threats - Publications Office of the EU.

Gomes, A. & Okano-Heijmans, M. (2024). *Too late to act? Europe's quest for cloud sovereignty*. Clingendael. https://www.clingendael.org/sites/default/files/2024-02/Policy_brief_Cloud_sovereignty.pdf.

Houtkamp, C., & Drost, N. (2023). *Oekraïense en Russische gemeenschappen in Nederland*. Clingendael. https://www.clingendael.org/publication/oekraiense-en-russische-gemeenschappen-nederland.

Houtkamp, C., Van Heukelingen, N., & Van Der Laan, T. (2024). *Patriottisme ontmoet pragmatisme: Het Turkse diasporabeleid in Nederland*. Clingendael. https://www.clingendael.org/sites/default/files/2024-10/Clingendael_rapport_Turkse_diasporabeleid_in_Nederland.pdf.

Hybrid Centre of Excellence. (2022). *Hybrid threats as a concept*. Via https://www.hybridcoe.fi/ hybrid-threats-as-a-phenomenon/.

Kahmann, M., & Bellaart, H. (2025). *Ontwikkelingen in de Marokkaans-Nederlandse gemeenschap*. Verwey-Jonker Instituut. https://www.verwey-jonker.nl/wp-content/uploads/2025/06/224240_Ontwikkelingen-in-de-Marokkaans-Nederlandse-gemeenschap-Informatieblad.pdf.

Koster, M. (2023, 18 maart). Russische spionnen die EU-landen zijn uitgezet, werken nu vanuit Servië. RTL. https://www.rtl.nl/nieuws/buitenland/artikel/5372369/rusland-spionage-servie-diplomaten.

Militaire Inlichtingen en Veiligheid (MIVD) (2025). *Openbaar jaarverslag 2024, Militaire Inlichtingen- en Veiligheidsdienst*. Ministerie van Defensie. Openbaar jaarverslag 2024, Militaire Inlichtingen- en Veiligheidsdienst | Jaarverslag | Defensie.nl.

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

Ministerie van Buitenlandse Zaken. (2023). *Algemeen ambtsbericht Iran*. https://open.overheid.nl/documenten/ronl-58198142a5208814509d74495662d9cb772684aa/pdf.

Ministerie van Defensie. (2024). Via MIVD onthult werkwijze Chinese spionage in Nederland | Nieuwsbericht | Defensie.nl.

Ministerie van Defensie. (2025, 21 mei). Via MIVD: Nederland ook doelwit spionagecampagne Russische hackers | Nieuwsbericht | Defensie.nl.

Ministerie van Defensie. (2025). *Russian GRU Targeting Western Logistics Entities and Technology Companies* Russian GRU Targeting Western Logistics Entities and Technology Companies | Rapport | Defensie.nl.

Modderkolk, H. (2021, 17 april). *Huawei kon alle gesprekken van mobiele kpn-klanten afluisteren inclusief die van politici.* Volkskrant. Via https://www.volkskrant.nl/nieuws-achtergrond/huawei kon-alle-gesprekken-van-mobiele-kpn-klanten-afluisteren inclusief-die-van-politici~bd1aece1/.

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

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2025a, januari 29). *Fenomeenanalyse "Over de grens"*. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/documenten/2024/10/17/fenomeenanalyse-over-de-grens.

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2025b, augustus 20). *Ongewenste buitenlandse inmenging*. Ministerie van Justitie en Veiligheid. https://www.nctv.nl/onderwerpen/o/ongewenste-buitenlandse-inmenging.

Nationaal Cyber Security Centrum (NCSC). (2024, 10 juni). *Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices.* Via https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices.

Nationaal Cyber Security Centrum (NCSC). (2025a, 10 februari). *ORB-netwerken en hun impact op de digitale veiligheid in Nederland*. Via https://www.ncsc.nl/actueel/weblog/weblog/2025/orb-netwerken-en-hun-impact-op-de-digitale-veiligheid-in-nederland.

Nationaal Cyber Security Centrum (NCSC). (2025b, 13 augustus). *Casus: Citrix kwetsbaarheid* (update 13-08-2025). Via https://www.ncsc.nl/actueel/nieuws/2025/07/22/casus-citrix-kwetsbaarheid.

Nationaal Cyber Security Centrum. (2024). *Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT*. Via TLP-CLEAR+MIVD+AIVD+Advisory+COATHANGER (1).pdf.

NOS. (2023, 18 februari). *Nederland zet opnieuw Russiche diplomaten uit om spionage.* Via https://nos.nl/artikel/2464355-nederland-zet-opnieuw-russische-diplomaten-uit-om-spionage

NOS. (2025, 7 augustus). Inspectie: veiligheidsregio's moeten zich voorbereiden op landelijke stroomuitvall. Via Inspectie: veiligheidsregio's moeten zich voorbereiden op landelijke stroomuitval.

Openbaar Ministerie (OM). (2025, 26 februari). *Uitbreiding verdenking in zaak Tarwekamp*. Via https://www.om.nl/actueel/nieuws/2025/02/26/uitbreiding-verdenking-in-zaak-tarwekamp.

Pieke, F. N. (2021). *De Chinese gemeenschap in Nederland: Een verkennend onderzoek naar Chinese organisaties, media, en invloed van de Chinese overheid*. Leiden Asia Centre. https://leidenasiacentre.nl/wp-content/uploads/2021/03/F.N.-Pieke.-Chinas-invloed-en-de-Chinese-gemeenschap-in-Nederland.pdf.

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

Rijksoverheid (2025, 7 maart). *Screening voor wetenschappers die met sensitieve kennis willen werken*. Via: Screening voor wetenschappers die met sensitieve kennis willen werken | Nieuwsbericht | Rijksoverheid.nl.

Rijksoverheid. (2025, 15 mei). *Vanaf 15 mei: meer vormen van spionage strafbaar*. Via https://www.rijksoverheid.nl/actueel/nieuws/2025/05/15/vanaf-15-mei-meer-vormen-van-spionage-strafbaar.

Sari, A. (2025). *Protecting maritime infrastructure from hybrid threats: Legal options.* Hybrid CoE. Via: Hybrid CoE Research Report 14: Protecting maritime infrastructure from hybrid threats: legal options.

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*. Clingendael. https://www.clingendael.org/sites/default/files/2025-03/Tussen-Hoop-en-Vrees-2025.pdf.

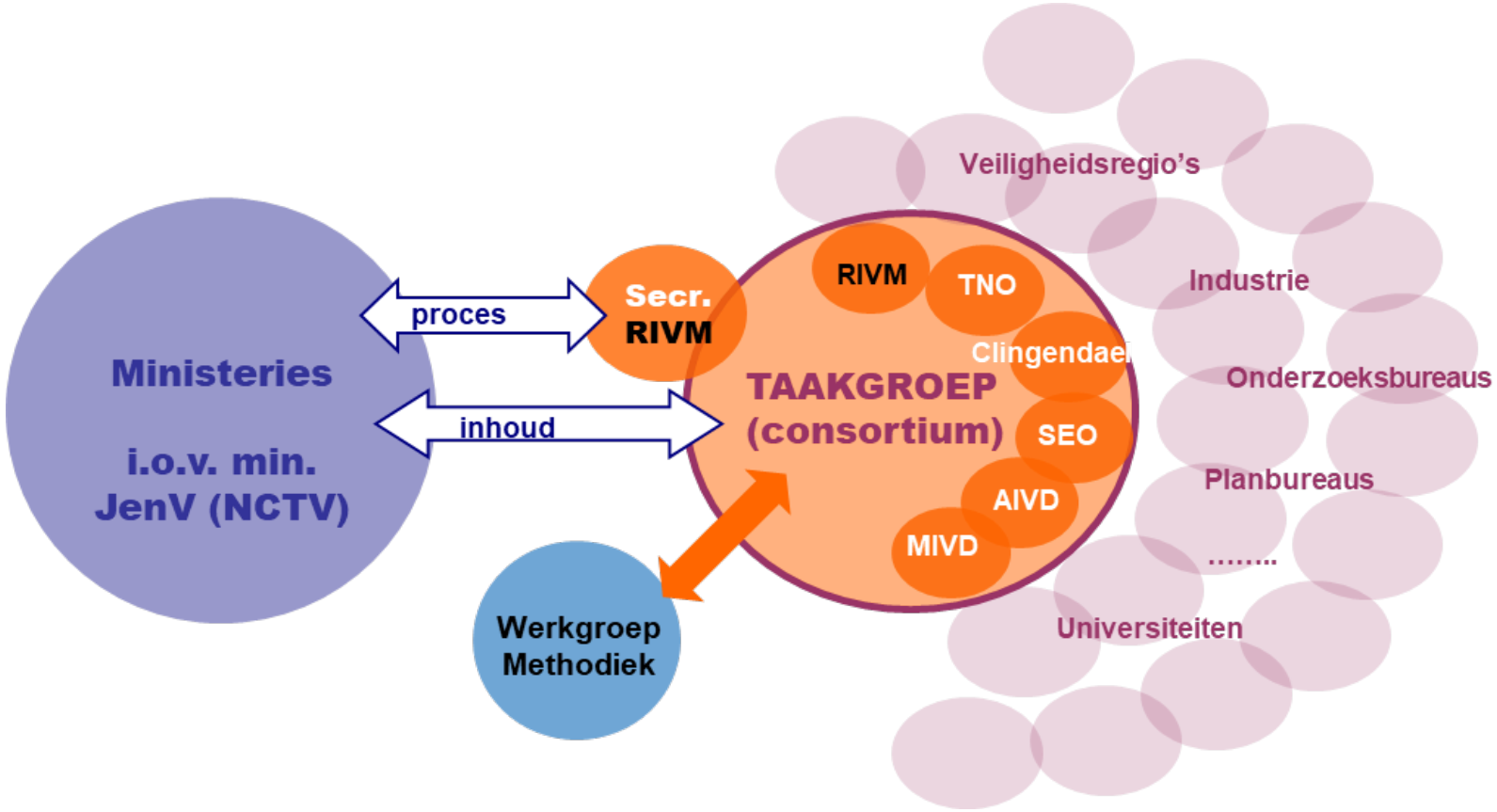
The White House. (2025, 6 februari). *Imposing sanctions on the International Criminal Court.* Via https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.

Van Rosenthal, E. B., & Van Rosenthal, E. B. (2022, 14 oktober). *Uitgezette Russen deden in Nederland aan contraspionage en spionage hightech-sector*. NOS. Via https://nos.nl/artikel/2448319-uitgezette-russen-deden-in-nederland-aan-contraspionage-en-spionage-hightech-sector.

Veiligheidsregio ZHZ (2024). *Regionaal Risicoprofiel.*

Wettenbank (2025). *Wet veiligheidstoets investeringen, fusies en overnames*. Via wetten.nl - Regeling - Wet veiligheidstoets investeringen, fusies en overnames - BWBR0046747.

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