

Verbondenheid in veiligheid

De contouren van een onderzoeks-
agenda voor drie ministeries

Margriet Drent
Danny Pronk
Minke Meijnders

Clingendael Rapport



Clingendael

Netherlands Institute of International Relations



Clingendael

Netherlands Institute of International Relations

Verbondenheid in veiligheid

De contouren van een onderzoeksagenda
voor drie ministeries

Margriet Drent
Danny Pronk
Minke Meijnders

Clingendael Rapport
Oktober 2020

Oktober 2020

Coverfoto: © Pixabay

Ongeautoriseerd gebruik van enig materiaal is een inbreuk op copyright, merkrecht, en / of ander recht. Indien een gebruiker materiaal wil downloaden van de website of van enige andere bron gerelateerd aan het Nederlands Instituut voor Internationale Betrekkingen 'Clingendael' of Instituut Clingendael, voor persoonlijk of niet-commercieel gebruik, dan moet de gebruiker alle voorschriften en wetgeving voor copyright, merkrecht of overige gelijklopende kennisgevingen die zijn opgenomen en weergegeven in het oorspronkelijke materiaal in acht nemen.





Materiaal op de website mag worden gereproduceerd of openbaar gemaakt, verspreid of gebruikt voor publieke en niet-commerciële doeleinden, onder de voorwaarde dat Instituut Clingendael duidelijk als bron wordt vermeld. Toestemming voor gebruik van het logo van Instituut Clingendael is vereist. Deze toestemming kan worden verkregen door een mail te sturen aan de afdeling Communicatie van Instituut Clingendael via press@clingendael.org.

De hiernavolgende web link activiteiten zijn door Instituut Clingendael verboden en kunnen leiden tot inbreuk op merkrecht en copyright: links met oneigenlijk en ongeautoriseerd gebruik van het Clingendael logo in enige vorm, framing, inline links, of metatags, en hyperlinks of enige vorm van gebruik of toepassing van een link die de URL verbergt.

Dit rapport is geschreven in opdracht van het ministeries van Buitenlandse Zaken, het ministerie van Defensie en de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het onderzoek voor dit rapport is afgerond in november 2019.

The Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Volg ons op sociale media

 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute
 clingendael_institute

Email: info@clingendael.org
Website: www.clingendael.org

Inhoudsopgave

Inleiding	1
1 Conceptueel kader voor de interne en externe veiligheidsnexus	3
Inleiding	3
Nexus interne en externe veiligheid	3
Internationaliseringsfenomeen	8
De donkere kant van globalisering	9
Relatieve kwetsbaarheid van Nederland	13
Transportbanden tussen interne en externe veiligheid	15
Conclusies en suggesties onderzoekskader	17
2 Grensoverschrijdende dreigingen en dreigingsactoren volgens Nederlandse beleidsdocumenten	18
Inleiding	18
Grensoverschrijdende dreigingen in de Nederlandse beleidsdocumenten	18
Caribische delen van het Koninkrijk (Aruba, Curaçao, Sint-Maarten en de BES-eilanden)	24
Conclusies	26
3 Onderzoeksbenaderingen risicoanalyses nationale veiligheid	28
Inleiding	28
Elementen voor de onderzoeksagenda	42
4 Een casus voor de gecombineerde actor- en dreiging-centrische benadering: “hybride conflictvoering”	43
Inleiding	43
Een dreiging-centrische benadering	43
Een actor-centrische benadering	44
De gecombineerde actor- en dreiging-centrische benadering	45
Stap 1A: Wat zijn de verschillende manifestaties van de dreigingen?	46
Stap 1B: Komt de dreiging van een bekende en moedwillige actor?	46
Stap 2: Analyseer welke intentie, welk vermogen en welke gelegenheid de actor heeft om deze dreiging uit te voeren.	46
Stap 3: Van welk palet aan andere dreigingen van deze actor is deze dreiging onderdeel?	47
Stap 4: Zijn er nog andere actoren en welke dreigingen worden verwacht in de komende vijf jaar aan de hand van intentie, vermogen en gelegenheid?	52
Conclusies	54

5	De percepties, performativiteit, politiek en politiea ten aanzien van grensoverschrijdende veiligheidsvraagstukken	55
	Inleiding	55
	Onzekerheid door complexiteit	55
	Perceptieverschillen over problemen	57
	Performativiteit van beleid	58
	'Wicked Problems'	58
	De politieke context	60
	Verticale coördinatie	63
	Horizontale coördinatie	65
	Van theorie naar onderzoek	66
6	Verbondenheid in veiligheid: contouren van een gemeenschappelijke onderzoeksagenda	68
	Bijlagen	74
	Literatuurlijst	74
	Belang: Internationale Rechtsorde	80

Inleiding

Het landschap van de nationale en internationale veiligheid is sterk aan het veranderen. Door globalisering vervaagt steeds meer het onderscheid tussen lokaal, nationaal, Europees en mondiaal en dat heeft zijn effecten op veiligheid. Er is een nieuwe veiligheidsagenda ontstaan. De gevolgen hiervan voor dreigingsanalyses, de kennisbasis en hoe we ons organiseren om deze nieuwe dreigingsagenda het hoofd te kunnen bieden, zijn nog niet uitgekristalliseerd.

Het doel van dit rapport is om kaders te identificeren voor een onderzoeksagenda voor de ministeries van Buitenlandse Zaken, Justitie & Veiligheid en Defensie over de dreigingen voor de nationale veiligheid voortkomend uit de effecten van globalisering.¹ Hoe kunnen we de zogenaamde 'nexus interne en externe veiligheid' beter begrijpen in de context van een zich transformerende globalisering? Op welke wijze kunnen we de risico's die op ons af komen beter analyseren, zodat Nederland anticiperend kan handelen? Welke kennis hebben de drie ministeries nodig om gezamenlijk deze uitdagingen aan te gaan? Dit rapport zal de stand van zaken van de literatuur bespreken, knelpunten en oplossingsrichtingen aangeven en suggesties doen voor toekomstige onderzoeksprioriteiten. De bedoeling is aan de hand van dit stuk de drie ministeries meer houvast te geven in de structurering van hun gezamenlijke onderzoeksagenda.

In een poging de nexus tussen interne en externe veiligheidsvraagstukken te conceptualiseren en te komen tot een wetenschappelijke onderzoeksagenda, stelden de Zweden Eriksson en Rhinard in 2009 voor om vijf dimensies van elkaar te onderscheiden, te weten: *problems*, *perceptions*, *policies*, *politics* en *polity*. 'Problemen' zijn in dit verband de grensoverschrijdende veiligheidsvraagstukken die relevant zijn voor de nationale veiligheid, de overige vier hebben te maken met respectievelijk de manier waarop en het perspectief van waaruit deze problemen worden waargenomen door burgers en beleidsmakers; met de beleidsaanpak van de problemen; met de politieke constellaties die ermee zijn gemoeid en met de institutionele structuren die een rol spelen bij de aanpak ervan.² Deze vijf dimensies komen ook terug in ons rapport.

1 De auteurs zijn een aantal collega's bij Clingendael zeer dankbaar voor hun bijdragen, deze zijn: Kimberley Kruijver, Jurgen Oppel, Adája Stoetman, Kevin de Raat en Dick Zandee.

2 J. Eriksson & M. Rhinard, (2009), 'The Internal-External Security Nexus: Notes on an Emerging Research Agenda', in *Cooperation and Conflict*, 44(3), pp. 243-267.

In het eerste hoofdstuk zal worden ingegaan op de dimensie van *problems*: wat verstaan we onder de term 'nexus interne en externe veiligheid', en hoe kunnen we deze verder conceptualiseren, zodat deze relevant wordt voor de Nederlandse context? In hoofdstuk twee volgt een korte scan van bestaande strategiedocumenten en risicoanalyses om te bepalen wat de belangrijkste trends zijn in de aard, ernst en omvang van grensoverschrijdende dreigingen voor de Nederlandse nationale veiligheid (inclusief de overzeese gebieden). Vervolgens wordt in hoofdstuk drie geanalyseerd op welke wijze in Nederland geïntegreerde risicoanalyses worden uitgevoerd die recht doen aan de veranderende aard van nationale en internationale veiligheidsdreigingen. Het rapport doet naar aanleiding van die analyse aanbevelingen voor verbeteringen en doet een voorstel voor een 'gecombineerde actor- en dreigingsanalyse'. In het hoofdstuk daaropvolgend wordt de gecombineerde actor en dreigingsanalyse getoetst op het fenomeen 'hybride dreigingen' om via deze casus te bepalen wat een dergelijke analyse oplevert en welke lessen we eruit kunnen leren.

Daarna komen in hoofdstuk vijf *perceptions, policies, politics* en *polity* aan bod. De Nederlandse termen *percepties, performativiteit, politiek* en *politeia* worden gebruikt. Hier wordt ingegaan op de manier waarop en het perspectief van waaruit de vraagstukken worden waargenomen door de betrokken beleidsmakers. Ook wordt de inhoudelijke en procesmatige effectiviteit van het beleid en de politieke context waarbinnen de interdepartementale samenwerking plaatsvindt geanalyseerd. Tenslotte komen de bestuurlijke arrangementen aan bod die een rol spelen bij de ambtelijke coördinatie van de aanpak van grensoverschrijdende veiligheidsvraagstukken.

Het rapport sluit af met het identificeren van de kaders voor een onderzoeksagenda over de dreigingen voor de nationale veiligheid voortkomend uit de nexus tussen interne en externe veiligheid. Bij de suggesties welke prioriteiten, problemen en oplossingsrichtingen hierbij aandacht verdienen, wordt rekening gehouden met de handelingsperspectieven van de drie ministeries en de benodigde en beschikbare kennis, intenties, vermogens en gelegenheid om te handelen. De veranderende veiligheidsagenda vereist 'verbondenheid in veiligheid' van deze ministeries.

1 Conceptueel kader voor de interne en externe veiligheidsnexus

Inleiding

De grenzeloosheid van onze veiligheid is zeker geen nieuw fenomeen. In de afgelopen jaren lijkt de scheidslijn tussen interne en externe veiligheid echter steeds sneller te vervagen door mondialiseringseffecten, aangejaagd door de razendsnelle technologische en digitale ontwikkelingen. Geografisch afgebakende landsgrenzen zijn steeds minder relevant voor het categoriseren van dreigingen. De complexe relatie tussen nationale en internationale veiligheid en tussen dreigingen die traditioneel werden gezien als behorend bij interne of externe veiligheid wordt een zogenaamde 'nexus' genoemd. Dit hoofdstuk analyseert op welke wijze de beleidsmatige en academische literatuur deze nexus beschouwt. Daarna volgt het vraagstuk hoe er wordt gedacht over 'internationalisering' of 'globalisering' en welk verband dit heeft met veiligheidsdreigingen. Nederland is relatief kwetsbaar voor deze 'donkere kant' van globalisering. Waarom dit het geval is wordt hier besproken. Tenslotte gaat dit hoofdstuk in op welke wijze de 'transportband' tussen dreigingen en factoren in onze samenleving kan worden geconcipieerd. Het hoofdstuk sluit af met een samenvatting van elementen ten behoeve van een onderzoeksagenda op het gebied van de interne- en externe veiligheidsnexus.

Nexus interne en externe veiligheid

In Nederlandse beleidsdocumenten wordt niet expliciet gesproken over de 'interne en externe veiligheidsnexus'.³ Een term die wel vaak naar voren komt is 'verwevenheid'. Zowel in de Geïntegreerde Buitenland en Veiligheidsstrategie (GBVS)⁴ als in de BHOS-nota en de HGIS-nota⁵ wordt erkend dat dreigingen binnen en buiten Nederland steeds

3 Ministerie van Buitenlandse Zaken, (2013), *Internationale Veiligheidsstrategie: Veilige Wereld, Veilig Nederland*, p. 2.

4 Ministerie van Buitenlandse Zaken. (2018). *Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022*.

5 Nota Buitenlandse Handel en Ontwikkelingssamenwerking, *Investeren in Perspectief*, 18-5-2018 en de Nota Homogene Groep Internationale Samenwerking 2019 (18-9-2018).

meer verweven zijn geraakt en dat daarmee een groeiende verwevenheid is ontstaan tussen interne en externe veiligheid. De Defensienota (2018) spreekt in dit verband van een ‘verknoping’ van de Nederlandse veiligheid met die van de buitenwereld. Ook de Nationale Contraterrorisme Strategie (2016-2020) herkent deze trend: “extern is intern – we spelen in op de verwevenheid van de internationale, nationale en lokale dimensies⁶ van extremisme en terrorisme”. Het kabinet onderschrijft de conclusie van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat een strategisch en samenhangend veiligheids- en defensiebeleid gestoeld moet zijn op een breed veiligheidsbegrip en een geïntegreerde benadering. De brief ‘Tegengaan statelijke dreigingen’ (18 april 2019) spreekt van verwevenheid van ‘geopolitiek, economie en veiligheid’. De kabinetsbrede Nationale Veiligheid Strategie 2019, dat zowel over *safety* als *security*⁷ gaat, benadrukt relatief laat in het document (op pagina 17) dat nationale veiligheid niet ophoudt bij de landsgrenzen en dat “Interne en externe veiligheid meer en meer met elkaar verweven [zijn] en vragen om meer integratie van de nationale veiligheidsaanpak.”⁸ De Nationale Veiligheid Strategie gebruikt wel het begrip ‘interne en externe veiligheidsnexus’, maar doet dit in verband met het ontwikkelen van een gezamenlijke onderzoeksagenda waar dit rapport aan moet bijdragen.

De academische literatuur over het concept ‘interne en externe veiligheidsnexus’ is beperkt en de term wordt niet vaak gebruikt noch goed uitgewerkt. Er wordt nog het meest aan gerefereerd in het kader van de Europese Unie.⁹ In de internationale veiligheidsliteratuur werd tot ongeveer het jaar 2000 traditioneel een scheiding aangehouden tussen interne en externe veiligheidsvraagstukken. Het bipolaire karakter van de wereldorde in de periode 1945-1990 hield deze scheiding mede in stand. De existentiële militaire dreigingen waarmee de Sovjet-Unie en de Verenigde Staten en bondgenoten elkaar in de greep hielden, waren typisch een externe, militaire statelijke dreiging. De ernst van deze dreigingen en de logica van afschrikking

6 Alleen het ministerie van Justitie en Veiligheid noemt lokale dimensies. Het ministerie van Defensie kent ‘nationale taken’ voor de krijgsmacht, die nauw samenhangen met de civiel-militaire samenwerking in Nederland.

7 Het Nederlands kent niet zoals het Engels een goed onderscheid tussen ‘*safety*’ en ‘*security*’. Waar ‘*safety*’ gaat over het vrij zijn van dreigingen die niet intentioneel zijn, is ‘*security*’ een begrip waarmee vrijheid van moedwillige dreigingen afkomstig van andere menselijke actoren aangeduid wordt.

8 *Nationale Veiligheid Strategie 2019*, via: <https://www.nctv.nl/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019>

9 I. Ioannides & G. Collantes-Celador, (2011), ‘The internal-external security nexus and EU police/rule of law missions in the Western Balkans’, in *Conflict, Security & Development*, 11(4), pp. 415-445; F. Trauner, (2011), ‘The Internal-External Security Nexus: More Coherence Under Lisbon?’, in *SSRN Electronic Journal*; I. Ioannides, (2014), ‘Inside-out and outside-in: EU security in the neighbourhood’, in *The International Spectator*; W. Rees, (2008), ‘Inside Out: the External Face of EU Internal Security Policy’, in *Journal of European Integration*, 30(1), pp. 97-111.

vertroebeelden het zicht op andere typen dreigingen.¹⁰ De grote veranderingen op economisch, technologisch en sociaal gebied in combinatie met het einde van de Koude Oorlog, maakten de veranderingen in de veiligheidsdreigingen steeds meer zichtbaar.¹¹ De wijze waarop maatschappijen veranderden en werden ingericht, maakte ze kwetsbaarder voor grensoverschrijdende veiligheidskwesties. Militaire dreigingen bleven, ook al veranderden zij van gedaante, maar steeds prominenter kwamen grensoverschrijdende dreigingen op die niet eenvoudig aan een bepaalde departementale verantwoordelijkheid toe te schrijven waren. Er is in de literatuur en in beleidsdocumenten een consensus ontstaan dat belangrijke veiligheidsdreigingen voor het Euro-Atlantisch gebied noch puur intern, noch puur extern van aard zijn, maar transnationaal. Deze de-territorialisering¹² van dreigingen, of *transboundary threats* worden in de literatuur getypeerd aan de hand van de oorsprong, welk traject ze afleggen en de primaire en secundaire effecten die ze hebben op veiligheid:

[Transboundary threats] originate from opaque locations, cross political and functional boundaries with ease and can affect a wide variety of referent objects.¹³

Huidige veiligheidsvraagstukken kenmerken zich doordat dreigingen – gefaciliteerd door globalisering – een grotere *complexiteit* kennen in termen van de oorsprong van een dreiging, het traject dat de dreiging aflegt en de primaire en secundaire effecten die zij heeft. Dit staat buiten kijf wat betreft zogenaamde 'niet-moedwillige' dreigingen, zoals pandemieën, technische storingen en overstromingen, waar de bron van de dreiging obscuur kan zijn. Denk aan het tot wapen maken van pathogenen door terroristische groeperingen, het hacken van technische systemen door *proxies* van staten en de rol van de mens in klimaatverandering. De wederzijdse afhankelijkheid en verbondenheid op allerlei terreinen kan zorgen voor complexe knooppunten en onvoorspelbare wegen waarlangs een dreiging reist en haar effecten uitoefent. Interstatelijke competitie bestaat nog steeds, en maakt, sterker nog, een stevige *comeback*. De intenties en vitale belangen van verschillende actoren lijken onveranderd, maar de wijze waarop zij deze belangen en intenties verdedigen en er uitvoering aan geven, is echter grotendeels wel veranderd. Ook als slechts één actor schuilt achter een bepaalde dreiging, vraagt de toegenomen kwetsbaarheid van samenlevingen alertheid op de verschillende wijzen waarop instrumenten door die actor wordt ingezet. Doordat het weefsel van onze wereld

10 J. Eriksson & M. Rhinard, (2009), 'The Internal-External Security Nexus: Notes on an Emerging Agenda', in *Cooperation and Conflict*, 44 (3), p. 245.

11 B. Buzan, O. Waever, & J. de Wilde, (1998), *Security: A New Framework for Analysis*. (Boulder-CO: Lynne Rienner Publishers).

12 Zie: Rees (2008), 'Inside Out: the External Face of EU International Security Policy', in *Journal of European Integration*, 30(1), p. 97.

13 Eriksson & Rhinard, The internal-external security nexus, p. 247.

en samenleving door globalisering zo is gewijzigd, zijn strategieën en hun instrumenten daaraan aangepast. Onderdeel van deze strategieën zijn onvoorspelbaarheid, anonimiteit en een grote diversiteit aan verschillende, vaak niet-militaire, instrumenten, tactieken en doelen.

De veiligheidsnexus wordt daarmee niet alleen gekenmerkt door grensoverschrijdendheid in strikte zin (intern versus extern), maar ook door het overstijgen van de traditionele grenzen tussen verschillende sectoren en domeinen (justitie-, defensie-, economisch, financieel, industrieel, technologisch, politie-, sociaal, culturele, maatschappelijke, ecologische en politieke domeinen).¹⁴ Doordat de dreigingen veelal multi-sectoraal zijn geworden, zal een succesvolle voorkoming, afschrikking en bestrijding vaak ook multi-sectoraal moeten worden aangepakt. Het zal niet alleen op een '*whole-of-government*' manier moeten worden vormgegeven (zie hiervoor ook Hoofdstuk 5), maar op een '*whole-of-society*' manier. Door op een nieuwe manier van omgaan met veiligheid zijn in de keten belangen-preventie-dreigingen-weerbaarheid, de preventieve maatregelenkant en de weerbaarheidzijde nog onderontwikkeld en behoeven deze meer conceptualisering.

Het denken over dreigingen in interne of externe veiligheidscategorieën lijkt achterhaald. Voor analytische helderheid kan nagedacht worden langs de lijnen van in welke mate dreigingen qua oorsprong nationaal of internationaal zijn, of in welke mate ze een combinatie van beide zijn; het traject dat de dreiging aflegt van bron naar impact en waar de impact wordt gevoeld. In tabel 1 wordt hier een voorbeeld van gegeven.

14 A. P. Brandao, (2015), 'The internal-external security nexus in the security narrative of the EU', *JANUS.NET, e-journal of International Relations*, 6(1), p. 4.

Tabel 1 Taxonomie van de veiligheidsnexus

Oorsprong	Traject	Impact	Voorbeelden
1. Bron puur nationaal	Binnen geo-grafische grenzen	Nationaal	Lokale criminaliteit (bv: huiselijk geweld) Windmolenterrorisme Illiberale groeperingen
2. Bron combinatie van nationaal/ internationaal	Grensoverschrijdend	Nationaal en internationaal	Mondiaal terrorisme Hybride dreigingen Cyberdreigingen Ongewenste buitenlandse beïnvloeding Grensoverschrijdende criminaliteit
3. Bron puur internationaal	Grensoverschrijdend	Nationaal en internationaal	Interstatelijke nucleaire dreiging Interstatelijke conventionele dreiging

In het rapport 'Een wereld van verbindingen' uit 2017, adviseert de WRR een geïntegreerde veiligheidsstrategie uit te werken die de interne en externe veiligheid omvat voor zover die intrinsiek met elkaar verband houden. De WRR hint hierbij impliciet op een taxonomie, waarin 'gewone' criminaliteit niet thuis zou horen. Wel noemt de WRR "de bestrijding van internationaal terrorisme en cyberaanvallen door andere staten; daarbij gaat het immers", aldus het rapport, "om door organisaties zoals Da'esh of andere staten aangezette pogingen om de Nederlandse samenleving te ontwrichten".¹⁵ Het rapport van de WRR laat echter in het midden welke interne en externe veiligheidskwesties "intrinsiek" met elkaar verband houden. Een taxonomie of classificatie zoals hierboven in de tabel weergegeven, laat zien dat de oorsprong of de bron van een dreiging zelden een puur nationaal karakter heeft. Door de aard van onze samenlevingen kan ook 'gewone' criminaliteit een duidelijke link over onze grenzen hebben. Denk bijvoorbeeld aan de onlangs bekend geworden criminaliteitscijfers onder asielzoekers, culturele aspecten van huiselijk geweld, delicten die worden gepleegd ter ondersteuning van terroristische organisaties of de transnationale netwerken van bepaalde actievoerders (bv. de gele hesjes of klimaatactivisten). Ook wanneer de bron 'puur internationaal' is, kent deze zogenaamde 'puur internationale' categorie van veiligheidsdreigingen een nationale dimensie. Uiteraard gaat het hier over de impact van de nucleaire en/of conventioneel militaire dreiging voor het Nederlands grondgebied, maar ook over de nucleaire taak in het kader van de NAVO en de bijstandsverplichting die Nederland is aangegaan ten aanzien van zijn bondgenoten.

Deze poging om de veiligheidsnexus te ontwarren in categorieën van intern versus extern en daarmee de terreinen te onderscheiden die daadwerkelijk (of 'intrinsiek') grensoverschrijdend zijn, laat zien hoe verweven nagenoeg alle dreigingen zijn. Derhalve is het de vraag in hoeverre het nog zinvol is te spreken over een 'interne-

¹⁵ WRR, (2017), *Veiligheid in een Wereld van Verbindingen. Een strategische visie op het defensiebeleid*, (Den Haag), p. 174.

externe veiligheidsnexus' en of het niet correcter is om over een 'veiligheidsnexus' te spreken, zonder het bijvoeglijk naamwoord 'interne-externe' erbij. Alleen spreken over 'veiligheidsdreigingen' in het algemeen valt ook te overwegen. Echter, vanwege de andere vier domeinen van de interne-externe veiligheidsnexus van Eriksson en Rhinard – *perceptions, policies, politics en polity* – zal het discours nog een tijd overeind blijven. Meer hierover volgt in hoofdstuk 5.

Internationaliseringsfenomeen

Het fenomeen 'globalisering' kent meerdere gezichten, maar in de context van veiligheid wordt het gezien als één van de belangrijkste aanjagers van de verandering van het veiligheidsconcept. De term kent een rijke geschiedenis in de academische literatuur en werd al in de jaren dertig van de vorige eeuw gebruikt. Er zijn auteurs die in de economische expansie van de zestiende eeuw al een vorm van globalisering zien. Ook zijn er scholen die allerlei 'golven' van globalisering onderscheiden. Deze golven vallen ruwweg samen met de verschillende industriële revoluties.¹⁶ De NCTV ontwijkt in de startnotitie voor dit rapport de term globalisering en gebruikt 'internationalisering', dat wordt gedefinieerd als: "het mondiale proces van vrij(er) wordend verkeer van mensen; goederen; kapitaal en informatie (incl. gedachtegoed)". Het Ministerie van Buitenlandse Zaken (BZ) gebruikt beide termen 'internationalisering' en 'globalisering', en verstaat onder 'globalisering': "een voortdurend/permanent proces van wereldwijde economische, politieke, sociale en culturele integratie, met als centraal kenmerk het verdwijnen van absolute en relatieve afstanden, dankzij voortschrijdende informatie- en communicatietechnologie en internationale handel".¹⁷ De definities verschillen met name in het aspect dat die van BZ gedetailleerder is en de term 'integratie' gebruikt.

De term globalisering is kwalitatief een andere dan de term internationalisering. Hoewel beide termen vaak worden gebruikt om hetzelfde aan te geven, zijn ze niet uitwisselbaar. Voor verder onderzoek en begrip van de nationale veiligheidsaspecten van het maatschappelijk fenomeen dat geassocieerd wordt met globalisering, is het belangrijk duidelijk te maken wat de definities van beide zijn. Scholte is één van de auteurs die het belang van een goede definitie van de term globalisering onderstreept. Hij constateert een onterecht gebruik van termen als synoniemen van globalisering zoals 'internationalisering', 'universalisering', 'liberalisering' en 'westernisering'.¹⁸ Hier wordt alleen ingegaan op de verschillen tussen globalisering en internationalisering.

16 Zie: P. James & M. B. Steger, (2014), 'A Genealogy of 'Globalization': The Career of a Concept', in *Globalizations*, 11(4), pp. 417-434.

17 GBVS, 2018.

18 J.A. Scholte, (2007), 'Defining Globalization', in *Cim.economía*, 10, pp. 15-63.

Internationalisering wordt door sommige auteurs gebruikt als synoniem voor globalisering en door anderen als een subcategorie, namelijk als een bepaalde mate van globalisering. Scholte vindt dat als globalisering wordt geïnterpreteerd als internationalisering, dit verwijst naar een groei van transacties en interdependentie tussen staten. Vanuit dat perspectief, zo betoogt hij, gaat het alleen om de kwantiteit van interacties en de mondiale schaal en niet om de kwalitatieve transformatie.¹⁹

Globalisering is volgens hem meer dan een overtreffende trap van internationalisering. Als er geen kwalitatief verschil is, behalve in gradatie, dan is het ook niet mogelijk om een onderscheid te maken in de fase van globalisering ten opzichte van historische fases (zoals de late 19^e eeuw) waarin grensoverschrijdende fenomenen ook sterk groeiden. Ook is het interstatelijke karakter van internationalisering te beperkt, zo betoogt Scholte. 'Globalisering-als-Internationalisering' impliceert dat sociale relaties alleen georganiseerd kunnen zijn in termen van landen, regeringen en nationale gemeenschappen. Globalisering behelst echter een fundamentele wijziging van het karakter van de onderliggende sociale geografie: de mondiale spreiding van de connecties tussen mensen en zelfs het verdwijnen van obstakels van de stroom van goederen en diensten tussen landen (supra-territorialiteit). Deze ontwikkeling is al veel langer gaande, maar de mate waarin is rond de eeuwwisseling enorm versneld. Mensen zijn fysiek, juridisch, cultureel en psychologisch in staat om elkaar te ontmoeten waar zij zich op aarde ook bevinden.

De snelheid waarmee globalisering zich transformeert, neemt steeds verder toe, aangejaagd door technologische ontwikkelingen. Dit betekent dat de wereld zich anno 2019 nog in een vroege fase van de transformatie bevindt. Digitalisering, robotisering, kunstmatige intelligentie, het *internet of things* en *3D printing* zullen verder onze wijze van produceren, werken, mobiliteit en consumeren sterk veranderen. Het is daarom belangrijk beter te begrijpen op welke wijze de aard van globalisering onze maatschappij en de wereld waarin wij leven verder gaat beïnvloeden, en daarmee ook onze veiligheid in brede zin op de middellange en langere termijn.²⁰

De donkere kant van globalisering

De nationale veiligheidsaspecten van globalisering worden door vele auteurs in de literatuur onderstreept. Globalisering kan opgevat worden als een "complexe matrix van oorzaak- en gevolg- verbanden", die ertoe hebben geleid dat statische concepten

¹⁹ Ibid, p. 21.

²⁰ European Commission, (2017), *Reflection Paper on Harnessing Globalisation*, via: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-globalisation_en.pdf.

van veiligheid moeten worden heroverwogen.²¹ In de academische literatuur zijn de meningen verdeeld of globalisering nu de internationale veiligheidssituatie verslechtert of verbetert. Dat staten en samenlevingen, naarmate ze meer 'geglobaliseerd' zijn, meer te maken hebben met de rest van de wereld is duidelijk. De manier waarop samenlevingen zijn georganiseerd, versterkt de dynamiek van grensoverschrijdende veiligheidskwesties.²² Dit kan zowel negatieve (veiligheidsproblemen) als positieve (meer welvaart, kennis en invloed) effecten opleveren. De liberale, democratische vrede en normatieve scholen in de Leer der Internationale Betrekkingen beargumenteren dat juist de toename van interacties en afhankelijkheid tussen actoren en de verspreiding van gedeelde normen en waarden, de kans op conflict en oorlog verkleint. Anderen claimen dat globalisering de rol van de traditionele soevereine staat als producent van veiligheid dermate aantast dat de veiligheid van staten en hun burgers afneemt.²³

De rol van de staat is een zeer veel bediscussieerd onderwerp in de academische literatuur over internationale veiligheid. In reactie op de krachten en effecten van globalisering lijken de laatste jaren juist nationalistische krachten weer de kop op te steken. De Amerikaanse presidentiële kandidaat Donald Trump verklaarde bijvoorbeeld in een speech in 2016: "*we will no longer surrender this country or its people to the false song of globalism.*"²⁴ In het algemeen lijkt globalisering kansen te bieden voor Nederlanders en Europeanen, maar het is gebleken dat deze de vruchten van globalisering eenzijdig terecht komen bij hoogopgeleide kenniswerkers, wat een tweedeling in maatschappijen teweeg heeft gebracht. Grote groepen vrezen dat hun kinderen slechter af zullen zijn dan zijzelf en voelen een verlies van hun identiteit en tradities.²⁵ Polarisatie in de Nederlandse en Europese samenlevingen, mede veroorzaakt door effecten van globalisering, heeft impact op de nationale veiligheid omdat dit het draagvlak onder de gedeelde waarden en normen van de nationale en internationale rechtsorde kan aantasten. Hierdoor is het erg belangrijk om voldoende aandacht te geven aan de subjectiviteit van dreigingen en de verschillen in percepties tussen de elite en het brede publiek. De veiligheidsbeleving onder verschillende segmenten van de samenleving kan sterk verschillen en vraagt daardoor sensitiviteit voor de aanpak van veiligheidsdreigingen.

21 C. Rudolph, (2003), 'Globalization and Security: Migration and Evolving Conceptions of Security in Statecraft and Scholarship', in: *Security Studies*, 13(1), pp. 1-32.

22 M. Kaldor, (2006), *New and Old Wars: Organized Violence in a Global Era*. (Palo Alto, CA: Stanford University Press).

23 N.M. Ripsam, (2010), 'Globalization and the National Security State', *Foreign Affairs*, pp. 20-21.

24 O. Rosenboim, (2017), 'Globalism and Nationalism. Why interconnectedness does not threaten sovereignty', in *Foreign Affairs*. Trump ziet 'Globalism' als een ideologie van groeperingen die de VS het fenomeen van globalisering willen opdringen. Hij gebruikt 'patriotism' als tegenhanger van 'globalism'. Zie: G. Rachman, (2018), 'Why Globalism is Good for You', in *Financial Times*, 29 oktober.

25 European Commission, (2017), *Reflection Paper on Harnessing Globalisation*, p. 9, via: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-globalisation_en.pdf.

Meer directe veiligheidsdreigingen, die in verband worden gebracht met (de effecten van) globalisering, en die in de literatuur het meest worden genoemd zijn ongecontroleerde migratie²⁶, georganiseerde transnationale criminaliteit, terrorisme en vormen van cyberdreigingen (spionage, criminaliteit, sabotage). Zie ter illustratie een overzicht uit een korte, niet uitputtende, literatuurstudie in tabel 2.

Tabel 2 Overzicht veiligheidsdreigingen en bijbehorende actoren
(als aanjagers of als manifestaties)

Veiligheidsdreigingen	Actoren ²⁷
Ongecontroleerde, irreguliere migratie ²⁸	<ul style="list-style-type: none"> • Illegale migranten²⁹
Georganiseerde misdaad ³⁰ (m.n. drugs- en mensensmokkel) ³¹ Transnationale georganiseerde misdaad (drugs- en mensensmokkel) ³²	<ul style="list-style-type: none"> • “Colombian, Nigerian, Russian, Albanian, Turkish and other non-EU groups”³³ • Georganiseerde criminele netwerken³⁴ • Polen, Servië, Rusland³⁵ • Drugskartels, gangs, illegale netwerken³⁶
Terrorisme ³⁷	<ul style="list-style-type: none"> • Islamitische staat / Da’esh³⁸ • Extremistische groeperingen³⁹ (e.g. Al-Qaida)⁴⁰ • Falende staten⁴¹ • Staten en terroristische groeperingen⁴²

26 ‘Ongecontroleerde migratie’, in de zin van verplaatsing van mensen buiten vooraf afgesproken regels.

27 Sommige actoren worden niet genoemd in de geraadpleegde literatuur, deze vakjes zijn leeg.

28 Council of the European Union, doc. 15446/05, op. cit. in note 3, p. 5-8; EU Global Strategy (EUGS) 2016; Van der Laan, F. & M. Drent (2017) “Veranderende veiligheidsomgeving – Grip op het grenzeloze werk van de Nederlandse Politie” in: *Cahier Politiestudies*; Drent, M., Dinnissen, R., van Ginkel, B., Hogeboom, H. & Homan, K. (2015) *The Relationship between internal and external security*; Trauner, F. (2011), p. 7.

29 “The State of Internal Security in the EU. A joint Report by EUROPOL, EUROJUST, and FRONTEX”.

30 Van der Laan, F. & M. Drent (2017) “Veranderende veiligheidsomgeving – Grip op het grenzeloze werk van de Nederlandse Politie”, in: *Cahier Politiestudies*; EUGS, (2016); Trauner, F. (2011), p. 7.

31 Council of the European Union, doc. 15446/05, op. cit. in note 3, p. 5-8.

32 McQuaid, J. & P. G. Faber & Z. Gold (2017) *Transnational Challenges and U.S. National Security: Defining and Prioritizing Borderless Threats*, p. 7.

33 “The State of Internal Security in the EU. A joint Report by EUROPOL, EUROJUST, and FRONTEX”.

34 Trauner, F. (2011) The internal-external security nexus: more coherence under Lisbon?, Occasional paper EUISS.

35 Rees, W. (2008), ‘Inside Out: The External Face of EU Internal Security Policy’ in: *European Integration*, 30(1), 97-111.

36 McQuaid et al., (2017), p. 7.

37 Council of the European Union, doc. 15446/05, op. cit. in note 3, p. 5-8; Drent, M., et. al (2015); Trauner, F. (2011), p. 7.

38 Mogherini, F. (2015); van der Laan, F. & M. Drent (2017).

39 Trauner, F. (2011) The internal-external security nexus: more coherence under Lisbon?, Occasional paper EUISS.

40 McQuaid et al., (2017), p. 7.

41 Trauner, F. (2011).

42 Renard, T. (2016). ‘Partnering for Global Security: the EU, Its Strategic Partners and Transnational Security Challenge’, in: *European Foreign Affairs Review*, 21(1), p. 12.

Veiligheidsdreigingen	Actoren
Cyberaanval ⁴³ Cyber (<i>spionage, oorlogsvoering, terrorisme en criminaliteit</i>) ⁴⁴ Cyberonveiligheid /cyberaanvallen ⁴⁵ Consumenten cybercriminaliteit ⁴⁶ Digitale/cyber connectiviteit ⁴⁷	<ul style="list-style-type: none"> In China, Rusland, Zuid-Afrika: regering en wetshandhaving instanties⁴⁸
Public order ('openbare orde') ⁴⁹	
Hybride dreigingen ⁵⁰	<ul style="list-style-type: none"> Rusland⁵¹ "Poetin-regering"⁵²
Klimaatverandering ⁵³ Vernietiging van het milieu ⁵⁴ Milieuvervuiling ⁵⁵	
Energieveiligheid ⁵⁶ <ul style="list-style-type: none"> Aardbevingen in het noorden van Nederland en de daaruit volgende afhankelijkheid van Russisch gas.⁵⁷ 	
Economische volatiliteit ⁵⁸ Economische instabiliteit ⁵⁹	<ul style="list-style-type: none"> Economische en monetaire unie, douane-unie, vrijhandelszones⁶⁰ BRICS⁶¹ Private financiële actoren⁶²

43 Trauner, F. (2011); Drent, M. et al. (2015).

44 Van der Laan, F. & M. Drent (2017).

45 Kovalčíková, N. (2014). 'Globalisation and the threats it poses in the twenty-first century', in: *European View*, 13: 169-179.

46 Ibid.

47 McQuaid et al., (2017), p. 8.

48 Kovalčíková, N. (2014).

49 Van der Laan, F. & M. Drent (2017).

50 EUGS (2016).

51 Ibid.

52 Van der Laan, F. & M. Drent (2017).

53 EUGS (2016).

54 Kovalčíková, N. (2014).

55 Drent, M. et al. (2015).

56 EUGS (2016); Kovalčíková, N. (2014).

57 Jovanovic et al., (2016).

58 EUGS (2016).

59 Kovalčíková, N. (2014).

60 McQuaid et al., (2017), p. 8.

61 Ibid.

62 Ibid.

Veiligheidsdreigingen	Actoren
Militaire conflicten ⁶³ • Rusland-Oekraïne conflict ⁶⁴	
Dreigingen voor de gezondheidszorg ⁶⁵ (epidemieën en ziektes ⁶⁶)	
Humanitaire crises (effect op menselijke welvaart, massaal humanitair lijden) ⁶⁷ • Natuurrampen • Genocide en oorlogsmisdaad	• Vluchtelingen; migranten; gender/religieuze/etnische minderheden ⁶⁸
Transnationaal religieus geweld ⁶⁹	
Prolifерatie van massavernietigingswapens ⁷⁰ Nucleaire proliferatie ⁷¹	

Relatieve kwetsbaarheid van Nederland

Juist Nederland is bij uitstek kwetsbaar voor de huidige (grensoverschrijdende) veiligheidsdreigingen. Dit komt onder andere omdat Nederland een van de meest geglobaliseerde en geïntegreerde landen in de wereld is.⁷² Dit blijkt uit het feit dat Nederland vrijwel altijd binnen de top drie landen van diverse globaliseringsonderzoeken prijkt.⁷³ Dit betreft zowel hoge scores op de economische en sociale, als de politieke categorieën.⁷⁴ Ook Amsterdam staat op nummer 22 in de top 25 ‘*Global Cities Index*’.⁷⁵ Bij de categorie ‘*Global Cities Outlook*’, die evalueert welke steden de meest prominente in de wereld zullen worden, staat Amsterdam op de zestiende plaats.⁷⁶

63 Ibid.

64 Jovanovic et al., (2016).

65 McQuaid et al., (2017), p. 7.

66 Drent, M. et al., (2015).

67 McQuaid et al., (2017), p. 8.

68 Ibid.

69 Jovanovic et al., (2016). Transnationaal religieus geweld wordt hier gezien als door religie geïnspireerd geweld dat zich over meerdere landen uitstrekt.

70 Renard, T. (2016), p. 11.

71 Ibid.

72 DHL, *DHL Global Connectedness Index 2018: The State of Globalization in a Fragile World*, p. 4; J. Weiß, A. Sachs, H. Weinelt, (2018), *2018 Globalization Report. Who Benefits Most from Globalization?* (Bertelsmann Stiftung), p. 47.

73 Weiß, et al., *2018 Globalization Report; DHL Global Connectedness Index 2018: The State of Globalization in a Fragile World; KOF Globalisation Index*, 2016.

74 Kleinere en sterk ontwikkelde economieën horen bij de meest geglobaliseerde netwerklanden; Nederland zit in de top drie sinds 1990 (MT Globalization Report 2018, p. 12).

75 AT Kearney, (2017), *Global Cities 2017: Leaders in a World of Disruptive Innovation*.

76 Ibid.

Hoe komt het dat Nederland en diens steden hoog op de globaliseringslijsten staan? Dit heeft met name te maken met een aantal economische, culturele en geografische eigenschappen. Zo kent Nederland een hoge mate van connectiviteit, wat betekent dat handel-, kapitaal-, informatie- en mensenstromen vooral internationaal georiënteerd zijn en dat deze stromen in diverse richtingen over de wereld verspreid zijn.⁷⁷ De Nederlandse economie is dan ook een open economie⁷⁸, mede door de interregionale significantie van de haven in Rotterdam (de grootste haven van Europa en plek elf van grootste havens wereldwijd).⁷⁹ Ook Schiphol is hier van belang, gezien het feit dat de luchthaven het derde drukbezochteste vliegveld van Europa is en de nummer elf wereldwijd.⁸⁰ De hub-functie en mate van connectiviteit is de basis voor het Nederlands economisch succes, maar tegelijkertijd zorgt het er ook voor dat het land kwetsbaar is voor bepaalde grensoverschrijdende dreigingen.

Doordat Nederland functioneert als doorvoerland (maar ook als productieland of bestemmingsland) is het ontvankelijk voor (internationaal) georganiseerde criminaliteit, ook wel 'transit criminaliteit'⁸¹ genoemd.⁸² Bovendien is het belastingklimaat in Nederland, als vijfde land op de '*International Tax Competitiveness Index*', aantrekkelijk voor internationale bedrijven die wet- en regelgevingen willen omzeilen.⁸³ Ook is Nederland gevoelig voor cyberaanvallen. Vrijwel alles in Nederland is met elkaar verweven door middel van informatie- en communicatietechnologie (ICT), wat de vitale infrastructuur zeer gevoelig maakt voor digitale aanvallen die bovendien een digitaal domino-effect zouden kunnen veroorzaken. Daarbovenop heeft de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) recentelijk vastgesteld dat de weerbaarheid van overheidsinstellingen en bedrijven nog niet voldoende is.⁸⁴ Recente voorbeelden zijn storingen bij luchthaven Schiphol en bij telecomaandbieder Tele2 in augustus 2018.

77 DHL Global Connectedness Index 2018: *The State of Globalization in a Fragile World*, p. 8-9.

78 Openheid: export plus import als percentage van het BBP.

79 Weiß, et al., 2018 *Globalization Report*, p. 12; Zie: <http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports>.

80 Rapport World Air Traffic, Zie: <https://aci.aero/news/2018/09/20/aci-world-publishes-annual-world-airport-traffic-report>/<https://aci.aero/news/2019/03/13/preliminary-world-airport-traffic-rankings-released/>.

81 Dit betreft meestal de smokkel van mensen en verboden waar, zoals drugs, wapens en gestolen auto's, en illegale grensoverschrijdende handelingen, zoals ondergronds bankieren en het ontduiken van heffingen en accijnzen.

82 E.W. Kruisbergen, H.G. van de Bunt & E.R. Kleemans, (2012), 306 Onderzoek en beleid Georganiseerde criminaliteit in Nederland Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC). ; <https://www.nrc.nl/nieuws/2019/05/26/nederland-is-nu-transitland-voor-mensensmokkel-a3961645>.

83 https://files.taxfoundation.org/20190213134207/ITCI_2018.pdf.

84 NCTV, (2019), <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/12/tk-bijlage-cybersecuritybeeld-nederland-csbn-2019>.

Dergelijke aanvallen kunnen onderdeel uitmaken van ongewenste buitenlandse inmenging en ondermijning.⁸⁵ Dit kan zich concreet voltrekken door middel van bijvoorbeeld verspreiding van desinformatie door statelijke actoren, acties van internationale hackerscollectieven, digitale spionage en sabotage, met als doel om de Nederlandse samenleving te destabiliseren en de eigen invloedssfeer uit te breiden. Naast het digitale domein is Nederland ook vatbaar voor destabilisering via de beïnvloeding van migrantengemeenschappen. Zulke inmenging kan onder andere de vorm aannemen van ongewenste buitenlandse financiering van religieuze instellingen en gebedshuizen.⁸⁶ Hiermee samenhangend bestaat er het risico van een terroristische dreiging door uit IS-gebied teruggekeerde uitreizigers. Naast de concrete terroristische dreiging, kunnen terugkerende uitreizigers zorgen voor een radicaliserend effect onder kwetsbare jongeren. Dit kan voorts weer leiden tot gewelddadig extremisme, versterking van criminele netwerken en transnationale georganiseerde misdaad.⁸⁷

Het is duidelijk dat Nederland niet alleen vatbaar is voor een groot aantal grensoverschrijdende dreigingen, maar dat deze ook met elkaar zijn verweven. Dit betekent dat de aard van onze samenleving, economie, geografie en mate van digitalisering zorgen voor push en pull factoren voor dreigingen. Deze dreigingen kunnen elkaar bovendien versterken, veroorzaken, aanjagen en anderszins beïnvloeden.

Transportbanden tussen interne en externe veiligheid

Voor een beter begrip van de relatieve kwetsbaarheid van Nederland kan de metafoor van een transportband nuttig zijn. Auteurs van een Clingendaelstudie uit 2016 naar de mate waarin het werkveld van de politie verandert vanwege de interne en externe veiligheidsnexus, hebben een vereenvoudigd theoretisch ordeningskader ontwikkeld, dat vier typen connecties onderscheidt die zich tussen interne en externe veiligheidsproblemen kunnen voordoen: logistieke, sociale, digitale en culturele connecties (of 'transportbanden'). Voor elk van de typen zijn één of twee hypothesen geformuleerd over de werking van de connectie, zie hiervoor onderstaande tabel 3.⁸⁸

85 GBVS, 2018, p. 20.

86 GBVS, 2018, p. 20.

87 GBVS, 2018, p. 19.

88 F. van der Laan et al., (2016), *Het Grenzeloze Werkveld van de Politie. Externe Veiligheidsontwikkelingen en hun Implicaties voor Internationale Samenwerking*, Clingendael Rapport, p. 9, via: https://www.clingendael.org/sites/default/files/pdfs/het_grenzeloze_werkveld_van_de_politie.pdf.

Tabel 3 Theoretisch ordeningskader type connecties interne-externe veiligheidsproblemen

Connecties interne/externe veiligheid	Omschrijving	Hypotheses
Logistieke connecties	Irreguliere of illegale goederen of personen verplaatsen zich van A naar B	Criminele handel lift mee met reguliere goederenstromen, verkeer van personen of financiële stromen
Sociale connecties	Criminele actoren, terroristen, faciliteerders of (potentiële) slachtoffers uit verschillende landen kennen elkaar	Reis- en migratiebewegingen en aanwezigheid etnische minderheden faciliteren de organisatie van criminaliteit en terrorisme
Digitale connecties	Digitale verbondenheid versterkt logistieke, sociale of culturele connecties, brengt vraag en aanbod van illegale goederen of diensten samen en cyberspace biedt gelegenheid voor criminaliteit	Aansluiting op internet en <i>social media</i> versterken sociale connecties die organisatie van criminaliteit en terrorisme kunnen bevorderen <i>Sophisticated digital skills</i> bevorderen <i>high tech cybercrime</i>
Culturele connecties	Grensoverschrijdende culturele verwantschap	Grensoverschrijdende culturele verwantschap tussen groepen kan leiden tot <i>spillover</i> of besmettingseffecten: het kopiëren van gedragingen in de criminele, terroristische of openbare orde-sfeer

Dit ordeningskader is ontwikkeld ten behoeve van de Nationale Politie en is daardoor beperkt tot het gebied van criminaliteit.⁸⁹ Een uitbreiding of aanpassing van het ordeningskader kan echter ook relevant zijn voor het beter inzichtelijk maken welke push en pull factoren voor de nationale en internationale veiligheid van belang zijn. Zo brengen politieke en juridische connecties verantwoordelijkheden en plichten met zich mee, die externe ontwikkelingen naar 'binnen' kunnen halen. Ondanks dat Nederland zich in een geopolitiek relatief rustig hoekje van de wereld bevindt, kunnen humanitaire crises en conflicten migratiestromen en andere spillover-effecten op gang brengen die zich langs de politieke en juridische lijn in Nederland doen gelden. Daarnaast zijn niet alleen digitale connecties van belang, maar ook technologische connecties kunnen onze vitale infrastructuur in gevaar brengen door afhankelijkheid, monopolisering, sabotage of spionage en kunnen een grote impact op onze (economische) veiligheid hebben.

Door beter te begrijpen welke connecties voor Nederland van belang zijn, is er een beter inzicht te verkrijgen in de mate van kwetsbaarheid en daarmee waar de weerbaarheid moet worden versterkt. In het huidige complexe dreigingslandschap, waar dreigingen sector- en grensoverschrijdend zijn, is de invloed die we hebben op deze dreigingen beperkt, waardoor het versterken van weerbaarheid het beste handelingsperspectief is.

89 Zie ook: F. van der Laan & M. Drent, (2017), 'Grip op het grenzeloze werkveld van de politie', in: *Cahier Politiestudies*, 2017, 3(44), p. 15.

Conclusies en suggesties onderzoekskader

Er is relatief weinig aandacht in de academische literatuur voor de term 'nexus interne en externe veiligheid' of synoniemen daarvan. Veel van de literatuur houdt zich bezig met de Europese Unie als veiligheidsactor en de relatie tussen de beschikbare instrumenten van de Unie voor interne en externe veiligheid. Er is duidelijk nog een zoektocht gaande naar de ontwarring en conceptualisering van de verschillende termen en definities die de nieuwe dynamiek van veiligheid in een nieuwe fase van globalisering kan vatten. Veel houvast biedt de huidige literatuur hier niet voor, behalve in het aanreiken van kaders zodat de ontoreikendheid van de kaders kan worden aangetoond. Een nieuwe terminologie en een nieuw veiligheidsparadigma lijkt nodig om de grenzeloosheid van veiligheidsvraagstukken beter te kunnen omschrijven en bevatten. Globalisering is altijd al een moeilijk te definiëren fenomeen geweest, maar duidelijk is dat de relatie tussen globalisering en veiligheid een zeer hechte is. Toch lijkt dit nog niet systematisch onderzocht en is de aard van deze relatie nog onvoldoende in kaart gebracht. Alle parameters wijzen erop dat Nederland een sterk 'geglobaliseerd' land is. Om de weerbaarheid uit te bouwen, is het behulpzaam om inzichtelijk te maken hoe de connectie tussen de Nederlandse samenleving in brede zin en globalisering, effect heeft op onze veiligheid. Dit leidt tot de volgende suggesties voor het onderzoekskader:

- De 'interne en externe **veiligheidsnexus**' is nog een relatieve black box: verder onderzoek is nodig om te bepalen of het zinvol is het narratief van 'binnen' en 'buiten' in relatie tot veiligheid te behouden.
- Kennis vergroten over concept **afschrikking** over het volle spectrum van (statelijke) dreigingen.
- Kennis over '**whole of government**', '**whole of society**' (maatschappijbrede) benaderingen vergroten.
- In de keten **preventie-dreigingen-weerbaarheid**, zijn de preventieve maatregelenkant en de weerbaarheidszijde nog onderontwikkeld en behoeven deze meer conceptualisering (verdergaand dan in termen van capaciteiten), meetbaarheid en een gemeenschappelijk (nationaal en internationaal) begrippenkader.
- Aandacht voor de **subjectiviteit** van dreigingen en de verschillen in percepties tussen de elite en het brede publiek (draagvlakprobleem).
- Digitalisering, robotisering, kunstmatige intelligentie, de *internet of things* en 3D *printing* zullen verder onze wijze van produceren, werken, mobiliteit en consumeren sterk veranderen. Het is daarom belangrijk beter te begrijpen op welke wijze deze **nieuwe fase van globalisering** onze veiligheid in brede zin verder gaat beïnvloeden.
- Verder ontwikkelen van een **ordeningskader** om de belangrijkste connecties tussen interne en externe veiligheid inzichtelijk te maken. Met een dergelijk ordeningskader kan de Nederlandse kwetsbaarheid voor dreigingen die deze connecties met zich meebrengen in kaart worden gebracht zodat de weerbaarheid kan worden versterkt.

2 Grensoverschrijdende dreigingen en dreigingsactoren volgens Nederlandse beleidsdocumenten

Inleiding

In Nederlandse strategiedocumenten en risicoanalyses wordt regelmatig gerefereerd aan grensoverschrijdende dreigingen. Wat zijn de belangrijkste trends in de aard, ernst en omvang van deze grensoverschrijdende dreigingen in deze documenten? En wat zijn de belangrijkste dreigingsactoren? In dit hoofdstuk wordt eerst kort ingegaan op de belangrijkste dreigingen voor de Nederlandse nationale veiligheid en daarna gekeken naar de overzeese gebieden.

Grensoverschrijdende dreigingen in de Nederlandse beleidsdocumenten

Het onderstaande schema geeft een overzicht van de in strategiedocumenten en risicoanalyses genoemde dreigingen voor Nederland en de daarbij horende dreigingsactoren (indien genoemd).⁹⁰ Deze worden verderop in dit hoofdstuk nader uitgewerkt.

90 De volgende documenten zijn daarvoor gebruikt: Horizonscan Nationale Veiligheid 2019 (2019), Nationale Veiligheidsstrategie (2019), GRA (2019), GBVS (2018), Defensienota (2014), Defensienota (2018), Meerjarig perspectief krijgsmacht (2017), HGIS (2019), BHOS (2018), China-notitie (2018), Kamerbrief Tegengaan statelijke dreigingen (2019), Nationale Contraterrorisme strategie 2016-2020 (2016).

Tabel 5 Grensoverschrijdende dreigingen in Nederlandse strategiedocumenten en risicoanalyses

Grensoverschrijdende dreiging	Genoemd in strategie/ dreigingsanalyse	Actoren (indien genoemd)
Instabiliteit nabij Europa	Horizonscan 2019 (2019), NVS (2019), GRA (2019), HGIS (2019), GBVS (2018), Defensienota (2018), BHOS (2018), Nationale CT- strategie (2016), Defensie-nota (2014)	Libië, Jemen, Syrië
Grensoverschrijdende criminaliteit	NVS (2019), GRA (2019), HGIS (2019), GBVS (2018)	Criminele bendes
Terrorisme en extremisme	Horizonscan 2019 (2019), NVS (2019), GRA (2019), HGIS (2019), GBVS (2018), Horizonscan 2018 (2018), Meerjarig perspectief krijgsmacht (2017), Nationale CT- strategie (2016)	Terroristische groeperingen als ISIS, Al-Qaida, terugkeerders
Ongewenste buitenlandse inmenging en ondermijning	Horizonscan 2019 (2019), NVS (2019), GRA (2019), Kamerbrief Tegengaan statelijke dreigingen (2019), HGIS-nota, (2019), GBVS, (2018), Meerjarig perspectief krijgsmacht (2017)	Statelijke actoren (o.a. Rusland); Internationale hackerscollectieven; criminelen
Digitale en cyber-dreigingen	Horizonscan 2019 (2019), NVS (2019), GRA (2019), HGIS (2019), China-notitie (2019), Kamerbrief Tegengaan statelijke dreigingen (2019), GBVS, (2018), Horizonscan 2018 (2018), Meerjarig perspectief krijgsmacht (2017),	Statelijke actoren (Rusland, China)
Militaire dreigingen	Horizonscan 2019 (2019), NVS (2019), China-notitie (2019), HGIS (2019), GBVS (2018), Defensienota's (2014, 2018), Meerjarig perspectief krijgsmacht (2017)	Met name Rusland, maar er wordt ook verwezen naar toenemende spanningen Zuidoost-Azië (China-VS, China-Japan)
Bedreiging van vitale economische processen/handel	Horizonscan 2019 (2019), NVS (2019), GRA (2019), China-notitie (2019), Kamerbrief Tegengaan statelijke dreigingen (2019), GBVS (2018), Horizonscan 2018 (2018), BHOS (2018), Meerjarig perspectief krijgsmacht (2017), Defensie-nota (2014)	Statelijke actoren (China specifiek genoemd); piraten
Technologische ontwikkelingen	Horizonscan 2019 (2019), NVS (2019), GRA (2019), Kamerbrief Tegengaan statelijke dreigingen (2019), China-notitie (2019), Defensienota (2018), Meerjarig perspectief krijgsmacht (2017)	Statelijke actoren; terroristische organisaties; geradicaliseerde individuen
CBRN-proliferatie	NVS (2019), GRA (2019), China-notitie (2019), HGIS (2019), Defensienota, (2018), Horizonscan 2018 (2018), Meerjarig perspectief krijgsmacht (2017)	Statelijke actoren (o.a. Noord-Korea, Rusland, India, China); terroristische groeperingen

Instabiliteit nabij Europa

Meerdere Nederlandse beleidsdocumenten en risicoanalyses wijzen op de toegenomen instabiliteit aan de randen van Europa. Zo wordt in de recent verschenen NVS (2019) en GRA (2019) de verwachting uitgesproken dat de fragiliteit in de wijde ring rondom Europa de komende 5-10 jaar verder zal toenemen: met name in West-Afrika, de Sahel, de Hoorn van Afrika, het Midden-Oosten en Noord-Afrika. Landen als Mali, Afghanistan, Libië, Syrië en Irak zijn de laatste jaren door oorlogen en geweld onveiliger geworden. Direct grenzend aan Europa is de fragiliteit van o.a. Oekraïne en Bosnië-Herzegovina toegenomen.

Conflict, terreur, klimaatverandering, armoede, grensoverschrijdende criminaliteit, bevolkingsgroei en irreguliere migratie zijn nauw met elkaar verbonden problemen. Deze problemen hebben in eerste instantie grote gevolgen voor de bevolking aldaar. Of een land te maken krijgt met conflict en fragiliteit, bepaalt in hoge mate het ontwikkelingsperspectief. De BHOS-nota (2018) spreekt de verwachting uit dat in 2030 80% van de extreem armen in landen leven die te stellen hebben met conflict of fragiliteit. Deze fragiliteit en instabiliteit kunnen directe *spillover* effecten hebben op de Nederlandse nationale veiligheid: de verwevenheid van 'interne' en 'externe' veiligheid is hier duidelijk zichtbaar. Fragiele landen kunnen een toevluchtsoord vormen voor extremistische en terroristische groeperingen, en kunnen grensoverschrijdende criminaliteit als mensen- en drugsmokkel faciliteren. Omringende landen kunnen worden meegezogen in deze neerwaartse spiraal. Bovendien brengt deze problematiek vaak vluchtelingen- en (illegale) migratiestromen op de been, wat kan zorgen voor humanitaire en veiligheidsproblemen aan de grens. Tot slot kan het vluchtelingen- en migratievraagstuk zorgen voor politieke en sociaal-maatschappelijke spanningen in Nederland.

Grensoverschrijdende criminaliteit

Instabiliteit rondom Europa wordt vaak direct in verband gebracht met de dreiging van grensoverschrijdende criminaliteit, bijvoorbeeld illegale handel en smokkel van mensen, drugs en goederen. Één van de doelen die wordt benoemd in de GBVS (2019) is de aanpak van internationale (georganiseerde) criminaliteit. Door de verwevenheid van interne en externe veiligheid is deze criminaliteit in toenemende mate een dreiging voor de nationale veiligheid. Behalve de illegale smokkel van mensen, drugs en goederen, gaat het bijvoorbeeld ook om cybercrime en financieel-economische criminaliteit. Deze laatste twee dreigingen worden ook behandeld in (themaportages van) de GRA (2019), die ten grondslag lag aan de Nationale Veiligheidsstrategie 2019.

Terrorisme en extremisme

De Nationale CT-strategie (2016) van de NCTV besteedt uitgebreid aandacht aan de dreiging die uitgaat van terrorisme. Terroristische dreigingen in Nederland komen bijna volledig voort uit jihadisme. Hoewel de kanttekening wordt geplaatst dat de dreiging sterk fluctueert en zich moeilijk laat voorspellen, wordt de verwachting uitgesproken dat de dreiging van jihadisme de komende jaren verder toeneemt, in verschillende uitingsvormen: transnationale netwerken, terugkeerders, (potentieel) gewelddadige eenlingen en snelle radicalisering (bijv. van huidige gedetineerde jihadisten). Volgens de NCTV wordt de dreiging ook steeds meer grensoverschrijdend, waarbij ontwikkelingen in het buitenland steeds directer worden gevoeld in Nederland (en andersom). Ook volgens de GBVS (2018) en de verschillende publicaties van Defensie blijft terrorisme een constante zorg: met name religieus geïnspireerd terrorisme zal de komende jaren een van de belangrijkste dreigingen blijven. Terroristische groeperingen als ISIS en Al-Qaida zullen gebruik blijven maken van wetteloosheid in instabiele landen. Nederland moet daarbij vooral rekening houden met de dreiging van terugkeerders. De Horizonscan 2018 wijst in dit verband op vrouwen als een aparte risicocategorie. Zij vormen de grootste groep van recente terugkeerders, en worden steeds vaker ingezet voor het voorbereiden en uitvoeren van terroristische aanslagen. Tot slot waarschuwen deze strategiedocumenten voor het radicaliserende effect van terugkeerders op kwetsbare jongeren binnen en buiten Europa.

In de Nationale CT-strategie (2016), de NVS (2019) en de GRA (2019) wordt ook aandacht besteed aan andere vormen van terrorisme en extremisme, in het bijzonder aan rechtsextremisme. De angst voor immigranten en de Islam heeft bijgedragen aan de groei van extreemrechts, waar ook een terroristische dreiging van uitgaat. Bovendien is in reactie hierop extreemlinks in Nederland weer actiever geworden. De NVS (2019) en de GRA (2019) signaleren nieuwe fenomenen zoals 'identitair extremisme', wat wellicht de klassieke tegenstelling tussen rechts- en links overstijgt.

Ongewenste buitenlandse inmenging, ondermijning democratische rechtstaat, hybride operaties

In de risicoanalyses en strategiedocumenten worden verschillende termen gehanteerd die verwijzen naar ondermijnende dreigingen van statelijke en niet-statale actoren: 'ongewenste buitenlandse inmenging' (OBI), ondermijning, hybride conflictvoering, etc. De GBVS (2018) waarschuwt bijvoorbeeld voor het ondermijnende effect van desinformatiecampagnes door statelijke actoren, acties van internationale hackerscollectieven, digitale spionage en sabotage (met daarbij cyber als middel), beïnvloeding van de migrantengemeenschappen in Nederland vanuit nationalistische motieven en onwenselijke buitenlandse financiering van religieuze instellingen en gebedshuizen. De recente Kamerbrief Tegengaan statelijke dreigingen (2019) wijst in het algemeen op de dreiging die uitgaat van ondermijning van statelijke actoren en bespreekt met

name de mogelijke effecten die het kan hebben op de Nederlandse maatschappij. De GRA (2019) en het Meerjarig perspectief krijgsmacht (2017) refereren expliciet naar de dreiging die uitgaat van Rusland, en het instrumentarium dat dit land gebruikt (beïnvloeding van media, cyberaanvallen en propaganda). In de notitie wordt verder ingegaan op het concept 'hybride conflictvoering': staten en niet-statelijke actoren die deze strategie hanteren, orkestreren alle mogelijke "misleidende, ondermijnende en openlijk ontwrichtende activiteiten" om bepaalde strategische of geopolitieke doelstellingen te behalen, maar blijven daarbij onder de drempel van grootschalige militaire escalatie.⁹¹ Hierbij worden alle instrumenten van de staat gebruikt, denk aan desinformatiecampagnes, propaganda, militaire middelen, economische instrumenten, diplomatie, etc. De GRA, maar ook de nieuwe China-notitie (2019), besteedt daarnaast ook aandacht aan ondermijnende activiteiten door China. In de China-notitie wordt gewezen op het risico van 'eenzijdige strategische afhankelijkheden' waarmee Nederland potentieel kwetsbaar wordt voor buitenlandse inmenging vanuit China die maatschappelijke ontwrichting tot gevolg kan hebben.

In hoofdstuk vier van dit rapport wordt nader ingegaan op de verschillende manifestaties van deze dreigingen en de actoren die hierachter schuilgaan, als onderdeel van een casestudy.

Digitale en cyberdreigingen

Het digitale domein wordt steeds vaker gebruikt door tegenstanders. In veel risico-analyse – en strategiedocumenten wordt naar deze dreiging gerefereerd. De GRA bijvoorbeeld besteedt aandacht aan zowel de aantasting van het functioneren van het internet, digitale sabotage, digitale spionage en cybercriminaliteit en werkt daarvoor verschillende scenario's uit. In algemene zin kan worden gesteld dat de digitale dreiging groot is, en dat deze de komende jaren zal groeien vanwege de toenemende digitalisering van de maatschappij. De GRA (2019) en de Kamerbrief Tegengaan statelijke dreigingen (2019) benadrukken de dreiging die uitgaat van statelijke actoren, die het cyberdomein vaak gebruiken als middel voor beïnvloeding of hybride operaties en daarmee de democratische samenleving willen ondermijnen, strategische informatie willen bemachtigen, of vitale systemen trachten te verstoren. Niet alleen het aantal staten dat deze digitale capaciteiten ontwikkelt groeit, maar de aanvallen worden ook complexer. Er wordt daarbij met name verwezen naar de dreiging die uitgaat van Rusland en China. Ook in de China-notitie uit 2019 wordt er verwezen naar de directe invloed van Chinese cybercapaciteiten op de Nederlandse nationale veiligheid.

91 Ministerie van Defensie, (2017), *Houvast in een onzekere wereld – Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gereed en snel inzetbare krijgsmacht*, p. 8.

Militaire dreigingen

O.a. de GRA (2019) en de GBVS (2018) stellen dat de militaire dreigingen tegen ons eigen en het bondgenootschappelijk grondgebied toenemen. Dit is te wijten aan oplopende spanningen tussen grootmachten en doordat landen zich in toenemende mate profileren op het militaire terrein. Belangrijke indicatoren zijn de toegenomen defensie-uitgaven wereldwijd, agressievere retoriek, grootschaligere militaire oefeningen en de vele schendingen van territoriale wateren en het luchtruim. De militaire dreigingen manifesteren zich ook steeds vaker in het hybride spectrum. Het Meerjarig perspectief krijgsmacht uit 2017 expliciteert de dreiging die uitgaat van het destabiliserende optreden van Rusland en stelt dat Rusland een “onvoorspelbare factor” is geworden.⁹² Ook verwijst deze nota naar de toenemende spanningen in Oost- en Zuidoost-Azië (China-VS, China-Japan, Noord-Korea – Zuid-Korea), die mogelijk zouden kunnen escaleren tot een militair conflict. De substantiële investeringen van China in zijn expeditiecapaciteiten stellen China in staat de belangen in die regio's met militaire middelen kracht bij te zetten, wat volgens de China-notitie potentieel gevolgen kan hebben voor bijvoorbeeld de internationale handel over zee.

Bedreiging van vitale economische processen

De GBVS vraagt aandacht voor dreigingen die vitale economische processen kunnen raken, denk aan cyberspionage of de verstoring van fysieke en digitale aanvoerroutes door bijvoorbeeld piraterij of cyberaanvallen. Daarnaast gaat het om het veiligstellen van grondstoffen en het borgen van de nationale veiligheid in het kader van investeringen. In de Geïntegreerde Risico Analyse (GRA) zijn meerdere scenario's uitgewerkt waarin de knooppuntfunctie van Nederland centraal staat, bijvoorbeeld een scenario waarin militaire spanningen op de Zuid-Chinese zee escaleren en de vrije doorvaart belemmeren. De BHOS (2018) waarschuwt voor de verharding van economische verhoudingen en het toenemende protectionisme: internationale samenwerking op dit terrein staat ernstig onder druk. In de GRA (2019) is om die reden een scenario uitgewerkt over de potentiële effecten van een handelsoorlog.

Bovendien roept de economische verwevenheid met staatsgeleide economieën zoals China en Rusland ook vragen op over onze economische veiligheid. In de onlangs verschenen China-notitie (2019) worden bijvoorbeeld vraagtekens gezet bij de geopolitieke motieven van China als het gaat om investeringen in de fysieke infrastructuur en de hightechsector in andere landen. Ook wordt er gewezen op de risico's van eenzijdige strategische belangen, bijvoorbeeld als het gaat om zeldzame aardmetalen of sleuteltechnologieën.

92 Ministerie van Defensie, (2017), *Houvast in een onzekere wereld – Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gereed en snel inzetbare krijgsmacht*, p. 7.

CBRN-dreiging

Onder meer de GRA (2019) en de GBVS (2018) signaleren dat de dreiging van de proliferatie van massavernietigingswapens toeneemt. Nucleaire wapenarsenalen worden wereldwijd uitgebreid (o.a. door Noord-Korea, China, Pakistan en India) en gemoderniseerd (o.a. door Rusland, VK en VS). In de China-notitie (2019) wordt expliciet aandacht besteed aan de modernisering en uitbreiding van de Chinese nucleaire capaciteit, die – hoewel het land zegt deze uitsluitend voor zelfverdediging te gebruiken – potentieel ook de internationale vrede en veiligheid kan bedreigen. In de overige strategiedocumenten wordt overigens niet alleen gewezen op het gevaar van statelijke actoren, maar ook op de groeiende kennis en capaciteiten van terroristische groeperingen. Extra zorgwekkend is dat het nucleaire wapenbeheersingsregime onder druk staat en doctrines voor het gebruik van nucleaire wapens in conflicten aan het veranderen zijn. Zowel Rusland als de VS hebben de drempel voor de inzet van nucleaire wapens verlaagd.

Technologische dreigingen

Technologie wordt steeds geavanceerder, goedkoper en is beschikbaar voor steeds meer actoren. Dit biedt kansen, maar kan ook veiligheidsrisico's met zich meebrengen als deze technologie in de verkeerde handen valt. Het Meerjarig perspectief krijgsmacht (2017) en de Defensienota (2018) besteden expliciet aandacht aan de dreiging van nieuwe technologieën wanneer die worden ingezet voor oorlogsvoering: kunstmatige intelligentie (KI), *big data* analyse, kwantumcomputers, robotica, onbemande voertuigen, biotechnologie, nano- en kwantumtechnologie en *3D printing*. Door deze technologische ontwikkelingen nemen de mogelijkheden voor hybride conflictvoering toe.

Technologie is bovendien onderdeel van de competitie om de wereldmacht, zo stelt de China-notitie (2019). China heeft de ambitie uitgesproken een technologische supermacht te worden en op veel terreinen (denk aan 5G, KI, robotica, batterij-technologie, nano- en kwantumtechnologie, *3D printing*) in 2025 marktleider te willen zijn.

Caribische delen van het Koninkrijk (Aruba, Curaçao, Sint-Maarten en de BES-eilanden)

De overzeese gebieden hebben te maken met een ander dreigingspalet. Er bestaat (nog) geen aparte dreigingsanalyse voor het Caribisch deel van het Koninkrijk, maar daar wordt binnen het Analisten Netwerk Veiligheid (ANV) wel naar toegewerkt. In de verschillende risicoanalyse- en strategiedocumenten wordt er hier en daar verwezen naar specifieke grensoverschrijdende dreigingen waarmee de overzeese gebieden te maken hebben (zie tabel 6). In de GRA en de HGIS-nota bijvoorbeeld, wordt aandacht

gevraagd voor de instabiliteit in de regio, meer specifiek voor de directe gevolgen die de politieke en economische situatie in Venezuela kunnen hebben voor het Caribisch deel van het Koninkrijk. De verslechterde humanitaire en economische omstandigheden hebben migratiestromen veroorzaakt. Deze migratiestromen worden op grote schaal uitgebuit door georganiseerde bendes (mensensmokkel, drugssmokkel, etc.).

Tabel 6 Grensoverschrijdende dreigingen in Nederlandse strategiedocumenten en risicoanalyses met betrekking tot de Caribische delen van het Koninkrijk

Grensoverschrijdende dreiging	Genoemd in strategie/ risicoanalyse	Dreigingsactor (als genoemd)
Instabiliteit nabij de Caribische delen van het Koninkrijk	GBVS (2018), HGIS (2019), Defensienota (2018)	Staatelijke actoren (met name Venezuela, maar ook bijv. Colombia)
Georganiseerde criminaliteit	Veiligheidsbeeld BES (2018), GBVS (2018)	Transnationale georganiseerde groeperingen (uit verschillende delen van de wereld: Venezuela, Colombia, Nederland, Caribisch deel van het Koninkrijk, China), denk aan: Barrio 18, MS 13, de Familia Michacana, Juarez Cartel, Jalisco Cartel New Generation, Sinaloa Cartel, maar ook aan motorbendes
Illegale migratie	Veiligheidsbeeld BES (2018)	Illegale migranten uit met name Zuid- en Centraal-Amerika
Piraterij	Veiligheidsbeeld BES (2018)	Piraten
Bedreiging van vitale economische processen (investerings/ <i>debt trap</i>) ⁹³	China-notitie (2019)	Staatelijke actor (China)

In het Veiligheidsbeeld BES worden de verschillende verschijningsvormen van georganiseerde criminaliteit waar de eilanden mee kampen toegelicht. Het stelt dat de “ aantrekkelijkheid van het gebied voor georganiseerde criminele groeperingen onverminderd groot is”. Er zou sprake zijn van een “*trafficking revival*”, met name in drugs. Daarbij is aantal georganiseerde groeperingen, maar ook hun omvang en macht toegenomen.⁹⁴ Deze groeperingen zijn vaak internationaal georganiseerd en hebben cellen in meerdere landen en op meerdere continenten. De schaal waarop deze groeperingen opereren is ongekend groot en de winsten zijn enorm. Naast

93 Een *debt trap* is een politiek instrument van een staatelijke actor om geld te lenen aan een andere staat die dit onmogelijk terug kan betalen, zodat de schuldeiser later de schuld kan innen met als doel politieke en/of economische invloed uit te oefenen.

94 Veiligheidsbeeld BES, 2018, p. 22.

georganiseerde criminaliteit, hebben de eilanden te stellen met 'organisatiecriminaliteit' (witwassen, fraude, etc.) en grootschalige corruptie. Bovendien zouden ook piraterij en maritieme criminaliteit weer terug zijn in het Caribisch gebied.⁹⁵ Tot slot kampen de overzeese gebieden met illegale migratie. Niet alleen de stromen uit Venezuela zijn zeer zorgwekkend; migranten komen ook uit andere landen in de regio (Peru, Colombia, Dominicaanse Republiek). Deze groep is kwetsbaar voor arbeidsuitbuiting, criminaliteit en illegale prostitutie.

In de China-notitie (2019) wordt melding gemaakt van de groeiende belangstelling van het land voor de Caribische delen van het Koninkrijk. Deze belangstelling is zowel politiek als economisch gemotiveerd. Het toenemende aantal Chinese investeringen wordt gezien als een risico: omdat de eilandstaten een relatief kleine economie hebben, kunnen zelfs bescheiden investeringen al een grote impact hebben en snel(ler) leiden tot hoge schulden.

Conclusies

In dit hoofdstuk is een overzicht gegeven van de belangrijkste grensoverschrijdende dreigingen die genoemd worden in Nederlandse risicoanalyses, beleidsnota's en strategieën. In de meeste gevallen wordt uitgegaan van de dreiging, en niet van (specifieke) dreigingsactoren. De recent verschenen Kamerbrief *Tegengaan statelijke dreigingen* uit april 2019 is hierop een belangrijke uitzondering. Hierin worden, zonder expliciet bepaalde staten te noemen, de dreigingen en risico's benoemd die uitgaan van statelijke actoren en die potentieel een ondermijnend effect kunnen hebben op de rechtstaat en op de openheid en stabiliteit van de Nederlandse samenleving. Denk hierbij aan: digitale dreigingen, economische dreigingen, ongewenste buitenlandse beïnvloeding en afhankelijkheid van nieuwe technologieën. Ook in andere risicoanalyses (bijvoorbeeld de GRA en het *Meerjarig perspectief krijgsmacht*) is er een verandering zichtbaar, in de zin dat de dreigingsactor vaker expliciet wordt benoemd. In deze documenten wordt bijvoorbeeld verwezen naar Rusland of China als dreigingsactor. Dit is echter wel iets anders dan een (volledige) actoranalyse, omdat hier niet naar de actor in zijn geheel wordt gekeken, met de daarbij behorende capaciteiten, intenties en gelegenheid.

Ditzelfde geldt ook voor de risicoanalyses voor de overzeese gebieden, waarin met name de dreigingen worden benoemd. Als er al een actor wordt benoemd (bijv. Venezuela), dan wordt niet naar het volle palet aan dreigingen gekeken dat van deze actor uitgaat. Het is tot slot belangrijk om te melden dat er geen complete risicoanalyse voor het

95 Veiligheidsbeeld BES, 2018, p. 23.

Caribisch gedeelte van het Koninkrijk bestaat, terwijl deze gebieden te stellen hebben met een heel ander palet aan grensoverschrijdende dreigingen dan het Europese deel.

Dit geeft het volgende element ten behoeve van het onderzoekskader, verdere elementen volgen na de toetsing van de gecombineerde actor-dreigingsanalyse in Hoofdstuk 4:

- Aanvullen van een, nu ontbrekende, actor- en dreigingsanalyse voor het **Caribisch deel van het Koninkrijk**.

3 Onderzoeksbenaderingen risicoanalyses nationale veiligheid

Inleiding

Nederland kent een ministeriële autonomie en zelfs een in de wet vastgelegde opdracht (bijvoorbeeld voor het ministerie van Defensie) om periodiek beleidsnota's of strategieën te schrijven ten behoeve van het stellen en prioriteren van doelen voor het alloceren van middelen. Er is een duidelijke tendens om steeds nauwer interdepartementaal samen te werken in de aanloop naar departementale nota's en strategieën. Na de Geïntegreerde Buitenland en Veiligheidsstrategie (GBVS) van het ministerie van Buitenlandse Zaken en de Defensienota van het ministerie van Defensie in 2018, verscheen in 2019 een kabinetsbrede Nationale Veiligheid Strategie.⁹⁶ Het ministerie van Justitie en Veiligheid herbergt de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), een orgaan dat coördinerend moet optreden op het terrein van terrorismebestrijding en veiligheid in het algemeen. De NCTV is daarom penvoerder voor deze Nationale Veiligheid Strategie en stuurt namens de kabinetsbrede Stuurgroep Nationale Veiligheid (SNV)⁹⁷ de onderliggende risicoanalyses aan.

In dit hoofdstuk wordt kort de Nederlandse praktijk van risicoanalyse ten behoeve van nationale veiligheid behandeld. Dit leidt tot een overzicht van het werk van het Analistennetwerk Nationale Veiligheid (ANV), een netwerk waarin Nederland zijn risicoanalyses heeft geborgd namens de Stuurgroep Nationale Veiligheid. Vooral de methode wordt kritisch beschouwd en in internationaal perspectief geplaatst. De dreigings- en gevarenanalyse van het ANV, zo zal blijken, kent een aantal pijnpunten. Een deel hiervan is overigens ook bekend bij het ANV zelf. Dit hoofdstuk zal deze pijnpunten benoemen en een aantal aanvullingen op deze methode suggereren. Deze aanvullingen geven slechts een denkrichting weer voor vervolgonderzoek. Dit hoofdstuk wil vooral aangeven waar nog behoefte aan nader onderzoek bestaat om de strategische cyclus van Nederland op het gebied van nationale veiligheid zo goed mogelijk te voorzien van analytische onderbouwing.

96 *Nationale Veiligheid Strategie 2019.*

97 Voor meer informatie over de Stuurgroep Nationale Veiligheid (SNV), zie: <https://wetten.overheid.nl/BWBR0027277/2010-02-23>.

De Nederlandse praktijk van risicoanalyse naar nationale veiligheid

Sinds 2011 maakt het ANV analyses ten behoeve van de nationale veiligheid. Dat doet zij in opdracht van het ministerie van Justitie en Veiligheid namens de interdepartementale Stuurgroep Nationale Veiligheid. Voorheen werden deze analyses gerapporteerd in de Nationale Risicobeoordeling (NRB), maar in 2016 zijn zij in de vorm van een Nationaal Veiligheidsprofiel (NVP), met onderliggende themarapportages, gepresenteerd. Om tegemoet te komen aan de behoefte om continu risico's en dreigingen te inventariseren in plaats van één keer in de vier jaar, heeft het ANV in 2018 een eerste Horizonscan Nationale Veiligheid uitgevoerd. Deze exercitie, waarbij wordt gescand op actuele en opkomende gevaren en dreigingen aan de hand van vijf brede autonome ontwikkelingen, is in 2019 herhaald en zal ook in 2020 uitgevoerd worden. Ten behoeve van de kabinetsbrede Nationale Veiligheid Strategie die in de zomer van 2019 uit kwam, is begin 2019 een 'Geïntegreerde Risicoanalyse' (GRA) geschreven. De GRA is een uitgebreide analyse van verschillende thema's en risicocategorieën. Daarnaast voert het ANV ook themaverdiepingen uit, waaronder recent bijvoorbeeld op het gebied van hybride dreigingen, een technologieverkenning, de gevolgen van de energietransitie en de perceptie van veiligheidsdreigingen. De Horizonscans en de GRA zijn onderdeel van de nieuwe driejarige strategische cyclus die Nederland wil gaan aanhouden (mede ingegeven door de verplichting vanuit de EU om dit te doen). Dit behelst een Horizonscan in jaar één, nog een Horizonscan in jaar twee, gevolgd door een Geïntegreerde Risicoanalyse en het uitkomen van een nieuwe Nationale Veiligheid Strategie in jaar drie. Nagenoeg continu scannen en de periodieke herhaling van analyses is een goede stap vooruit in het neerzetten van een adequate strategische cyclus. De juiste vorm vinden voor en het doorontwikkelen van de gebruikte analytische producten, de Horizonscans en de GRA, zal echter een voortdurende opgave blijven.

Zowel het Nationaal Veiligheidsprofiel uit 2016 als de GRA uit 2019 geeft een *all hazard* overzicht⁹⁸ van de belangrijkste risico's voor de nationale veiligheid. Het NVP was een vrij grote exercitie waarbij per risicocategorie op diverse dreigingen illustratieve scenario's werden geanalyseerd aan de hand van onderling vergelijkbare impactcriteria op de, toen nog, vijf Nederlandse veiligheidsbelangen. De scenario-exercities werden gedaan in groepen van thema- en methode-experts. De impactscores werden verrekend met de waarschijnlijkheid dat het scenario zich voordoet, leidend tot een totaalscore variërend tussen A en E, waarbij een A-score een beperkte impact betekent en de E-score het ernstigste risico voor de nationale veiligheid betekent (catastrofaal). Voor de GRA uit 2019 werden de risicocategorieën aangevuld op basis van een inventarisatie van beleids- en strategiedocumenten van de Nederlandse overheid, waaronder ook de ANV

98 All hazard: alle risicocategorieën met relevantie voor de nationale veiligheid, dus moedwillige en niet-moedwillige dreigingen (*safety* én *security* categorieën).

Horizonscan Nationale Veiligheid 2018. Bestaande scenario's werden geactualiseerd en er werden nieuwe scenario's geschreven voor de nieuwe risicocategorieën.

Verwevenheid

De bedoeling van de nieuwe Nationale Veiligheid Strategie was dat het een kabinets-brede, geïntegreerde strategie zou worden. De onderliggende analyse zou dit moeten reflecteren. Ondanks de naam *Geïntegreerde* Risicoanalyse is in de methodologie van de GRA nog weinig aandacht aan dit aspect besteed. Er is bij de GRA voortgebouwd op de bestaande methodologie en analyses van het NVP, waarbij extra risicocategorieën zijn toegevoegd. Kort gezegd wordt op basis van scenario's de impact en waarschijnlijkheid van een dreiging geanalyseerd, aangevuld met thematische literatuurstudies. In een apart hoofdstuk wordt in de GRA ingegaan op de dwarsverbanden tussen verschillende risicocategorieën en dreigingen, waarbij niet wordt aangegeven welke methodologie hieraan ten grondslag ligt. Er is niet op systematische wijze gekeken naar de aard van de verbanden tussen verschillende dreigingen, waardoor de verkokering tussen de thema's en risicocategorieën in stand blijft. Het is duidelijk dat met een uitbreiding naar negen dreigingsthema's en 27 risicocategorieën van uiteenlopende *safety* en *security* aard het goed uitvoeren van de scenario's, het bepalen van de impact en waarschijnlijkheid van dreigingen en gevaren in allerlei expertsessies een grote opgave is (zie voor een overzicht tabel 4).

Tabel 4 Overzicht dreigingsthema's en risicocategorieën

Thema	Risicocategorie
1. Bedreigingen voor gezondheid en milieu	1. Infectieziekten humaan
	2. Dierziekten en zoönose
2. Natuurrampen	3. Extreem weer
	4. Overstroming
	5. Natuurbrand
	6. Aardbeving
3. Verstoring vitale infrastructuur	7. Verstoring vitale infrastructuur
4. Zware ongevallen	8. Stralingsongevallen
	9. Chemische incidenten
5. Cyberdreigingen	10. Digitale sabotage
	11. Aantasting internetcapaciteit
	12. Cyberspionage
	13. Cybercriminaliteit
6. Ondernijning democratische rechtsstaat	14. Niet-gewelddadig extremisme
	15. Ondernijnde criminaliteit (enclavevorming)
	16. Ongewenste buitenlandse inmenging
	17. Ongewenste buitenlandse beïnvloeding (via hybride operaties)

Thema	Risicocategorie
7. Extremisme en terrorisme	18. Terrorisme
	19. Extremisme
8. Financieel-economische bedreigingen	20. Criminele inmenging
	21. Bedreigingen van de knooppuntfunctie en de aan- en afvoerlijnen van Nederland (flow security)
	22. Handelskrimp/verstoring internationale handel
	23. Destabilisatie financieel systeem
9. Bedreigingen internationale vrede en veiligheid	24. Instabiliteit rondom EU
	25. Militaire dreigingen (NAVO-lidstaat)
	26. CBRN-proliferatie
	27. Veiligheidsarrangementen onder druk (NAVO, EU)

Op welke wijze recht kan worden gedaan aan de verwevenheid van de verschillende thema's vereist een nadere bezinning op de juiste methode hiervoor. In de Horizonscan Nationale Veiligheid 2019 is geprobeerd beter grip te krijgen op de verwevenheid van dreigingen in een multidisciplinaire expertsessie. De bedoeling was om de in de diverse scans opgehaalde belangrijkste dreigingen uit de afgebakende silo's van de thema's (of in dit geval: de autonome ontwikkelingen) te halen.⁹⁹ Er is op dit terrein nauwelijks of geen beschikbare literatuur of een op de plank liggende methodologie. In hoeverre in andere landen op het terrein van analyse van sectoroverstijgende en grensoverschrijdende gevaren en dreigingen ervaring is opgedaan, zou verder onderzocht moeten worden. Op dit moment probeert het ANV zelf het wiel uit te vinden.¹⁰⁰

De overgang naar een strategische cyclus stelt het ANV en de aangesloten organisaties beter in staat om menskracht beschikbaar te hebben om een verdere verdiepingsslag en professionalisering van de analyses mogelijk te maken.

99 Het ANV onderscheidt vijf 'autonome ontwikkelingen': internationale politieke, internationale economische, ecologische, demografisch-maatschappelijke en technologische. Zie: Margriet Drent en Minke Meijnders (red.), *Horizonscan Nationale Veiligheid 2018*, Analistennetwerk Nationale Veiligheid, Den Haag, 2018 p. 9.

100 Bijvoorbeeld door te proberen om 'MARVEL (Method to Analyse Relations between Variables using Enriched Loops) modelling' toe te passen, zie: https://www.tno.nl/media/9516/def_alg_paper_marvel_sds_2007.pdf.

Updaten methode

Het ANV is transparant over de gevolgde methode middels het publiceren en updaten van de zogenaamde ‘Leidraad’.¹⁰¹ De snel veranderende veiligheidssituatie vereist dat deze Leidraad een levend document is. Het is onder meer in 2019 aangepast (publicatie volgt nog). Er zijn in deze nieuwe versie twee extra impactcriteria uitgewerkt voor het vitale belang ‘territoriale integriteit’, namelijk ‘digitale ruimte’ en ‘integriteit van het bondgenootschappelijk grondgebied’. Aantasting van de integriteit van de digitale ruimte gaat over het verlies van functioneren van en/of zeggenschap over de digitale ruimte, doordat beschikbaarheid, vertrouwelijkheid en integriteit van essentiële informatiesystemen wordt aangetast. Digitale ruimte is hierbij gedefinieerd als: ‘het conglomeraat van ICT-middelen en diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn’. De integriteit van het bondgenootschappelijk grondgebied betreft het niet toegankelijk zijn van, dan wel het verlies van zeggenschap over, (delen van) het grondgebied van lidstaten van de EU en NAVO (bondgenoten), inclusief het luchtruim, territoriale wateren en de digitale ruimte.

Daarnaast is besloten om een zesde vitaal belang aan de vijf bestaande toe te voegen (zie figuur 1 voor een overzicht van de zes vitale belangen). De opgave uit de Nederlandse grondwet om de internationale rechtsorde te bevorderen en de erkenning dat deze rechtsorde van wezenlijk belang is voor de Nederlandse veiligheid in brede zin, heeft geleid tot het toevoegen van dit zogenaamde ‘zesde belang’. De definitie hiervan is “het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid.” Deze definitie is uitgewerkt in een notitie.¹⁰² Voor het prioriteren van dreigingen die zich buiten de landsgrenzen afspelen, maar niet scoorden op impactcriteria van de andere, meer nationaal georiënteerde vitale belangen, is deze toevoeging van belang. Ook komt met dit extra belang de nexus van interne en externe veiligheid beter tot uitdrukking.¹⁰³ De grenzen van dit zesde belang waren onderdeel van de discussie in aanloop naar de acceptatie ervan door de Stuurgroep Nationale Veiligheid. Onderdeel van dit debat is dat de internationale rechtsorde een ander karakter heeft dan de overige vijf veiligheidsbelangen, namelijk dat deze op één of andere wijze meer te maken hebben met het Nederlandse grondgebied. Een gezichtspunt in dit debat is ook dat de internationale rechtsorde meer instrumenteel van aard is voor het bereiken van de Nederlandse belangen. In bijlage 1 zijn de impactcriteria van ‘internationale rechtsorde’ op onze nationale veiligheid uitgewerkt, waardoor de brede definitie van

101 Ministerie van Justitie en Veiligheid, (2013), Analistennetwerk Nationale Veiligheid (2019), *Leidraad Risicobeoordeling. Geïntegreerde Risicoanalyse Nationale Veiligheid*, ANV-methode.

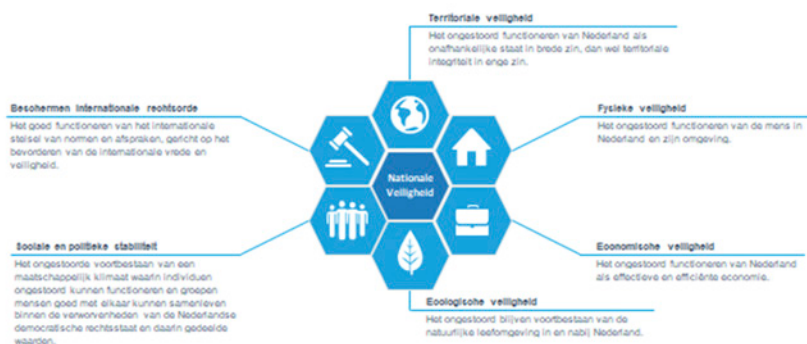
102 M. Drent & M. Meijnders, (2019), *De Internationale Rechtsorde als zesde nationaal veiligheidsbelang*, Analistennetwerk Nationale Veiligheid, (op te vragen bij het RIVM).

103 Zie ook: K. de Bruijne, (2018), ‘Vitale Belangen’, *Clingendael Policy Brief*, (Den Haag: Instituut Clingendael).

het belang verder wordt gepreciseerd. Deze precisering en scoringscriteria maakt het mogelijk om de impact van scenario's op de 'internationale rechtsorde' door experts vrij nauwkeurig te scoren. Zo wordt bij impactcriterium 1 'aantasting van staatssoevereiniteit (...)' onderscheid gemaakt tussen (A) blokkades, inperken van gezag van soevereine staat, (B) geweldsconflicten zonder grensoverschrijding, (C) geweldsconflicten met grensoverschrijdingen, (D) gebruik van massavernietigingswapens, inperken essentiële onderdelen van de staatssoevereiniteit en (E) permanente bezetting of gebruik van massavernietigingswapens door meerdere staten (zie bijlage 1).

De scoring op vier verschillende impactcriteria wordt vervolgens samengevoegd met de scoring op de andere vijf vitale belangen. Zo weegt de mate van aantasting van de internationale rechtsorde mee in de inschatting in welke mate onze nationale veiligheid wordt bedreigd. Dit betekent in de praktijk dat bijvoorbeeld de burgeroorlog in Libië naast een lage score op de internationale rechtsorde, ook op een ander vitaal belang scoort (zie hieronder) als het (om wat te noemen) gevolgen heeft voor de sociale en politieke stabiliteit door vluchtelingenstromen. Zo weegt voor de Nederlandse veiligheidsanalyses vanaf 2019 de internationale rechtsorde wel mee en wordt het gewogen in samenhang met onze vijf andere belangen. De discussie in hoeverre het voor Nederland terecht en verstandig is dat dit als vitaal belang wordt bestempeld, wat precies onderdeel is van dit belang (in hoeverre bijvoorbeeld mensenrechten worden meegewogen of het internationaal-financieel economisch stelsel er ook deel van uitmaakt) woedt nog steeds. Verdere meningsvorming hierover zou gebaat zijn bij nader onderzoek.

Figuur 1 Overzicht van de zes vitale belangen voor de nationale veiligheid



Internationale reflectie op methoden

Het ANV maakt gebruik van een methodiek voor het Nationaal Veiligheidsprofiel en de Geïntegreerde Risicoanalyse die vergelijkbaar is met de methodes van bijvoorbeeld het *Department of Homeland Security* in de Verenigde Staten of de *National Security Council* in het Verenigd Koninkrijk. De *UK National Security Risk Assessment* (NSRA) werd in 2010 geïntroduceerd in samenhang met de hervormingen die in dat jaar werden doorgevoerd, resulterend, onder meer, in een *National Security Council* en een vijfjaarlijkse *National Security Strategy* en een *Strategic Defence and Security Review* (in 2010 en 2015). De NSRA was bedoeld om deze strategieën te voorzien van een robuuste en onderbouwde prioritering van de Britse nationale veiligheidsdreigingen op basis van een samengestelde berekening van waarschijnlijkheid en impact. Dit levert een prioritering op in drie categorieën, waarvan de eerste categorie urgent is en directe actie vereist.¹⁰⁴ De NSRA werkt met twee tijdshorizonnen, namelijk één van vijf en één van twintig jaar, wat de Britten in staat stelt om korte termijndreigingen en middellange termijnontwikkelingen in hun analyse mee te nemen.

Het *Department of Homeland Security* van de Verenigde Staten kent de '*Homeland Security National Risk Characterization*' (HSNRC), dit is ook een *all hazard* risico-beoordeling. De HSNRC lag in zowel 2010 als 2014 onder vuur van de Amerikaanse Algemene Rekenkamer (de *Government Accounting Office*, GAO). Deze concludeerde dat de methode onvoldoende was gedocumenteerd om de resultaten voldoende reproduceerbaar te maken en ze te kunnen verantwoorden. *Homeland Security* vroeg in 2016 aan de RAND Corporation om een methodologie voor een risicoanalyse te ontwikkelen en deze risicoanalyse in 2018 vervolgens ook op te leveren. In de voorgestelde selectieprocedure van de dreigingen en gevaren valt op, dat deze ook moeten voldoen aan het criterium van 'operationeel relevant', in de zin dat *Homeland Security* moet kunnen bijdragen aan risicoreductie.¹⁰⁵ De dreigingen gerelateerd aan terrorisme, cyber en illegale handelingen worden meegenomen, maar de dreigingen uit het traditionele internationale domein vallen onder de strategieën van het Witte Huis, het Pentagon en het *State Department*. De in de HSNRC gebruikte methode van impact x waarschijnlijkheid verschilt niet wezenlijk van die gebruikt door Nederland.

104 De volledige NSRA is gerubriceerd en wordt niet gepubliceerd, wel een factsheet: *National Security and Risk Assessment*, Factsheet, 2015.

105 H. H. Willis et al., (2018), *Homeland Security National Risk Categorization. Risk Assessment Methodology*, (Santa Monica: RAND Corporation).

De door Nederland gehanteerde methode wijkt dus niet veel af van die van de twee risicoanalyses die we hier hebben bekeken.¹⁰⁶ Een meer systematische inventarisatie van de verschillende praktijken in meerdere landen zou zinvol zijn voor Nederland om zo te kunnen leren van *best practices*. Frankrijk, Canada, Finland, Zweden en Australië zijn naast het VK en de VS voor Nederland interessante casestudies. De Britse NSRA is zeker interessant en vergelijkbaar met de Nederlandse praktijk, mede door de ‘*whole-of-government*’ benadering. Er vallen dan ook uit de kritiek op de NSRA algemene lessen te leren, die ook voor Nederland relevant kunnen zijn.¹⁰⁷ Samengevat zijn deze lessen de volgende:

1. Onvergelijkbaarheid van de impact- en waarschijnlijkheid-inschatting van de risicocategorieën.

De numerieke omzettingen van impactscores zodat ze onderling per belang vergelijkbaar zijn geeft een pseudo-zekerheid en maakt een kwantificeerbare vergelijking problematisch. Dit is goed mogelijk wanneer het om statistisch kwantificeerbare fenomenen gaat, zoals bijvoorbeeld overstromingen en de uitbraak van ziekten, maar deze vergelijken met de impact van extremisme is lastig. Deze inschattingen kunnen het beste worden gedaan door experts, zoals nu ook gebeurt bij het ANV, maar door de zeer verschillende betrokken disciplines gaat het hier om experts met volledig verschillende referentiekaders en terminologie. In hoeverre deelt een specialist in de internationale betrekkingen dezelfde objectieve criteria met een specialist op het gebied van ecologie bij de inschatting van impact en waarschijnlijkheid van volledig andere scenario's?

2. Grote kwalitatieve variatie binnen risicocategorieën en gebruik scenario-methodiek.

Een blik op **tabel 4** met de lijst van dreigingsthema's en risicocategorieën laat zien dat het terugbrengen tot handzame categorieën het gevaar in zich draagt dat de nuance verloren gaat. Zo zijn een terroristisch gemotiveerd steekincident of een '9/11 type' catastrofale terroristische aanslag volledig verschillend te beoordelen dreigingen, die wel in hetzelfde thema en dezelfde categorie zijn ondergebracht. De keuze voor welke scenario's binnen de risicocategorie worden uitgewerkt, zijn hiermee bepalend, vooral omdat het aantal scenario's gezien de tijd en middelen die deze kosten, vaak beperkt zijn tot twee. In een risicocategorie zo breed als 'militaire dreigingen' of 'terrorisme' staat de representativiteit van de scenario's op het spel en dreigt generalisatie en onder- of overschatting. De meer narratieve themarapportages die de rangschikking begeleiden, zijn dan ook sterk noodzakelijk

¹⁰⁶ Vanwege de aard van de opdracht voor dit rapport en de beperkte tijd beschikbaar, hebben we ons hier beperkt tot deze twee risicoanalyses. Er is gekozen voor deze twee, vanwege de overeenkomst met de Nederlandse praktijk (VK) en de beschikbaarheid van kritische studies over de risicoanalyse (VS).

¹⁰⁷ D. Blagden, (2018), 'The flawed promise of National Security Risk Assessment: nine lessons from the British approach', *Intelligence and National Security*, 33(5), pp. 716-736.

voor het leveren van de nodige nuance op een risico-matrix. Sterker nog, er valt voor te pleiten het scoren van scenario's alleen te doen ter illustratie of ondersteuning van de kwalitatieve analyse van een thema en de risicocategorieën. Dit voorkomt de schijnzekerheid van de ranglijsten van dreigingen, zeker omdat prioritering op basis van aantasting van belangen uiteindelijk een keuze van de politiek is.¹⁰⁸ Dit geldt in mindere mate voor de categorie niet-moedwillige dreigingen, oftewel 'gevaaren'. Maar ook hier is het een politieke keuze om op basis van historische statistieken bijvoorbeeld een overstroming eens in de 10.000 of eens in de 5.000 jaar acceptabel te achten.

3. Safety vs. Security.

Het hanteren van kansberekening in het security domein is lastiger dan in het safety domein. Dit komt omdat men in het security domein vaak te maken heeft 'intelligente' actoren die hun strategie kunnen aanpassen aan een veranderende context.¹⁰⁹ Immers als uit een risicoanalyse blijkt dat er een grote kans is dat terroristen gebouw A zullen aanvallen en de overheid maatregelen neemt om gebouw A te beschermen, kunnen terroristen ervoor kiezen om gebouw B als doelwit te nemen.¹¹⁰ Intelligente actoren leren en passen hun strategie aan op de strategie van de overheid. Er is dus sprake van een sequentiële reeks van actie en reactie die niet relatief eenvoudig door kansberekening, gebaseerd op in verleden gemaakte observaties, gevat kan worden. Eenzelfde methodologie toepassen op fenomenen uit het safety en uit het security domein, lijkt derhalve onverstandig.

4. Het verdisconteren van weerbaarheid.

In een impact x waarschijnlijkheid berekening wordt het gevaar of de dreiging ingeschat. In een 'impact x waarschijnlijkheid – weerbaarheid' inschatting wordt meegewogen in hoeverre er rekening is gehouden met genomen maatregelen, beschikbaar beleid, beschikbare capaciteiten en de robuustheid van de belangen. Dit levert een inschatting van het risico op. Bij de indicatoren van de impactcriteria van dreigingen wordt bij het ANV weerbaarheid niet consistent meegewogen, noch is het voldoende uitgewerkt hoe deze 'weerbaarheid' wordt gedefinieerd. Een voorbeeld: op basis van het investeren in campagnes over desinformatie kan verwacht worden dat de Nederlandse samenleving zich meer bewust is van deze praktijken en daarmee weerbaarder is voor deze dreiging voor onze sociaal-maatschappelijke stabiliteit. Echter, betekent deze weerbaarheid dan dat in een

108 Zie ook: K. Lund Petersen, (2011), 'Risk analysis – a field within security studies?', in *European Journal of International Relations*, 18(4), pp. 699-700.

109 S. D. Guikema & T. Aven, (2010), 'Assessing risk from intelligent attacks: A perspective on approaches', in *Reliability Engineering and System Safety*, Vol. 95, p. 479.

110 G. G. Brown & L.A. Cox Jr., (2011), 'How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysis', in *Risk Analysis*, 31(2), pp. 196-204.

volgende scoring van 'desinformatie' deze veel lager op de prioriteiten ranglijst staat? En betekent dit dan weer dat de investeringen die zijn gedaan teruggedraaid kunnen worden? Eenduidigheid over het wel of niet meewegen van weerbaarheid en zo ja, hoe dit vervolgens te definiëren is van belang voor de prioritering, vergelijkbaarheid tussen categorieën en vervolgens voor de allocatie van middelen.

5. Rekening houden met interactie tussen risicocategorieën.

De classificatie in thema's, risicocategorieën of zoals voor de Horizonscans, in autonome ontwikkelingen, kunnen een verkeerd beeld geven van 'domeinautonomie'. Op deze wijze kunnen interactie-effecten tussen thema's en risicocategorieën ten onrechte niet worden meegenomen. Een duidelijk voorbeeld is de in de GRA gebruikte risicocategorie 'militaire dreigingen'. Het is onwaarschijnlijk dat militaire dreigingen in isolement zullen worden toegepast door een actor. Een kenmerk van hedendaagse hybride oorlogsvoering is het gebruik van proxies, milities, desinformatie, beïnvloeding van diaspora, cyberaanvallen, ondermijnende criminaliteit en verdeel- en heerstactieken om bondgenoten tegen elkaar uit te spelen. Al deze dreigingen kunnen los van elkaar of in combinatie met elkaar worden ingezet door één of meer statelijke, maar ook niet-statelijke actoren. Een dreiging kan ook versterkend werken op een dreiging uit een andere risicocategorie. Bijvoorbeeld militaire dreigingen in het Midden-Oosten kunnen in Nederland extremisme en zelfs terrorisme in de hand werken. Classificatie in categorieën is nodig om complexe fenomenen hanteerbaar en onderzoekbaar te maken. Echter, zeker in de actuele veiligheidsomgeving waarin de verwevenheid van veiligheidsvraagstukken kenmerkend is, moet deze categorisatie geen keurslijf worden, die de beleidsreactie te veel in de kokers houdt.

6. 'Unknown unknowns'.

Een aspect dat van toepassing is op veel risicoanalyses, is het negeren van de 'unknown unknowns' of '*Black Swans*'. 'Black Swans' werd als concept populair nadat Nassim Nicholas Taleb in 2007 *The Black Swan* schreef.¹¹¹ Hierin beschrijft hij een *Black Swan* als een gebeurtenis met drie karakteristieken:

1. De gebeurtenis ligt buiten de normale range aan verwachtingen omdat niets in het verleden wijst naar het mogelijke bestaan of ontstaan van de gebeurtenis;
2. Het heeft een extreme impact;
3. Door de aard van de mens zal men na de gebeurtenis deze proberen te verklaren en impliceren dat de gebeurtenis te voorspellen was.

Volgens Taleb (2007) lijden mensen aan '*epistemic arrogance*', oftewel hebben ze de neiging om de richting van de toekomst die ze verwachten te overschatten. In risicoanalyses baseert men zich te vaak op trends die zich in het verleden hebben

111 N.N. Taleb, (2007), *The Black Swan: The impact of the highly improbable*, (London: Penguin Books).

voorgedaan om de toekomst in te schatten. Risico-analisten zien over het algemeen de toekomst als een lineair proces. Daardoor heeft men de neiging om te focussen op de meest waarschijnlijke scenario's waardoor men te weinig rekening houdt met het verkennen van alternatieve toekomstscenario's en -ontwikkelingen.¹¹² Taleb neemt de positie in dat het proberen te voorspellen van *Black Swans* zinloos is en dat men beter kan inzetten op het opbouwen van weerbaarheid. Taleb's boek heeft echter in risicoanalysekringen een discussie losgemaakt over het concept *Black Swan events* en hoe deze te voorspellen.

Volgens Jore et al. kan *foresight* gebaseerd op een scenario-methodologie toch helpen om beter grip te krijgen op *Black Swans*, met name als men zich richt op niet-traditionele alternatieve scenario's of '*wildcard*' scenario's. Het is daarbij belangrijk om te kijken naar trends en kleine dreigingen die ontzettend snel kunnen veranderen. Het doel is om breuken met de huidige trends te identificeren. Zwakke signalen kunnen worden omgezet in alternatieve toekomstscenario's. Het invullen van deze scenario's hangt veelal af van creativiteit en vindingrijkheid van de groep mensen die betrokken zijn bij een brainstorm en het kan nuttig zijn om daarbij bijvoorbeeld sciencefictionschrijvers te betrekken.

Lindaas en Pettersen noemen het bezwaar dat de focus op kleine of vage signalen en nieuwe creatieve ideeën het onmogelijk maakt om relevante signalen te onderscheiden van achtergrondruis.¹¹³ Daardoor zou men veel waardevolle en beperkte middelen verspillen aan relatief kleine of niet bestaande problemen. Zij stellen echter dat het wel de voorkeur heeft om nieuwe ideeën te verkennen boven compleet blind te zijn voor nieuwe dreigingen om '*false positives*' te voorkomen.

7. Focus op dreiging in plaats van rekening te houden met oorzaak.

Bij de analyses door het ANV, maar ook bij die van de NSRA ligt de focus sterk op de dreigingen en de uitkomsten daarvan en niet op de oorzaak. Een voorbeeld waarom dit problematisch kan zijn, is de dreiging van een chemische ramp. Dit kan de uitkomst zijn van een technische storing, maar ook van een cyberaanval van een vijandige mogendheid of sabotage door een terroristische groepering.¹¹⁴ De relevante beleidsreactie om dit te voorkomen is in de drie gevallen volledig anders, waardoor de opname van 'chemische ramp' als dreiging op zichzelf niet volstaat en een link moet worden gelegd met een oorzaak. In een gecombineerde actor- en dreiging-

112 S.H. Jore, I.F. Utland & V.H. Vatnamo, (2018), 'The contribution of foresight to improve long-term security planning', In *Foresight*, 20(1), pp. 68-83.

113 O.A. Lindaas & Pettersen, K. A., (2016), 'Risk analysis and Black Swans: Two strategies for de-blackening', in *Journal of Risk Research*, 19(10), pp. 1231-1245.

114 D. Blagden, (2018), 'The flawed promise of National Security Risk Assessment: nine lessons from the British approach', in *Intelligence and National Security*, 33(5), p. 723.

centrische methode moet worden afgepeld in hoeverre een dreiging moedwillig kan worden veroorzaakt of een niet-moedwillige oorzaak (technisch falen, menselijk falen) kan hebben. Door de oorsprong van een dreiging in ogenschouw te nemen, wordt vermeden dat in isolement naar de verschillende dreigingen wordt gekeken, terwijl deze in sommige gevallen één en dezelfde bron kunnen hebben.

Hieronder volgt een alternatieve benadering die een aantal van de pijnpunten van de huidige dreigings- en risicoanalyses zou kunnen ondervangen. Het is vooral bedoeld als denkrichting om de huidige risicoanalyses te verbeteren. Deze alternatieve aanpak behoeft verdere ontwikkeling, waarbij ook aandacht moet blijven voor prioritering en het verdisconteren van weerbaarheid goed moet worden belegd.

Een alternatief: de gecombineerde actor- en dreiging-centrische benadering

De door verschillende risicoanalyses (ANV, HSNRC, NSRA) gebruikte dreiging-centrische benadering kent voor- en nadelen. De voordelen zijn dat er een focus ligt op de aantasting van dat wat een land of organisatie wil beschermen, namelijk zijn vitale belangen. Dit plaatst de dreiging door middel van kwantificeerbare variabelen van impact en waarschijnlijkheid in perspectief ten opzichte van andere dreigingen. De vraag is echter, zoals hierboven al aangestipt, in hoeverre dit mogelijk is en zinvol. De oorsprong van dreiging-centrische benaderingen liggen in het bedrijfsleven en dan met name het bank- en verzekeringswezen. Dit is één van de redenen dat de risicoanalyses gestoeld zijn op een economische benadering van risico, waarin een kosten-baten calculatie centraal staat. Deze calculatie is voor rampen gebaseerd op statistieken die de waarschijnlijkheid van de materialisering van het risico weergeven. Een risico kan in deze logica worden gemeten en daarmee gecontroleerd, een zogenaamde “*measurable uncertainty*”.¹¹⁵ Een dergelijke methode is replicerbaar, kwantitatief onderbouwd en, mits gedegen uitgevoerd, daarmee het beste wat er momenteel op de markt is. Echter, de sterk toegenomen complexiteit van onze maatschappij en de verweving daarvan met de rest van de wereld brengt meer moedwillige dreigingen met zich mee, die veel minder voorspelbaar zijn (zie ook de sectie over de nexus en globalisering). Hier ligt ook het grote nadeel van de risicoanalyses die op dreigingsbenaderingen zijn gebaseerd.

Alle verbeterpunten die hierboven zijn genoemd hebben in meer of mindere mate te maken met het niet voldoende verdisconteren van complexiteit. Een aantal verbeterpunten kunnen worden aangebracht door niet naar de dreiging zelf te kijken, maar naar de bron of oorzaak van de dreiging. Dreiging-centrische benaderingen kunnen een blinde vlek voor actoren en hun intenties in de hand werken. Eén actor kan allerlei tactieken gecombineerd gebruiken ten behoeve van één strategie.

115 U. Beck, (1992), *Risk Society. Towards a New Modernity*, p. 697.

Bovendien heeft een actor-centrische benadering het voordeel dat het een duidelijk onderscheid maakt tussen moedwillige en niet-moedwillige dreigingen. Dit kan leiden tot een onderscheid in de methodologie en zo de kunstmatige analytische gelijkschakeling van rampen en ongelukken aan de ene kant en door vijanden toegebrachte aantasting van onze belangen aan de andere kant, opheffen. Dit betekent dat een 'actor-centrische benadering' van risicoanalyses zou moeten worden geïntroduceerd.

Een interessant voorbeeld van een actor-centrische benadering is bijvoorbeeld de 'Statelijke dreigingen' Kamerbrief van de NCTV.¹¹⁶ Hier wordt een categorisering gemaakt van dreigingen op basis van de bron van de dreiging, namelijk statelijke actoren. Niet-statelijke actoren worden bij de brief buiten beschouwing gelaten en ook worden de staten niet bij naam genoemd, maar Nederland wil generieke maatregelen treffen om de dreiging die uit gaat van deze actoren te ondervangen. In een publiek beschikbare communicatie is deze omzichtige wijze van omgaan met de 'bron' van dreiging te begrijpen. In analytische zin, en voor het effectief tegengaan van statelijke dreigingen zal man en paard moeten worden genoemd. Voor moderne afschrikking is een diepe kennis van de actor juist van groot belang om maatwerk te kunnen leveren om vijanden te ontmoedigen.

Het nadeel van een pure actor-centrische benadering is juist weer een mogelijke blinde vlek voor dreigingen, vooral van actoren die nog niet op het netvlies van eerdere risicoanalyses of beleidsstukken staan. Staten als dreigingsactoren zijn nog de meest eenvoudige categorie, hiervan komen in theorie 196 voor in aanmerking¹¹⁷, maar er manifesteren zich veel dreigingen die veroorzaakt worden door niet-statelijke actoren, zoals terroristische groeperingen, misdada syndicaten en transnationale extremistische bewegingen. De hoeveelheid potentiële niet-statelijke actoren is zeer groot, waardoor het een onmogelijke opgave wordt om de intentie X vermogen van al deze actoren te monitoren. Het kan ook voorkomen dat een dreiging wordt onderkend, zoals bijvoorbeeld grootschalige witwaspraktijken, waarvan het onduidelijk is wie of wat de bron is.¹¹⁸ Dit attributieprobleem komt ook veel voor bij cyberspionage, cybermisdad en cybersabotage.¹¹⁹ Ook kan bij te veel focus op actoren een bias ontstaan, waardoor de dreigingen van andere actoren kunnen worden gemist.

116 NCTV, (2019), *Tegengaan statelijke dreigingen*, Kamerbrief 2573867, 18 april 2019.

117 Er zijn 196 internationaal erkende nationale staten.

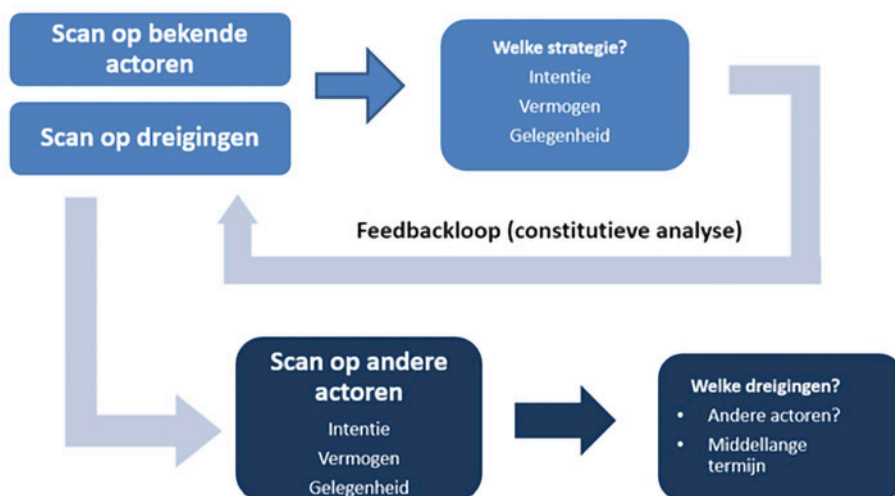
118 Actor centrische scenario's om statelijke en niet-statelijke dreigingsactoren te detecteren in het verplaatsen en witwassen van financiële middelen (bv: ISIS): <http://ownershiptransparency.com/aml/analysis-islamic-states-financial-withdrawal-poses-big-new-anti-laundering-challenge/>.

119 M. Arena, (2016), *Cyber Threat Intelligence: Comparing the incident-centric and actor-centric approaches*, via: <https://medium.com/@markarenaau/cyber-threat-intelligence-comparing-the-incident-centric-and-actor-centric-approaches-f20cfba2dea2>.

Een methode die bovenstaande nadelen kan ondervangen en daarbij wel de voordelen behoudt, is het gebruiken van een gecombineerde actor- en dreiging-centrische benadering. Het vertrekpunt van de analyse is hierbij niet alleen de dreiging, ook niet alleen de actor, maar *beide*. Een aantal actoren die op het lijstje staan omdat ze potentieel een dreiging vormen voor onze nationale veiligheid zijn immers al bekend. Niemand zal verrast zijn dat bijvoorbeeld Rusland of ISIS als interessante actoren worden beschouwd voor een risicoanalyse. Dit geeft een startpunt voor de risicoanalyse: deze actoren kunnen direct worden meegenomen in de scan op dreigingen en dreigingsactoren. Door echter de onderstaande stappen te doorlopen wordt actorbias voorkomen en worden ook dreigingen waarvan de oorsprong onduidelijk is, voldoende verdisconteerd. Een gecombineerde actor- en dreigingsanalyse zou derhalve de volgende stappen kunnen doorlopen (zie figuur 2):

- Voer een tweeledige scan uit:
 - 1) Scan op manifestaties van dreigingen;
 - 2) Scan tegelijkertijd ook op een lijst van bekende dreigingsactoren en analyseer welke dreigingen van hen uitgaan en welke dreigingen in de toekomst van deze actoren kunnen worden verwacht;
- Inventariseer van welk palet aan andere dreigingen van deze actoren deze dreiging onderdeel is;
- Gebruik deze informatie om de gescande dreiging verder te kunnen verdiepen en verfijnen.
- Scan daarna op actoren (statelijk en non-statelijk), welke dreigingen veroorzaken zij, zijn er nog andere actoren en welke dreigingen worden verwacht in de komende vijf jaar aan de hand van intentie, vermogen, gelegenheid.

Figuur 2 De gecombineerde actor- en dreigingsanalyse



Bij deze methode wordt een soort 'loop' gebruikt of een 'constitutieve analyse', waarbij de onderzoeker de belangrijkste moedwillige dreigingen terugvoert op bepaalde actoren, deze vervolgens onderzoekt op 'intentie + vermogen + gelegenheid' om te handelen en welk dreigingspalet ze hanteren om daarmee in een 'loop' terug te keren naar de dreigingen. Zo kan er een verfijning worden aangebracht in de mate van dreigingen en de attributie ervan. Kortom, een combinatie van zowel een 'actor-centrische' en 'dreiging-centrische' benadering, zonder in de valkuil van bias of 'actor- of dreigings-blindheid' te vallen. In hoofdstuk 4 wordt het voorbeeld van hybride dreigingen aan de hand van deze methode uitgewerkt.

Elementen voor de onderzoeksagenda

Dit hoofdstuk heeft een beknopt overzicht gegeven van hoe in Nederland risicoanalyses worden gedaan ten behoeve van de nationale veiligheid. De gebruikte methoden zijn in een beperkt internationaal perspectief geplaatst en een aantal problemen van de huidige methodiek zijn geïdentificeerd. Een gecombineerde actor- en dreiging-centrische benadering kan een aantal van deze problemen adresseren en is een interessante richting waarvoor meer onderzoek nodig is. Deze benadering wordt in hoofdstuk 4 verder getest. Daarnaast blijven er een aantal vragen over:

- Hoe kunnen we de complexe dreigingsomgeving zo weergeven dat het onderzoekbaar en repliceerbaar is, maar dat toch de complexe dwarsverbanden en verwevenheid goed in beeld worden gebracht?
- Welke lessen zijn er te leren van de praktijk van risicoanalyses van andere landen?
 - o Een comparatieve landenstudie naar *best practices* op het gebied van methoden van risicoanalyses. Het zou interessant zijn om toonaangevende veiligheidspartners te onderzoeken, zoals het VK de VS en Frankrijk Duitsland, maar ook landen van vergelijkbare grootte, zoals bijvoorbeeld Canada, Finland, Zweden en Australië.
- Hoe kan weerbaarheid ten opzichte van een dreiging worden gedefinieerd en hoe gaan we om met leereffecten van dreigingen op de calculatie van weerbaarheid?
- Op welke wijze kunnen we zinvol prioriteren tussen dreigingen en gevaren (*security* en *safety* fenomenen)?
- Op welke wijze kan Nederland zich beter voorbereiden op '*unknown unknowns*'?
- Nader onderzoek naar de 'internationale rechtsorde' als vitaal belang van Nederland is gewenst. Is het terecht en verstandig dat dit als vitaal belang wordt bestempeld? Wat maakt precies onderdeel uit van dit belang (in hoeverre worden bijvoorbeeld mensenrechten meegewogen of maakt het internationaal-financieel economisch stelsel er ook deel van uit)? Hoe gaan andere landen hiermee om? Welke gevolgen heeft het besluit van de SNV om het als zesde belang toe te voegen voor de Nederlandse positionering in het internationale krachtenveld? Hoe verhoudt dit vitale belang zich tot de buitenland- en veiligheidsbeleid agenda van Nederland?

4 Een casus voor de gecombineerde actor- en dreiging-centrische benadering: “hybride conflictvoering”

Inleiding

In hoofdstuk 3 zijn de voor- en nadelen van een actor- en dreigings-centrische benadering besproken en is er een alternatief gepresenteerd: de gecombineerde actor- en dreigingsanalyse. In dit hoofdstuk toetsen we deze gecombineerde benadering door ‘hybride conflictvoering’ onder de loep te nemen. Wat missen we als we dit fenomeen benaderen vanuit enkel de actor- of dreigings-centrische benadering? En wat levert de gecombineerde analyse op?¹²⁰

Een dreiging-centrische benadering

Er bestaan veel verschillende definities (en termen) voor hybride conflictvoering. Het ANV hanteert in de GRA de volgende definitie: het gaat over conflictvoering tussen staten, meestal onder het niveau van gewapend conflict, waarbij op geïntegreerde wijze gebruik wordt gemaakt van een spectrum aan middelen: economische, diplomatieke, culturele, digitale middelen, desinformatie, beïnvloeding, etc. Kenmerkend aan deze vorm van conflictvoering is dat het onderdeel uitmaakt van een strategie/campagne, met als doel het halen van bepaalde geopolitieke of strategische doelstellingen. In de verschillende Nederlandse strategie- en analyseproducten wordt dit fenomeen beschreven onder verschillende noemers, maar die feitelijk deel uitmaken van hetzelfde spectrum aan hybride dreigingen, denk aan ‘hybride operaties’ (GRA), ‘hybride oorlogsvoering’ (Meerjarig perspectief krijgsmacht), ‘ondermijning van de democratische rechtstaat door statelijke actoren’ (GRA), en ‘ongewenste buitenlandse inmenging en ondermijning’ (GBVS). Een voordeel van de dreiging-centrische

¹²⁰ Het doel van deze casestudie is niet per se een uitputtende uiteenzetting te geven van alle mogelijke dreigings(vormen) van hybride dreigingen, maar met name te testen wat een gecombineerde actor- en dreigingsanalyse oplevert. Er wordt daarom gebruik gemaakt van de input van bestaande analyses.

benadering, is dat snel de focus ligt op de potentiële gevaren voor de samenleving: hybride activiteiten zijn gericht op “het direct compromitteren, verzwakken, ondergraven en destabiliseren van Nederland zelf, zijn democratische rechtsstaat en open samenleving”.¹²¹ Bestaande kwetsbaarheden in de maatschappij worden slim uitgebuit door statelijke actoren. Spanningen tussen bevolkingsgroepen, maar ook tussen staten, worden vergroot en de legitimiteit van instituties wordt ter discussie gesteld. Uitingen daarvan zien we onder andere in de vorm van desinformatiecampagnes, cyberaanvallen, militaire acties en/of inmenging in democratische verkiezingen.

Er kleven echter ook nadelen aan een dreiging-centrische benadering. Een hybride aanval, zoals een desinformatiecampagne (*trolling*) of een cyberaanval, is in veel gevallen lastig te herkennen. Als de aanval al als dusdanig wordt herkend, dan is het achterhalen van de verantwoordelijke actor ook niet altijd eenvoudig en soms zelfs onmogelijk, mede door de inzet van proxies. Extra lastig is het bovendien om de verschillende uitingsvormen met elkaar te verbinden (*‘connecting the dots’*) en te herkennen als onderdeel van een georkestreerde strategie van een statelijke actor. Het is daarom ook noodzakelijk de tegenstander te kennen en te beredeneren vanuit deze actor: wat zijn de strategische doestellingen en intenties, en wat zijn de middelen die deze actor kan inzetten?

Een actor-centrische benadering

Meer recentelijk wordt de actor die achter de ondermijnende activiteiten schuilgaat, expliciet benoemd in de Nederlandse strategie- en analysedocumenten. In de departementaal vertrouwelijke themarapportage over ondermijning van de democratische rechtstaat, die onderdeel is van de GRA, worden twee specifieke scenario's uitgewerkt over hybride acties door Rusland en China. Ook in een verdiepende rapportage van het ANV uit 2018, worden de hybride dreigingen die uitgaan van China, Rusland en Noord-Korea verder uitgewerkt.¹²² In deze analyses wordt ingegaan op de intenties, middelen en doelen van de verschillende actoren, en wordt er met behulp van scenario's ingeschat wat het potentiële effect is van deze tactieken voor de nationale veiligheid. Hoewel het benoemen van specifieke actoren in dergelijke dreigingsanalyses een goede ontwikkeling is, is dit nog niet hetzelfde als een pure actor-centrische benadering. Deze analyses vertrekken nog altijd vanuit de dreiging, er wordt immers gekeken vanuit de dreiging ‘hybride conflictvoering’ naar de achterliggende actor, die ook vaak gebruik maakt van proxies, waardoor attributie moeilijk is. Daarbij wordt niet gekeken naar de onderliggende strategie en de potentieel andere uitingsvormen.

121 Analistennetwerk Nationale Veiligheid, Geïntegreerde risicoanalyse Nationale Veiligheid, 2019, p. 16.

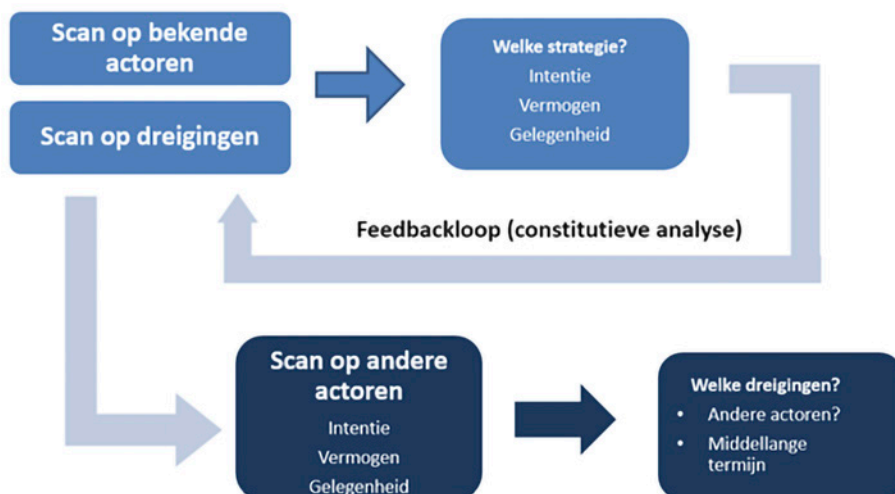
122 F.P. van der Putten et al. (ed), (2018), via: https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf.

Een voordeel van de actor-centrische benadering, is dat door de bredere intenties en strategie van de actor te kennen, inclusief het patroon van het rekruteren en gebruik van proxies, de overige manifestaties ook beter te herkennen zijn als onderdeel van die strategie. Echter, zelfs al ken je de tegenstander nog zo goed, stelt dat nog niet in staat alle verschillende uitingsvormen van 'hybride dreigingen' waarmee de Nederlandse samenleving te stellen heeft te herkennen. Het is immers de intentie van de actor om te opereren in het 'grijze gebied' van conflictvoering, onder de drempel van oorlogsvoering, en niet-attribueerbaar te handelen. In sommige gevallen zullen dreigingen zich manifesteren via andere actoren, al dan niet aangestuurd door een statelijke actor, denk aan: terroristische groeperingen, cybercriminelen of misdaadsyndicaten. Deze actoren maken veelal gebruik van de ambiguïteit omtrent de hybride campagnes van statelijke actoren. In weer andere gevallen wordt wel de dreiging gezien, zoals een grootschalige cyberaanval, maar is lang niet altijd duidelijk welke actor daarachter schuilgaat. Door te veel op een bepaalde actor te focussen, bestaat het risico dat andere (statelijke) actoren over het hoofd worden gezien.

De gecombineerde actor- en dreiging-centrische benadering

Een methode die de nadelen kan ondervangen van de twee bovengenoemde benaderingen, is het gebruiken van een gecombineerde actor- en dreiging-centrische benadering. Het vertrekpunt van de analyse is niet alleen de dreiging, ook niet alleen de actor, maar beide. Daarvoor worden de volgende stappen doorlopen (zie Figuur 3):

Figuur 3 De gecombineerde actor- en dreigingsanalyse



Stap 1A: Wat zijn de verschillende manifestaties van de dreigingen?

In de verschillende risicoanalyses worden er diverse manifestaties van de dreiging genoemd, waaronder:

- Desinformatiecampagnes/nepnieuws
- Economische spionage
- Propaganda
- Inmenging democratische verkiezingen
- Militaire activiteiten (onder de drempel van daadwerkelijke oorlogsvoering): geanonimiseerde strijdkrachten, (grootschalige) militaire oefeningen, etc.
- *Strategic Messaging*
- Cyberaanvallen
- Aanvallen op kritische infrastructuur

Stap 1B: Komt de dreiging van een bekende en moedwillige actor?

Zoals eerder beschreven, staan er meerdere statelijke actoren op het netvlies van Nederland waar potentiële dreigingen vanuit kunnen gaan. Dit betreft met name Rusland en China. Door stelselmatig te controleren of de hybride dreiging vanuit een van deze actoren komt, alvorens een bredere actorscan uit te voeren, kan er tijd worden gewonnen.

Stap 2: Analyseer welke intentie, welk vermogen en welke gelegenheid de actor heeft om deze dreiging uit te voeren.

De belangrijkste moedwillige actoren die achter deze dreigingen schuilgaan zijn statelijke actoren. Veel staten bedienen zich van hybride conflictvoering, maar niet alle landen doen dat met dezelfde hoge mate van integratie en activiteit. Twee landen die om die reden wel specifiek opvallen, zijn China en de Rusland.¹²³ De hybride activiteiten van Rusland krijgen nationaal en internationaal de meeste aandacht, vanwege de veelvoud aan activiteiten, maar ook omdat deze gepaard gaan met een hoge mate van agressiviteit: denk aan de inzet van anonieme strijdkrachten ('groene mannetjes') tijdens de annexatie van de Krim in 2014 en Russische betrokkenheid in het conflict in Oost-Oekraïne. Tegelijkertijd groeit ook het bewustzijn dat China activiteiten ontplooit die gericht zijn op het creëren of vergroten van invloed.

123 NCTV, (2019), Chimaera: Een duiding van het fenomeen 'hybride dreiging', (Den Haag), p. 15;
Analistennetwerk Nationale Veiligheid, Geïntegreerde risicoanalyse Nationale Veiligheid, 2019, p. 16.

De intenties en capaciteiten van China en Rusland verschillen behoorlijk, evenals de kwetsbaarheden die deze actoren uitbuiten binnen onze samenleving (de 'gelegenheid').

Tabel 7 gelegenheid, intentie en vermogen van Rusland en China¹²⁴

	Gelegenheid	Intentie	Vermogen/capaciteiten
Rusland	<ul style="list-style-type: none"> Mate van kwetsbaarheid van onze open samenleving en instituties (inclusief EU, NAVO) door polarisatie en uiteenlopende belangen; Technologische ontwikkelingen op het gebied van informatietechnologie; Diaspora/sympathisanten 	<ul style="list-style-type: none"> Ondermijnen eenheid EU/ NAVO Behouden/vergroten van machtspositie en invloed in 'near abroad' Ondermijning van democratische processen Eroderen van vertrouwen in politieke instituties, media 	<ul style="list-style-type: none"> Cyberaanvallen Desinformatiecampagnes (<i>trolling</i>) en propaganda Economische dwang Militaire activiteiten Heimelijke operaties Inzet proxies/niet-statelijke actoren
China	<ul style="list-style-type: none"> Mate van kwetsbaarheid van onze open samenleving, economie en instituties; Lage dreigingsperceptie door China's aantrekkelijkheid als economische partner; Verzwakkende waardengemeenschap met de VS 	<ul style="list-style-type: none"> In stand houden van regime/onderdrukken van kritische opvattingen Economische en politieke machtsbalans beïnvloeden Beeld over China beïnvloeden en steun krijgen voor standpunten/ beleid Beïnvloeden/ondergraven van liberale internationale orde Vergroten van onrust Wil militaire macht worden, die zelfs de VS kan verslaan 	<ul style="list-style-type: none"> Economische (digitale) spionage Invloed uitoefenen via personen in politiek, media, wetenschap of bedrijfsleven Invloed uitoefenen via diaspora Publieksdiplomatie Opzetten van onderzoeksnetwerken/ instituten Inzet proxies/niet-statelijke actoren

Stap 3: Van welk palet aan andere dreigingen van deze actor is deze dreiging onderdeel?

Het is belangrijk te realiseren dat hybride conflictvoering altijd al een rol heeft gespeeld in de internationale betrekkingen, niet alleen ten tijde van conflict. Hybride conflictvoering maakt een permanent onderdeel uit van het buitenlands beleid van

124 Input samengesteld uit o.a.: NCTV, (2019), [Chimaera: Een duiding van het fenomeen 'hybride dreiging'](#), (Den Haag); D. Pronk, (2019), 'The Return of Political Warfare', in: *Strategic-Monitor 2018-19*, Clingendael en HCSS; Analistennetwerk Nationale Veiligheid, themarapportage "Ondermijning van de democratische rechtstaat en open samenleving", onderdeel van de geïntegreerde risicoanalyse, maart 2019 (interdepartementaal vertrouwelijk); F.P. van der Putten et al. (ed.), (2018), https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf.

staten en is erg breed.¹²⁵ In deze derde analysestap gaat het dus om een bredere analyse, die niet enkel gericht is op hybride conflictvoering. Het is van belang, wat ook bepleit wordt in de recente Kamerbrief Tegengaan statelijke dreigingen, te kijken naar middelen en activiteiten die de “gehele breedte van het overheidsinstrumentarium bestrijken en al dan niet worden toepast als onderdelen van een doelgerichte strategie van hybride conflictvoering”.¹²⁶ De verschillende type machtsinstrumenten (we hanteren hiervoor het acroniem DIME¹²⁷) kunnen op hetzelfde moment worden ingezet, op verschillende niveaus en dimensies.¹²⁸

Rusland

In Nederland gaat relatief veel aandacht uit naar Russische acties als desinformatie-campagnes, het verspreiden van nepnieuws en inmenging in democratische verkiezingen. Om echter een compleet beeld te krijgen, moet er gekeken worden naar het gehele palet aan dreigingen die voortkomen uit de inzet van het volledige overheidsinstrumentarium¹²⁹:

- **Diplomatieke/politieke instrumenten:** hier gaat het vooral om Russische opstelling in internationale instituties, waar het bijvoorbeeld besluitvorming probeert te blokkeren (VNVR) of anderszins dwarsboomt. Een ander voorbeeld is het opschorten of opzeggen van verdragen, zoals in het geval van het INF-ontwapeningsverdrag (in reactie op eerdere opzegging door de VS).
- **Informatie-instrumenten:** Het informatiedomein is een zeer belangrijke in de Russische strategie, het land is zeer bedreven in de inzet van dit type middelen: “het is de rode draad door de wijze waarop in Moskou conflictvoering wordt bedreven”, aldus de NCTV.¹³⁰ Het gebruikt op grote schaal desinformatie- (en *internet trolls*) en propagandacampagnes om politieke besluitvorming te beïnvloeden en de publieke opinie te manipuleren. Rusland maakt daarbij gebruik van andere partijen als criminele organisaties, hackersgroepen en aan de staat-gelieerde media die zich voordoen als onafhankelijk. Ontwikkelingen in het cyber- en informatiedomein

125 F.P. van der Putten et al., ‘Hybrid Conflict’, p. 3.

126 NCTV, (2019), *Tegengaan statelijke dreigingen*, Kamerbrief 2573867, 18 april 2019, p. 3.

127 DIME is een veelgebruikt acroniem om alle machtsinstrumenten van de staat te benoemen: Diplomatic, Information, Military, Economic means.

128 F. Bekkers et. al., (2018), *Hybrid Conflicts: the New Normal?* TNO; MCDC, (2017), [MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare](#).

129 Het is hier niet de bedoeling een uitputtende lijst te geven van alle instrumenten die kunnen worden ingezet, maar voorbeelden te geven. Input is o.a. verzameld uit: NCTV, ‘Chimaera. Een duiding van het fenomeen ‘hybride dreiging’, april 2019, F. Bekkers et al., “[Hybrid Conflicts: the New Normal?](#)”, TNO, december 2018, Analistennetwerk Nationale Veiligheid, themarapportage “Ondermijning van de democratische rechtstaat en open samenleving”, onderdeel van de geïntegreerde risicoanalyse, maart 2019.

130 NCTV, (2019), Chimaera: Een duiding van het fenomeen ‘hybride dreiging’, (Den Haag), p. 28.

faciliteren dit type ondermijning. Cyberaanvallen worden in toenemende mate gebruikt om bijvoorbeeld gevoelige informatie te bemachtigen of om democratische processen te verstoren.

- **Militaire instrumenten:** het gaat hier om de inzet van conventionele (inclusief nucleaire) en onconventionele militaire middelen, denk bijvoorbeeld aan (onaan-gekondigde) grootschalige militaire oefeningen, het samentrekken van troepen aan de grens, de inzet van ‘groene mannetjes’ (geanonimiseerde troepen) of private militaire bedrijven. Rusland heeft in de laatste jaren flink geïnvesteerd in zijn krijgsmacht en heeft laten zien militaire middelen ook daadwerkelijk (demonstratief) in te zetten aan zijn grenzen, inclusief de inzet van (strategische) bommenwerpers en jachtvliegtuigen. Ook het dreigen met de inzet van nucleaire wapens is een goed voorbeeld van het inzetten van het militaire instrumentarium, evenals het verlagen van de inzetdrempel van nucleaire wapens. Daarnaast worden ook militaire interventies gebruikt, onder het mom van *peacekeeping*/humanitaire hulp.
- **Economische instrumenten:** een belangrijke troef die Rusland in handen heeft, is de inzet van de toegang tot de energievoorziening. Het land gebruikt de toegang tot gas als politiek drukmiddel, bijvoorbeeld door de gaskraan dicht te draaien in het geval van conflict (dit gebeurde bijv. in het geval van Georgië, Wit-Rusland, Oekraïne).¹³¹ Ook het gasbedrijf Gazprom blijkt een instrument en onderdeel van Ruslands buitenlandpolitiek: het zet Oost-Europese landen onder druk en probeert de energiemarkt naar zijn hand te zetten.¹³² In het debat over de pijpleiding Nord-Stream 2 speelt ook steeds meer de afhankelijkheidsvraag.¹³³ Andere middelen die behoren tot het economisch instrumentarium betreffen de inzet van sancties en boycots.

Tot slot is het belangrijk om te beseffen dat Rusland weliswaar zeer (en steeds beter) bedreven is in het inzetten van zijn gehele instrumentarium, maar dat er niet altijd sprake is van een coherente en perfect georkestreerde strategie. Het land zal opportuun, en soms ad hoc, gebruik maken van bestaande of nieuwe zwakheden en kloven in de Europese samenlevingen. Juist omdat de militaire capaciteit van Rusland relatief zwak is, is het op zoek naar andere instrumenten om zijn invloed uit te oefenen. Het land zoekt daarbij naar de weg van de minste weerstand en past voortdurend zijn tactieken aan.

131 Ministerie van Buitenlandse Zaken, (2018), [Kamerbrief over de Nederlandse gasrelatie met Rusland](#), 26 augustus 2018.

132 A. Evans-Pritchard, (2018), [‘Leaked EU files show Brussels cover-up and collusion on Putin’s Gazprom abuses’](#), *The Telegraph*.

133 M. Meijnders & M. Martens, (2019), [Global Security Pulse: Economic Security](#), (Clingendael Institute en HCSS).

China

Recentelijk is de aandacht voor de groeiende macht van China toegenomen. Het land heeft zijn positie op het wereldtoneel weten te verstevigen, met name via economische instrumenten. Maar ook China zet de volle breedte in van zijn staatsinstrumentarium¹³⁴:

- **Diplomatieke/politieke instrumenten:** hier moeten met name China's pogingen genoemd worden om bepaalde elementen van de westers gedomineerde liberale wereldorde om te vormen. Dit wordt ofwel gedaan in bestaande multilaterale instituties, ofwel door nieuwe, parallelle instituties op te richten waarbij andere normen gelden. Daarnaast gebruikt China (publieks-)diplomatieke middelen om het beeld van China als '*responsible stakeholder*' neer te zetten, en herhaalt het voortdurend het 'win-win' karakter van Chinese investeringen. Een ander instrument zijn de zogenaamde Confucius Instituten waar Chinese taal- en cultuur gepromoot wordt.
- **Informatie-instrumenten:** het informatie-machtsinstrument wordt sterk gedomineerd door de Chinese staat, en moet de diplomatieke boodschap van een vreedzame, moderne wereldmacht ondersteunen. Het maakt op grote schaal gebruik van spionageactiviteiten, grotendeels via het cyberdomein, maar ook via traditionele kanalen. Daarnaast zijn er zorgen over China's pogingen om officiële westerse media te beïnvloeden, hoewel tot nu toe beperkt. China probeert ook invloed uit te oefenen via onderwijs – en kennisinstellingen, waar het probeert de opinie over China en zijn standpunten op gevoelige kwesties (bijv. mensenrechten, Taiwan, Zuid-Chinese Zee, etc.) te beïnvloeden. Journalisten worden soms onder druk gezet.¹³⁵ Daarnaast probeert het de politieke elite en het bedrijfsleven te beïnvloeden, door pro-China personen strategisch te positioneren.
- **Economische instrumenten:** zoals gezegd gaat er veel aandacht uit naar China's groeiende invloed middels economische instrumenten, zoals Chinese investeringen en overnames, het opzetten van financiële instituties, mega-infrastructuur projecten als het *Belt and Road Initiative (BRI)* en economische beleidsplannen als '*Made in China 2025*'. Naast economische winst, zijn er daarmee ook afhankelijkheden gecreëerd die China zou kunnen uitbuiten. Andere economische middelen betreffen het beperken van de toegang tot de Chinese markt, of het inperken van toegang

134 Ook hier is het niet de bedoeling een uitputtend overzicht te geven van alle mogelijke manifestaties, maar gaat het om voorbeelden. Input is verzameld uit o.a.: NCTV, 'Chimaera. Een duiding van het fenomeen 'hybride dreiging', april 2019; ANV, themarapportage "Onderminning van de democratische rechtstaat en open samenleving", onderdeel van de geïntegreerde risicoanalyse, maart 2019; Thorsten Benner et al, "[Authoritarian Advance: Responding to China's Growing Political Influence in Europe](#)", Global Public Policy Institute and Merics, 2018; François Godement en Abigaël Vasselier, [China At The Gates: A New Power](#), [Audit Of EU-China Relations](#), European Council on Foreign Relations, 2017, Jarrod Stoutenborough, [China's Comprehensive Approach: Refining the U.S. Targeting Process to Inform U.S. Strategy](#), 2018.

135 AIVD Jaarverslag 2018, p. 10.

tot bepaalde grondstoffen (in het bijzonder tot zeldzame aardmetalen). China zet een breed scala aan heimelijke middelen in, waaronder economische spionage. “Verreweg de grootste dreiging op het gebied van economische spionage is afkomstig van China.”, zo stelde het meest recente jaarrapport van de AIVD het onomwonden.¹³⁶

- **Militaire instrumenten:** er is een duidelijke groei van China’s militaire capaciteiten te zien. China gebruikt dit militaire instrumentarium om een duidelijke boodschap af te geven over zijn militaire macht. Dit geldt niet zozeer in de richting van Europa of Nederland, maar speelt met name in het machtsspel in de Zuid-Chinese Zee regio. Op de langere termijn, richting 2049, beoogt China ook de VS in een militaire confrontatie aan te kunnen.

In het geval van China moet worden gerealiseerd dat zijn strategie een veel langere tijdshorizon kent; het is erop gericht zijn positie op de lange termijn – dat wil zeggen, de komende decennia – te vergroten.¹³⁷ De implicaties van China’s (veelal legale) beïnvloedingstactieken zullen wellicht ook pas op de lange termijn echt zichtbaar zijn. Door op veel verschillende plekken en op verschillende niveaus in onze economie, politiek, media, universiteiten etc. te opereren, zullen (wellicht ongemerkt) steeds meer ‘pro-China’ standpunten te horen zijn en het beleid beïnvloeden. Daarmee verandert China uiteindelijk de context waarbinnen Nederland opereert. Op dit moment gebruikt China zijn politieke en economische macht vooral als het direct aan zijn nationale belangen raakt (denk aan Zuid-Chinese Zee, Taiwan, Tibet). China’s macht zal de komende jaren alleen maar toenemen en de verwachting is dat China er niet voor zal schromen zijn economische macht in te zetten voor politieke doeleinden.

Concluderend geldt voor beide statelijke actoren dat de dreigingen die hiervan uitgaan verschillende onderdelen van de nationale veiligheid raken. Tegelijkertijd zijn er accentverschillen tussen beide actoren. Russische activiteiten raken voornamelijk democratische processen en maatschappelijke stabiliteit, digitale veiligheid en de stabiliteit van de bondgenootschappen. Chinese activiteiten hebben vooral effect op economische veiligheid en op de internationale rechtsorde. Door vanuit de actoren te redeneren en de volle breedte van de manifestaties in kaart te brengen, wordt het duidelijker hoe deze dreigingen met elkaar samenhangen en onderdeel vormen van één overkoepelende strategie.

¹³⁶ AIVD Jaarverslag 2018, p. 9.

¹³⁷ ANV, themarapportage “Ondermijning van de democratische rechtstaat en open samenleving”, p. 21.

Stap 4: Zijn er nog andere actoren en welke dreigingen worden verwacht in de komende vijf jaar aan de hand van intentie, vermogen en gelegenheid?

Om een compleet beeld te krijgen van de 'hybride dreigingen', moet er tot slot worden gekeken welke andere actoren, naast de al bekende in stap 1B, verder naar voren komen. Het gaat daarbij enerzijds om proxies die zich manifesteren tijdens de actorscan, in dit geval Rusland en China. Anderzijds gaat het om andere statelijke actoren die zich eveneens bedienen van beïnvloedingstactieken, al dan niet als onderdeel van een hybride strategie.

Proxies van China/Rusland

Uit bovenstaande analyse blijkt dat beide statelijke actoren gebruik maken van proxies om hun doelen te bereiken. In het geval van Rusland zien we de forse inzet van een hele reeks aan proxies: criminele hackerscollectieven, bedrijven (bijv. Gazprom)/zakenelite, politieke partijen, private militaire bedrijven, anonieme strijdtroepen, non-gouvernementele organisaties, (traditionele en alternatieve) media, etc. Naar verluidt zijn er bijvoorbeeld duizenden mensen aan het werk om maatwerk desinformatie te kunnen verspreiden.¹³⁸ Ook in het geval van China is het beeld divers: bedrijfsleven, studenten, Chinese diaspora, media, etc. Voor zowel Rusland als China geldt dat de verwachting is dat ze op grote schaal dergelijke proxies zullen inzetten, juist omdat ze onder de radar willen blijven en attributie willen voorkomen of bemoeilijken. Tegelijkertijd geldt ook dat de relatie tussen de staat en de proxies niet altijd eenduidig en zonder conflict is: met andere woorden, er is geen garantie dat de staat altijd 'in control' is.¹³⁹

Andere statelijke actoren die gebruik maken van beïnvloedingstactieken/hybride conflictvoering

Het is niet afdoende enkel vanuit een specifieke actor (in dit geval Rusland, China) en zijn proxies te beredeneren, daarmee worden andere actoren potentieel over het hoofd gezien (de 'actorbias'). Er zijn ook andere statelijke actoren die zich bedienen van de strategie hybride conflictvoering (en weer andere proxies gebruiken). Vaak is daarbij sprake van een minder hoge mate van integratie van machtsmiddelen van de staat. Een voorbeeld is Iran, dat wordt beticht van ongewenste inmenging. Het land beïnvloedt en intimideert diaspora in Nederland en richt zich op personen

138 NCTV, (2019), Chimaera: Een duiding van het fenomeen 'hybride dreiging', (Den Haag) p. 31.

139 M. Klein, *Private military companies – a growing instrument in Russia's foreign and security policy toolbox*, Hybrid Centre of Excellence, 2019, p. 5, via: https://www.hybridcoe.fi/wp-content/uploads/2019/06/HybridCoE_StrategicAnalysis_3_2019.pdf.

en organisaties die te boek staan als tegenstanders van het regime.¹⁴⁰ Iran is waarschijnlijk betrokken bij de (voorbereidingen op) liquidaties van twee Nederlanders van Iraanse komaf op Nederlands grondgebied. Ook elders in Europa is er sprake van ongewenste inmenging vanuit Iran: twee mislukte aanslagen in Denemarken en Frankrijk worden ook toegeschreven aan het Iraanse regime.¹⁴¹ De AIVD meldt dat Iran offensieve cyberprogramma's gericht heeft tegen Nederland en digitale middelen inzet voor (politieke) spionage en sabotage.¹⁴² Er loopt momenteel een uitgebreid inlichtingenonderzoek naar de intenties en handelswijze van Iran.¹⁴³

Een ander voorbeeld van een actor waarover zorgen zijn over ongewenste beïnvloedingsactiviteiten, is Turkije. Turkije voert al jaren een actief diasporabeleid voor eigen politieke doeleinden, ook richting Turkse Nederlanders. Sinds de coup poging in 2016 is het diasporabeleid van Turkije actiever en meer zichtbaar geworden, zoals onder meer waarneembaar werd rondom het Turkse referendum in april 2017.¹⁴⁴ Ook de oproep van de Turkse president Erdogan om te gaan stemmen in de verkiezingen afgelopen jaar, werd door het kabinet bestempeld als ongewenste buitenlandse beïnvloeding.¹⁴⁵

Naast Iran en Turkije, bestaan er ook zorgen rondom landen als Eritrea (het onder dwang innen van diasporabelasting) en Golfstaten (wegens ondoorzichtige financiering van religieuze instellingen) en Noord-Korea (sabotage ICT-infrastructuur).¹⁴⁶ Tot slot moet worden gerealiseerd dat ook westerse actoren tactieken van beïnvloeding en hybride conflictvoering gebruiken, bijvoorbeeld de VS.¹⁴⁷

De verwachting is dat het gebruik van hybride operaties toeneemt, mede door de moeilijkheid van attributie en omdat de mogelijkheden toenemen (met name binnen het cyber/informatiedomein). Dat geldt niet alleen voor het aantal staten dat dit type operaties gebruikt, maar ook de intensiteit. Daarbij moet wel worden aangetekend dat toekomstige ontwikkelingen op dit vlak samenhangen met de binnenlandse politiek van de genoemde staten. Als bijvoorbeeld sprake is van regimewisseling, dan kunnen intenties veranderen, wat zeer zeker zijn effect zal hebben op het uitgevoerde beleid van de betreffende staten.

140 AIVD Jaarverslag 2018, p. 10.

141 Ministerie van Buitenlandse Zaken, (2019), [Kamerbrief over sancties tegen Iran](#), 8 januari 2019.

142 AIVD Jaarverslag 2018, p. 8.

143 AIVD, "[Iran waarschijnlijk betrokken bij liquidaties in Nederland](#)", 8 januari 2019.

144 [Kamerbrief over ongewenste inmenging](#), Tweede Kamer vergaderjaar 2017-2018, 0821 nr. 42.

145 NOS, "[Kabinet: Turkse stemoproep Erdogan ongepast](#)", 15 juni 2018.

146 AIVD Jaarverslag 2018.

147 F.P. van der Putten et al. (red), "Hybrid Conflict", p. 3.

Conclusies

In dit hoofdstuk is het fenomeen ‘hybride conflictvoering’ gebruikt om de gecombineerde actor- dreigingsanalyse testen. Ten eerste is gebleken dat het moeilijk is om alle verschillende manifestaties met elkaar in verband te brengen en te herkennen als onderdeel van een strategie van één actor, wanneer men alleen redeneert vanuit de dreiging. Daarom is het nodig dieper in te gaan op de intenties, capaciteit en gelegenheid van de dreigingsactor. Een voordeel van de actor-centrische benadering is dat door de bredere intenties en strategie van de actor te kennen, inclusief het patroon van het rekruteren en gebruik van proxies, de overige manifestaties ook beter te herkennen zijn als onderdeel van die strategie. Maar tegelijkertijd is, ten tweede, een pure actorbenadering ook niet afdoende. Sommige bedreigingen zijn niet (direct) te herleiden tot een actor, of manifesteren zich via andere (niet-statelijke) actoren. Door te veel op een bepaalde actor te focussen, bestaat het risico dat andere (statelijke en niet-statelijke) actoren over het hoofd worden gezien.

De gecombineerde actor-dreigingsanalyse ondervangt deze analyseproblemen, door de verschillende manifestaties van de dreiging terug te voeren op een moedwillige actor, en daarvan de intentie, het vermogen en de gelegenheid te onderzoeken. Door zowel de actor als de dreiging als startpunt te nemen wordt het complete dreigingspalet zichtbaar, waarmee de ‘*loop*’ weer sluitend wordt gemaakt naar de dreiging en wellicht andere actoren. De gecombineerde dreigings-actoranalyse stelt dus niet alleen in staat om een heel compleet beeld te krijgen, maar ook om verfijning aan te brengen in de dreiging, en de attributie ervan. Ook voorkomt het tot slot een *actorbias*, door ook te kijken naar andere actoren die deze dreiging veroorzaken.

Dit geeft de volgende elementen voor het onderzoekskader:

- In hoeverre geeft een gecombineerde actor- en dreigingsanalyse een completer beeld ten behoeve van onze nationale veiligheid?
- In hoeverre is er een noodzaak om een actueel overzicht op te stellen van dreigingsactoren, zodat die routinematig in de analyse worden meegenomen?
- Hoe kan dit overzicht op systematische wijze tot stand komen en periodiek geactualiseerd worden, inclusief meeweging van een aantal landen en niet-statelijke actoren die misschien in de toekomst boven de drempel van dreigingsactor uit gaan komen?
- Wat zijn de voor- en nadelen van het openbaar maken van dit soort analyses?

5 De percepties, performativiteit, politiek en politeia ten aanzien van grensoverschrijdende veiligheidsvraagstukken

Inleiding

In de vier voorgaande hoofdstukken is ingegaan op de eerste dimensie uit het raamwerk van Eriksson en Rhinard (problemen). In dit hoofdstuk worden de vier overige dimensies beschouwd die een rol spelen bij het onderzoek naar grensoverschrijdende veiligheidsvraagstukken, te weten: de manier waarop en het perspectief van waaruit de vraagstukken worden waargenomen (percepties) door de betrokken beleidsmakers, de inhoudelijke en procesmatige effectiviteit (performativiteit)¹⁴⁸ van het beleid, de politieke context waarbinnen de interdepartementale samenwerking plaatsvindt (politics) en tenslotte de bestuurlijke arrangementen (politeia) die een rol spelen bij de ambtelijke coördinatie van de aanpak van grensoverschrijdende veiligheidsvraagstukken.¹⁴⁹ Op basis van deze, weliswaar beknopte, verkenning zullen aansluitend een aantal vragen worden geformuleerd ten behoeve van een toekomstig onderzoekskader.

Onzekerheid door complexiteit

In de afgelopen decennia is ons denken over interne en externe veiligheid wezenlijk veranderd. Niet langer wordt veiligheid uitsluitend gedefinieerd als de veiligheid van de staat die door de (militaire) macht van een andere mogendheid wordt bedreigd, maar veiligheid kan ook bedreigd worden door politieke, economische, maatschappelijke en klimatologische factoren, al dan niet in hun onderlinge samenhang. Tevens is niet alleen de veiligheid van de staat van belang, maar ook die van het individu, een regio of zelfs de wereld.¹⁵⁰ Zoals al eerder opgemerkt, is de scheidslijn tussen interne en externe veiligheid inmiddels volledig vervaagd.

148 De 'policy' dimensie wordt hier begrepen als 'performativiteit'.

149 Zie voor deze conceptuele indeling J. Eriksson en M. Rhinard, "The Internal-External Security Nexus: Notes on an Emerging Research Agenda", *Cooperation and Conflict* 44 (3) (2009) 243-267.

150 B. Buzan, (1991), *People, States and Fear* (Boulder: Lynne Rienner Publishers).

Om de politieke besluitvorming over en bestuurlijke coördinatie van activiteiten op het gebied van grensoverschrijdende veiligheidsvraagstukken samen te brengen, kennen verschillende landen een Nationale Veiligheidsraad om zo tot een geïntegreerde aanpak van deze complexe dreigingen te komen. Nederland kent een dergelijke raad nog niet, althans niet in formele zin. Wel wordt het idee regelmatig (zowel formeel als informeel) geopperd.¹⁵¹ Vooralsnog heeft deze discussie niet tot de daadwerkelijke oprichting van een Nationale Veiligheidsraad in Nederland geleid.

Door de herdefiniëring van het begrip *nationale veiligheid* spelen op nationaal niveau meerdere delen van de overheid (ministeries, zelfstandige bestuursorganen en agentschappen) een rol in de beleidsaanpak van de verschillende vormen van interne en externe veiligheidsvraagstukken. Deze diversiteit aan politieke en bestuurlijke actoren geeft twee problemen waar iedere grote organisatie mee worstelt. Ten eerste een coördinatieprobleem om de grote verscheidenheid aan departementen, agentschappen, directies, eenheden, etc. in min of meer dezelfde richting te krijgen zonder elkaars werkzaamheden te ondermijnen. En ten tweede een integratie- en organisatieprobleem over hoe de verschillende doelstellingen, culturen en wijzen van aansturing op elkaar afgestemd kunnen worden om interorganisationale samenwerking mogelijk te maken.¹⁵²

De beleidscomplexiteit van de hedendaagse grensoverschrijdende veiligheidsvraagstukken kan verklaard worden door drie soorten onzekerheid: inhoudelijke, strategische en institutionele onzekerheid.¹⁵³ Institutionele onzekerheid ontstaat doordat deelnemende actoren van verschillende organisaties afkomstig zijn. Deze organisaties hebben ieder hun eigen achtergrond voor wat betreft hun taken, procedures, regels, taal, cultuur, mandaat, etc. die niet per se overeenkomen met de institutionele

151 Eerder vond de discussie over een Nationale Veiligheidsraad plaats naar aanleiding van een voorstel van CDA-Tweede Kamerlid De Hoop Scheffer. Hij pleitte in september 2001 voor de oprichting ervan voor de aansturing van een strategie voor de bescherming van de nationale veiligheid tegen nationale en internationale dreigingen (Reformatorisch Dagblad, 19 september 2001). Deze gedachten werden verder uitgewerkt in het CDA-verkiezingsprogramma 2002-2006, waarin een voorstel werd gedaan voor een Nationale Veiligheidsraad als onderraad van de ministerraad. In 2004 kwam het zelfs tot een motie van de Kamerleden Verhagen (CDA), Van Aartsen (VVD) en Herben (LPF), waarin zij pleitten voor de oprichting van een Nationale Veiligheidsraad (Kamerstukken II 2003-2004, 27 925 nr. 124). Deze motie werd met meerderheid van stemmen aangenomen. Zie voor een geschiedenis van deze discussie L.J. Hazelbag, (2015), 'Nationale Veiligheidsraad: politiek wenselijk en staatsrechtelijk haalbaar?', *Militaire Spectator*, 184(4), pp. 184-197. Ook in het WRR-rapport *Veiligheid in een wereld van verbindingen: Een strategische visie op het defensiebeleid* (Den Haag: Wetenschappelijke Raad voor het Regeringsbeleid, 2017) werd aanbevolen een zgn. Algemene Raad voor de Veiligheid (ARV) in te stellen, die de veiligheidsstrategie van de regering kan vormgeven.

152 K. Mulgan, (2005), 'Joined-up Government: Past, Present and Future', in V. Bogdanor (ed.), *Joined-up Government*, (Oxford: Oxford University Press), pp. 175-187.

153 J. Koppenjan & E.H. Klijn, (2004), *Managing Uncertainties in Networks*, (Londen: Routledge).

achtergrond van de andere organisaties. Deze achtergrond is belangrijk omdat dit het gedrag van de actoren in de samenwerking beïnvloedt. Inhoudelijke en strategische onzekerheid ontstaan door de perceptieverschillen van de deelnemende actoren over de aard van het probleem, de oplossing, de doelstelling en de opstelling van de andere actoren. Daarmee zijn percepties dus in grote mate van invloed op de samenwerking tussen actoren.

Perceptieverschillen over problemen

Dat actoren tot hetzelfde coördinatiecluster behoren en op hetzelfde beleidsterrein actief zijn, hoeft nog niet te betekenen dat ze ook dezelfde perceptie over een probleem hebben. Deze perceptie wordt voor een belangrijk deel bepaald door de cultuur van de organisatie. Met andere woorden, de organisatie(cultuur) bepaalt voor een deel de wijze waarop we de wereld om ons heen percipiëren.¹⁵⁴ Indien één organisatie een bepaalde taak moet uitvoeren, hoeft dit niet direct tot problemen te leiden. Dat kan wel het geval zijn indien twee of meerdere organisaties, met verschillende culturen, gezamenlijk aan beleid moeten werken om een probleem aan te pakken. Onderzoekers hebben geconstateerd dat beleidsmakers, politici en academici een verschillende 'taal' gebruiken.¹⁵⁵ De crux van het probleem is dat ieder van de actoren de werkelijkheid vanuit zijn of haar perspectief percipieert en alleen dat deel van de werkelijkheid beziet dat bij de eigen cultuur past. Daarmee is de perceptie over de situatie in een samenwerkingsverband zeer belangrijk. Het geeft namelijk de richting aan waarin de oplossingen worden gezocht en is daarmee van groot belang voor de uitkomsten van het beleidsproces.¹⁵⁶ Door een verschil in perceptie over de aard van het probleem kunnen actoren ook van mening verschillen over hoe dat probleem opgelost moet worden.¹⁵⁷ Kortom, de perceptieverschillen tussen de actoren kunnen betrekking hebben op de aard van het probleem, de oplossing, maar ook op de doelstelling en zelfs het concept van de samenhangende aanpak. Die invloed kent twee kanten. Enerzijds kunnen perceptieverschillen tot controverses leiden waardoor verwacht mag worden dat een overeenkomst in percepties (in het algemeen) de procesperformance ten goede zal komen. Aan de andere kant kunnen de verschillende percepties tot een holistisch beeld van de complexe problematiek leiden en hiermee bijdragen aan een goede inhoudelijke performance. Een goed voorbeeld daarvan is de duiding van het fenomeen 'hybride

154 E.H. Schein, (2010), *Organizational Culture and Leadership*, 4th Edition (New York: Wiley and Sons).

155 J. Gross Stein, (2002), 'Psychological Explanations of International Conflict', in W. Carlsnaes, T. Risse-Kappen & B.A. Simmons (Eds.), *Handbook of International Relations* (Londen: Sage.), pp. 292-308.

156 J. Koppenjan & E.H. Klijn, (2004), *Managing Uncertainties in Networks*, (Londen: Routledge) p. 10.

157 E.E. Duchateau-Polkerman, (2016), 'Hoe perceptie ons veiligheidsgevoel beïnvloedt', in *Militaire Spectator*, 185 (1), pp. 4-18.

dreiging' zoals gegeven door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in een gelijknamige fenomeenstudie uit 2017.¹⁵⁸

Performativiteit van beleid¹⁵⁹

De aanleiding van interdepartementale samenwerking is de (wederzijdse) afhankelijkheid van overheidsactoren om bepaalde beleidsdoelstellingen te kunnen bereiken. De kwaliteit van de samenwerking zou dan ook aan de mate waarin die doelstellingen behaald worden afgemeten kunnen worden. Om een uitspraak over de uitkomsten van de samenwerking te kunnen doen, kan de samenwerking worden getaxeerd op basis van procesperformance en inhoudelijke performance, een indeling die in de literatuur over netwerken en complexe besluitvorming vaker wordt gebruikt.¹⁶⁰ Procesperformance richt zich op het verloop en de kwaliteit van de samenwerking en besluitvorming als proces. Inhoudelijke performance gaat daarentegen in op hetgeen inhoudelijk is bereikt en heeft betrekking op het innovatieve karakter van de samenwerking, de mate waarin actoren hun bijdrage in de uitkomsten herkennen, de mate waarin de problemen door het samenwerkingsverband ook daadwerkelijk worden aangepakt en de mate van samenhang in de gedeelde activiteiten.

'Wicked Problems'

Vanuit een bestuurlijke invalshoek bekeken worden grensoverschrijdende veiligheidsvraagstukken als zogenoemde '*Wicked Problems*' gezien.¹⁶¹ Om dergelijke problemen aan te pakken, zijn meerdere actoren nodig en tussen die actoren is coördinatie noodzakelijk om overlap, duplicatie, lacunes en tegenwerking bij de

158 NCTV, (2017), *Chimaera: een duiding van het fenomeen 'hybride dreiging'*, (Den Haag).

159 In 2010 introduceerde terrorismeonderzoeker Beatrice de Graaf een nieuwe methode om de zogenaamde 'performativiteit' van beleid te meten. Zie hiervoor B. de Graaf, *Theater van de angst: de strijd tegen terrorisme in Nederland, Duitsland, Italië en Amerika* (Amsterdam: Boom, 2010).

160 J. Koppenjan & E.H. Klijn, (2004), *Managing Uncertainties in Networks* (Londen: Routledge); W.J.M. Kickert, E.H. Klijn & J.F.M. Koppenjan, (1997), *Managing Complex Networks: Strategies for the Public Sector*, (Londen: SAGE Publications).

161 In de wetenschappelijke literatuur vertegenwoordigen deze '*Wicked Problems*' een bijzondere klasse van beleidsproblemen: problemen waarvoor geen evidente, geaccepteerde of gezond-verstand-oplossing bestaat, die niet gemakkelijk geduid kunnen worden en die tot de taakstelling van meerdere instituties of organisaties behoren. Problemen ook waarbij externe en interne veiligheid met elkaar versmolten zijn en die een complex van, vaak met elkaar verweven, oorzaken hebben. Zie o.a. M. Clarke & J. Stewart, (1997), *Handling the Wicked Issues: A Challenge for Government* (University of Birmingham: School of Public Policy,) en U.C. Schroeder, (2011), *The Organization of European Security Governance: Internal and External Security in Transition* (Londen: Routledge).

uitvoering van beleid te voorkomen en samenhang te bereiken.¹⁶² Meer en meer wordt onderkend dat grote sociale problemen per definitie in het interorganisatieveld vallen en niet langer door één individuele organisatie of actor kunnen worden opgelost.¹⁶³ Situaties waarin interorganisatiele samenwerkingsverbanden nodig zijn, hebben aan aantal kenmerken¹⁶⁴:

- Verschillende partijen hebben belang bij het oplossen van het probleem en zijn wederzijds van elkaar afhankelijk;
- Er kan een verschillend niveau van expertise en een ongelijkheid in de toegang tot relevante informatie bestaan;
- De bestaande manieren om de problemen op te lossen zijn niet succesvol gebleken;
- De problemen kenmerken zich door complexiteit en onzekerheid.

Er kan een typologie van problemen worden gemaakt op basis van hun complexiteit: dit betreft een onderscheid tussen 'simpele problemen' (er heerst consensus over de probleemdefinitie en de oplossing), 'complexe problemen' (wel consensus over de aard van het probleem, maar niet over de oplossing) en de zogenaamde *Wicked Problems*.¹⁶⁵ Deze kunnen omschreven worden als complexe problemen waar geen vaststaande kennis over voorhanden is en waarvoor geen vaststaande standaarden over hoe de gestelde doelen te bereiken beschikbaar zijn.¹⁶⁶ Kortom: wie het weet mag het zeggen.¹⁶⁷

Een hedendaagse manifestatie van 'Wicked Problems' wordt gevormd door zogenaamde hybride dreigingen, aangezien de aard van dergelijke problemen niet direct duidelijk is en bovendien adaptief en reflexief ingebed in onze pogingen ze te begrijpen en op te lossen.¹⁶⁸ Een analogie die in de literatuur ook wel wordt gemaakt betreft die van puzzels, mysteries en complexe problemen.¹⁶⁹ Al in 1967 werden de beperkingen van het traditionele verkokerde politieke systeem voor wat betreft definitie, bestuur en aanpak van complexe sociale problemen zichtbaar.¹⁷⁰ De omgang met 'Wicked Problems'

162 V. Bogdanor (Eds.), (2005), *Joined-Up Government*, (Oxford: Oxford University Press).

163 B. Gray, (1985), 'Conditions Facilitating Interorganizational Collaboration', in *Human Relations* 38(10), pp. 911-936.

164 B. Gray, (1989), *Collaborating. Finding Common Ground for Multiparty Problems* (San Francisco: Jossey-Bass).

165 N. Roberts, (2000), 'Wicked Problems and Network Approaches to Resolution', in *International Public Management Review* 1(1), pp. 1-19; T. Richey (2007), *Wicked Problems: Structuring Social Messes with Morphological Analysis* (Stockholm: Swedish Morphological Society).

166 APSG, (2007), *Tackling Wicked Problems: A Public Policy Perspective* (Barton: Australian Public Service Commission).

167 J. Koppenjan & E.H. Klijn, (2004), *Managing Uncertainties in Networks* (Londen: Routledge).

168 P. Cullen (2018), *Hybrid Threats as a New 'Wicked Problem' for Early Warning* (Helsinki: Hybrid CoE).

169 D.T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College, 2011), pp. 17-19.

170 C.W. Churchman, (1967), 'Wicked Problems', *Management Science*, 14(4)), pp. 141-142.

stelt bijzondere eisen op het vlak van *Governance*-aandacht vanwege de doorgaans hogere transactiekosten die zijn gemoeid met de noodzakelijke interdepartementale coördinatie.¹⁷¹

De politieke context

Het volgende perspectief richt zich daarmee op de politieke context van de samenwerking. Om een uitspraak over de te prefereren wijze van ambtelijke aansturing en coördinatie te kunnen doen, dient allereerst deze context, waarin de interdepartementale samenwerking zich afspeelt, te worden begrepen. De politieke context die een land kent, beïnvloedt de samenwerking tussen de ministeries op verschillende wijzen. De macht van de regeringsleider en de wijze waarop besluitvorming tot stand komt, wordt grotendeels bepaald door het democratische model. Lijphart onderscheidt twee standaardmodellen: het consensusmodel en het meerderheids- of Westminster-model.¹⁷² Het consensusmodel kenmerkt zich door een meerpartijstelsel waarbij geen van de partijen de meerderheid van het parlement kan behalen. Voor regeringsvorming is dus altijd een coalitie van twee of meer partijen noodzakelijk, waarbij deze partijen de macht moeten delen.

Deze eigenschappen zijn op de interdepartementale samenwerking van invloed daar ze bepalen in welke mate ministers (soms inclusief de premier) van elkaar afhankelijk zijn om tot besluitvorming te kunnen komen, maar ook op de mate waarin een premier zijn ministers tot samenwerking kan 'dwingen'. Van het meerderheidsmodel mag verwacht worden dat de premier veel macht heeft en dat de samenwerking meer verticaal gecoördineerd wordt terwijl in het consensusmodel er meer horizontaal gecoördineerd wordt. Dit maakt het kabinet een collectief besluitvormingsorgaan waarbij de ministers integraal voor de genomen besluiten verantwoordelijk zijn, ook indien deze niet hun departementen betreffen.¹⁷³

Ten slotte draagt het non-interventiebeginsel (de ongeschreven regel dat een minister zich alleen met zijn eigen departement bemoeit en niet met dat van een collega-minister) eraan bij dat een minister zich vooral op zijn eigen departement richt. Dit beginsel heeft niet alleen betrekking op de omgangsvormen tussen bewindslieden, maar heeft ook

171 M. Weber (1947), *The Theory of Social and Economic Organizations* (New York: Free Press); O. Williamson (1979), 'Transaction-cost Economics: The Governance of Contractual Relations', in *Journal of Law and Economics* 22, pp. 233-261; O. Williamson (1986), 'The Governance of Contractual Relations', in J. Barney & W. Ouchi (Eds.), *Organizational Economics* (San Francisco: Jossey-Brass), pp. 98-129.

172 A. Lijphart (1999), *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries* (New Haven: Yale University Press).

173 Voor de Nederlandse situatie is dit vastgelegd in artikel 45, lid 3 van de Grondwet.

een meer strategisch karakter. Door zich niet met het beleid van een ander te bemoeien beschermt de minister zijn eigen autonomie. Immers, derden zullen zich door het beginsel ook niet met zijn beleidsterrein bemoeien.¹⁷⁴

Om de meestal overvolle kabinetsagenda te ontlasten, worden in Nederland onderwerpen naar de zogenaamde onderraden gedelegeerd. In deze fora worden specifieke delen van het regeringsbeleid besproken, daarom zijn alleen de betrokken bewindslieden aanwezig. In de onderraden zullen de ministers zich wel met het regeringsbeleid bemoeien, daar dit ook op hun departement betrekking heeft. De onderraden zijn bij uitstek geschikte mechanismen om beleid te coördineren, beslissingen te nemen en conflicten tussen departementen op te lossen. Daarnaast komen departementale autonomie en collectieve besluitvorming in de onderraden samen.

Tabel 8 Overzicht stelsel onderraden en ministeriële commissies

Onderraden en ministeriële overlegorganen in de huidige kabinetsperiode ¹⁷⁵
Onderraden
Raad Werk, Inkomen, Zorg en Onderwijs (RWIZO)
Raad Financiële en Economische Zaken, Infrastructuur en Landbouw (RFEZIL)
Raad Bestuur en Justitie (RBJ)
Raad Veiligheid en Inlichtingen (RVI)
Raad voor Koninkrijksrelaties (RKR)
Raad Defensie en Internationale Aangelegenheden (RDIA)
Raad Europese Aangelegenheden (REA)
Ministeriële overlegorganen
Ministeriële Kerngroep Speciale Operaties (MKSO)
Ministeriële Commissie Vliegkamp Oekraïne (MCVO)
Ministeriële Commissie Wederopbouw Bovenwinden (MCWB)
Ministeriële Commissie Klimaat en Energie (MCKE)
Ministeriële Commissie Regionale Samenwerking (MCRS)
Ministeriële Commissie Economie en Veiligheid (MCEV)

Gecomplexeerde en meer technische onderwerpen worden op deze wijze nooit direct besproken in de ministerraad. Deze onderwerpen worden eerst behandeld in een specifieke onderraad door de ministers die er direct bij betrokken zijn.

174 R.B. Andeweg, "Ministers as Double Agents? The Delegation Process Between Cabinet and Ministers", *European Journal of Political Research* 37 (2000) 337-395.

175 Overzicht stelsel van onderraden en ministeriële commissies, Staatscourant Nr. 74580, 29 december 2017, Ministerie van Algemene Zaken.

Over het algemeen gelden voor de onderraden dezelfde regels als voor de ministerraad. De minister-president zit ook de vergaderingen van onderraden voor. Naast de onderraden zijn er ook enkele ministeriële overlegorganen. Het belangrijkste verschil met onderraden is dat deze overlegorganen of commissies tijdelijk zijn, in principe voor de duur van de kabinetsperiode. Ministeriële commissies worden gevormd voor een bepaald thema of onderwerp. De minister-president is ook hier de voorzitter.¹⁷⁶

Voor alle aspecten met betrekking tot de nationale veiligheid geldt dat een effectieve beleidsaanpak sterk afhangt van de mate waarin Nederland goed en vroegtijdig op de hoogte is van ontwikkelingen.¹⁷⁷ De Inlichtingen- en Veiligheidsdiensten spelen daarbij dan ook vanzelfsprekend een belangrijke rol. Bij zowel actualiteiten als beleid ten aanzien van nationale (en internationale) veiligheid neemt de Raad Veiligheid en Inlichtingen (RVI) als onderraad van de ministerraad daarom een belangrijke plaats in. De minister-president is zoals gezegd voorzitter van de RVI en de ministers van Binnenlandse Zaken en Koninkrijksrelaties, Defensie, Buitenlandse Zaken en Justitie en Veiligheid nemen deel aan de wekelijkse bijeenkomsten.

Ambtelijke voorportalen spelen een cruciale rol bij de coördinatie. In deze interdepartementale fora worden de activiteiten gecoördineerd en besluitvorming geïntegreerd voorbereid. Zo vindt de hoog-ambtelijke voorbereiding van de RVI plaats in de Commissie Veiligheids- en Inlichtingendiensten Nederland (CVIN), onder secretariaat van een Raadadviseur van het Ministerie van Algemene Zaken. Zowel de NCTV als de Directeur-Generaal van de AIVD en Directeur van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de Commandant der Strijdkrachten (CDS), de Korpschef van de Nationale Politie en indien nodig de Voorzitter van het College van Procureurs-Generaal zijn in dit forum betrokken.¹⁷⁸ Hierdoor wordt in de RVI op politiek niveau een koppeling gemaakt tussen vrijwel alle interne en externe veiligheidsvraagstukken, echter behalve de vraagstukken op het gebied van economische veiligheid.

Sinds 2019 kent Nederland een Ministeriële Commissie Economie en Veiligheid (MCEV), waarmee voor het eerst de koppeling is gemaakt tussen deze twee beleidsthema's.¹⁷⁹ Omdat economische veiligheid samen met de internationale rechtsorde, territoriale, fysieke, ecologische veiligheid en sociale en politieke stabiliteit geldt als één van de zes

176 Zie *Het blauwe boek: handboek voor bewindspersonen* (Rijksoverheid, april 2019), <https://www.rijksoverheid.nl/documenten/richtlijnen/2017/10/03/handboek-voor-bewindspersonen>

177 Hierbij is een belangrijke rol weggelegd voor kennisinstellingen, zoals de denktanks, enerzijds in het verband van het Analistenennetwerk Nationale Veiligheid (ANV), anderzijds in het verband van het meerjarige onderzoek ten behoeve van de ministeries van Buitenlandse Zaken en Defensie op het gebied van Strategic Foresight & Monitoring (Progress).

178 Overzicht stelsel van onderraden en ministeriële commissies, Staatscourant Nr. 74580, 29 december 2017, Ministerie van Algemene Zaken.

179 Het bijbehorende ambtelijke voorportaal is de Ambtelijke Commissie Economie en Veiligheid (ACEV).

ationale veiligheidsbelangen, is dit op zich niet meer dan logisch. Wel betreft het hier voorsnog een tijdelijk, van de RVI gescheiden opererend overlegorgaan tussen m.n. de ministers van Economische Zaken en Justitie en Veiligheid.

De Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) uit 2017 schrijft voor dat alle onderwerpen van onderzoek voor de AIVD en MIVD worden aangewezen in de vorm van een regeringsbesluit, de zogenoemde Geïntegreerde Aanwijzing Inlichtingen en Veiligheid (GA I&V). Het proces van het tot stand brengen van deze integrale behoeftestelling ten aanzien van de nationale en internationale veiligheid staat onder leiding van de Secretaris-Generaal van het ministerie van Algemene Zaken, tevens Coördinator Inlichtingen- en Veiligheidsdiensten. Het aantal behoeftestellers is momenteel beperkt tot de leden van de RVI, t.w. de ministeries van Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Defensie en Justitie en Veiligheid. Het ministerie van Justitie en Veiligheid wordt bij de formulering van de GA I&V *de facto* vertegenwoordigd door de NCTV.¹⁸⁰ Ook hier geldt dus dat de minister van Economische Zaken, ondanks het gegeven dat economische veiligheid inmiddels als één van de zes nationale veiligheidsbelangen is benoemd, voorsnog niet als formele behoeftesteller geldt van de twee diensten.

Verticale coördinatie

De verticale indeling in hiërarchische niveaus is kenmerkend voor publieke organisaties.¹⁸¹ Door dit gegeven zullen ambtenaren zich allereerst richten op het behalen van de doelstellingen van hun meerderen (in de eigen organisatie) en niet zozeer op de doelstellingen van andere organisaties of gedeelde doelstellingen. Dit feit heeft een sterk verkokerend effect, werkt departementalisme, bureaupolitiek en silomentaliteit in de hand en bemoeilijkt de interdepartementale samenwerking doordat effectieve prikkels daarvoor ontbreken.¹⁸²

De verticale ambtelijke coördinatie kent zowel een *bottom-up* richting, waarbij de informatie van lagere niveaus bijeenkomt en geïntegreerd moet worden, als een *top-down* richting waarin de besluiten van het politieke niveau aan de ministeries en overheidsdiensten worden overgedragen. Samenwerking en coördinatie tussen departementen vindt op verschillende bestuurlijke niveaus plaats, van het laagste niveau waar beleidsmedewerkers met elkaar overleggen, tot uiteindelijk het politieke en

180 Geïntegreerde Aanwijzing Inlichtingen en Veiligheid 2019-2022, Staatscourant Nr. 68088, 4 december 2018, Ministerie van Algemene Zaken.

181 M.A.P. Bovens, P. 't Hart & M.J.W. van Twist, (2007), *Openbaar bestuur: beleid, organisatie en politiek* (Alphen aan de Rijn: Kluwer).

182 B.G. Peters (1998), 'Managing Horizontal Government: The Politics of Co-ordination', in *Public Administration*, 76, pp. 295-311.

hoogste ambtelijke niveau. Op ieder niveau worden beslissingen genomen, afhankelijk van het mandaat en de te bereiken overeenstemming. Het mes van een gelaagde horizontale afstemming en samenwerking snijdt hier aan twee kanten. Enerzijds zorgt het ervoor dat het hogere niveau niet wordt (over)belast met beslissingen die ook op een lager niveau genomen kunnen worden en anderzijds dient het hogere niveau als escalatieniveau indien men op een lager niveau niet tot overeenstemming komt. Op hoog ambtelijk niveau geldt het politieke niveau als het ultieme escalatieniveau.¹⁸³

Er kunnen verschillende varianten van verticale aansturing worden onderkend. De meest voor de hand liggende variant is de coördinatie door de hoogste politieke bewindspersoon, zoals de premier. Waar de regeringsleider niet in staat is om al het regeringsbeleid te overzien, kan hij voor de coördinatie ondersteund worden door een staf of bureau. Maar de coördinatie kan ook naar een specifiek aangewezen actor worden gedelegeerd. Deze actor is dan namens de regeringsleider verantwoordelijk voor de coördinatie van de interdepartementale samenwerking. Het kabinet is na de regeringsleider het meest voor de hand liggende orgaan om interdepartementaal beleid te coördineren. Echter, in de praktijk is het kabinet veelal te groot voor effectieve coördinatie, hebben ministers te weinig tijd om zich met 'andermans' zaken bezig te houden en verwordt het kabinet tot de plaats waar ministers hun departementale beleid, budget en belangen tegenover de andere ministers verdedigen, terwijl de daadwerkelijke besluiten in andere ambtelijke arena's zijn genomen. Een onderraad waar een specifiek te coördineren beleidsterrein wordt behandeld, kan deze kritiek ondervangen. Het nadeel van dit systeem is dat de grenzen van beleid, en daarmee van de verantwoordelijkheden van de onderraad, zelden duidelijk zijn te trekken. En dit vereist dan weer coördinatie tussen de onderraden. De politieke structuur van gespecialiseerde ministeries kan samenwerking met andere departementen daarenboven bemoeilijken doordat ministeries zich meer op zichzelf en de eigen doelstellingen richten dan op gedeelde problemen en doelen.¹⁸⁴ In het zogenoemde bureaupolitieke model komt de uitkomst van de samenwerking tot stand door het 'duwen en trekken' tussen actoren, waarbij deze uitkomsten worden bepaald en beïnvloed door de concurrerende belangen van de actoren.¹⁸⁵ Ondanks een gedeeld regeerakkoord kunnen de belangen van de departementen (sterk) uiteen lopen. Dit kan weer een hindernis voor de interdepartementale samenwerking zijn. De gemene deler is dus dat naast verticale

183 Zie voor een uitgebreide verhandeling over *Wicked Problems*, horizontale en verticale coördinatie, hoofdstuk 3 (Theorie) van het proefschrift van L.J. Hazelbag over interdepartementale samenwerking in Nederland en het Verenigd Koninkrijk uit 2016 (Erasmus Universiteit Rotterdam) 60-95.

184 C. Hood (2005), 'The Idea of Joined-up Government: A Historical Perspective', in V. Bogdanor (Eds.), *Joined-up Government*, (Oxford: Oxford University Press), pp. 12-37.

185 G. Allison & P. Zelikow (1999), *Essence of Decision: Explaining the Cuban Missile Crisis*, (New York: Addison Wesley Longman).

coördinatie de nadruk ook op horizontale coördinatie tussen de diverse delen van het openbaar bestuur moet liggen.¹⁸⁶

Horizontale coördinatie

Horizontale coördinatie doelt op de afstemming van activiteiten aangaande een bepaald beleidsterrein tussen actoren op hetzelfde bestuursniveau.¹⁸⁷ Voor deze coördinatie zijn diverse motieven te noemen, maar de gemene deler van de motieven is het gegeven dat organisaties elkaar nodig hebben om complexe problemen op te kunnen lossen.¹⁸⁸ Alleen door samenwerking kunnen deze problemen (*Wicked Problems*) effectief worden aangepakt.

Zoals traditionele structuren niet voldoen om met de huidige complexe problemen om te kunnen gaan, voldoet ook traditionele aansturing niet om de vereiste samenwerking aan te sturen. Horizontale samenwerking kenmerkt zich namelijk door de afwezigheid van duidelijke hiërarchische verhoudingen. Daarom dient de samenwerking op een meer *Governance*-achtige wijze te worden aangestuurd. Daarbij zijn drie hoofdvormen van coördinatie te onderscheiden: gemeenschappelijke coördinatie, coördinatie door een centrale actor en coördinatie door een externe actor. De nadruk ligt in alle gevallen op horizontale sturing om meer draagvlak onder de deelnemers te creëren, een beter gebruik van kennis om aan kwaliteit te winnen, het vroegtijdig betrekken van deelnemers om aan legitimiteit te winnen en andere actoren eerder bij besluitvorming te betrekken. Dit om een gemeenschappelijke visie te ontwikkelen om vervolgens perceptieverschillen te kunnen overbruggen en onzekerheid te verminderen.¹⁸⁹ Welke actor de autoriteit en de mogelijkheid heeft om als coördinator te fungeren, wordt vooral bepaald door zijn strategische positie en de heersende regels binnen het samenwerkingsverband.

Ten aanzien van de coördinatie van interorganisatorische samenwerking zijn er verschillende organisatorische arrangementen denkbaar, zoals stuurgroepen, *taskforces*, werkgroepen, etc.¹⁹⁰ Hiermee kan op departementaal niveau de coördinatie worden

186 T. Christensen & P. Lægreid (2006), *The Whole-of-Government Approach*, (Stein Rokkan Centre for Social Studies Working Paper).

187 G. Bouckaert, B.G. Peters & K. Verhoest (2010), 'The Coordination of Public Sector Organizations', in B.G. Peters & G. Bouckaert (Eds.), *Shifting Patterns of Public Management*, (Hampshire: Palgrave MacMillan).

188 W.J.M. Kickert, E.H. Klijn & J.F.M. Koppenjan (1997), *Managing Complex Networks: Strategies for the Public Sector* (Londen: SAGE Publications).

189 J. Koppenjan & E.H. Klijn (2004), *Managing Uncertainties in Networks*, (Londen: Routledge) p. 108.

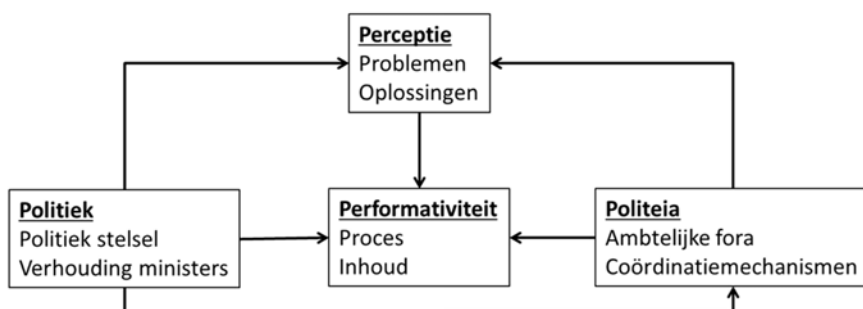
190 B. Steijn, E.H. Klijn & J. Edelenbos (2010), 'The Impact of Network Management on Outcomes in Governance Networks', *Public Administration*, 88(4), pp. 1063-1082.

vergemakkelijkt.¹⁹¹ Zo kunnen experts van andere ministeries in een stuurgroep worden opgenomen die de bewindspersoon van dat departement over beleid van de ander kan informeren en adviseren. Daarnaast kunnen een aantal departementen gezamenlijk een interdepartementale eenheid oprichten die de coördinatie tussen de departementen moet faciliteren en vereenvoudigen. Ook kunnen *taskforces* en werkgroepen worden opgericht waarin functionarissen van verschillende departementen gezamenlijk aan een beleidsterrein werken. Een laatste variant zijn interdepartementale commissies die als koppelorgaan tussen departementen kunnen dienen. In alle gevallen vraagt dit om werkwijzen om informatie uit te wisselen, tot een gemeenschappelijk beeld van een situatie te komen of in ieder geval eenieders perspectief op de situatie aan bod te laten komen.

Van theorie naar onderzoek

In de voorgaande paragrafen zijn achtereenvolgens de perceptieverschillen over problemen, de performativiteit van het beleid, de politieke context en de aspecten van verticale en horizontale coördinatie besproken. Met deze vier dimensies, samen te vatten als percepties, performativiteit, politiek en politeia, is het mogelijk een analysekader te maken. In dit analysekader zijn door pijlen tussen de variabelen de onderlinge relaties aangegeven. Zij bepalen uiteindelijk in hun onderlinge samenhang hoe effectief nationale overheden reageren op grensoverschrijdende veiligheidsvraagstukken. Het kan daarmee als bril dienen om naar de interdepartementale samenwerking in Nederland te kijken.

Figuur 4 Analysekader voor het onderzoek naar grensoverschrijdende veiligheidsvraagstukken



191 B.G. Peters (1998), 'Managing Horizontal Government: The Politics of Co-ordination', in *Public Administration*, 76, pp. 295-311.

Op basis van dit analysekader zijn de volgende deelvragen te formuleren om het onderzoek op het gebied van grensoverschrijdende veiligheidsvraagstukken in de toekomst mee vorm te geven:

- Welke invloed hebben de verschillende percepties over de aard van het probleem, de aanpak ervan en de beleidsdoelstelling op de interdepartementale samenwerking ten aanzien van grensoverschrijdende veiligheidsvraagstukken?
- Wat is de politieke context waarbinnen de interdepartementale samenwerking op het gebied van grensoverschrijdende veiligheidsvraagstukken plaatsvindt en wat is de impact hiervan op de effectiviteit van het beleid?
- Hoe is de aansturing, onderverdeeld in ambtelijk leiderschap en coördinatie-mechanismen, ten aanzien van grensoverschrijdende veiligheidsvraagstukken georganiseerd en wat is de impact hiervan op de doelmatigheid van het beleid?
- Hoe kan de aansturing, onderverdeeld in ambtelijk leiderschap en coördinatie-mechanismen, ten aanzien van grensoverschrijdende veiligheidsvraagstukken doelmatiger worden georganiseerd?
- Wat zijn de bepalende factoren van de proces- en de inhoudelijke performance van de interdepartementale samenwerking t.a.v. grensoverschrijdende veiligheidsvraagstukken en wat is de impact hiervan op de tijdigheid van het beleid?
- Wat is de invloed van de politieke context, de percepties over de aard van het probleem, de aanpak en de doelstelling, alsmede de ambtelijke aansturing en coördinatie op de proces- en de inhoudelijke performance van de interdepartementale samenwerking op het gebied van grensoverschrijdende veiligheidsvraagstukken?

6 Verbondenheid in veiligheid: contouren van een gemeenschappelijke onderzoeksagenda

In dit concluderende hoofdstuk vatten we de bevindingen van ons verkennende onderzoek samen en schetsen we de contouren van een gemeenschappelijke onderzoeksagenda voor de drie betrokken departementen op het gebied van de nexus tussen interne en externe veiligheidsvraagstukken. We sluiten af met een aanvullende richting voor toekomstig onderzoek.

In een poging de nexus tussen interne en externe veiligheidsvraagstukken te conceptualiseren en te komen tot een wetenschappelijke onderzoeksagenda op het vlak van deze grensoverschrijdende vraagstukken, stelden de Zweden Eriksson en Rhinard al in 2009 voor om vijf dimensies van elkaar te onderscheiden, te weten: *problems, perceptions, policies, politics* en *polity*. De problemen betreffen in dit verband de grensoverschrijdende veiligheidsvraagstukken die relevant zijn voor de nationale veiligheid, evenals de wijze van analyse ervan. De overige vier hebben te maken met respectievelijk de manier waarop en het perspectief van waaruit deze vraagstukken worden waargenomen door de betrokken beleidsmakers, met de inhoudelijke en procesmatige effectiviteit van het gevoerde beleid, met de politieke context waarbinnen interdepartementale samenwerking plaatsvindt en met de bestuurlijke arrangementen die een rol spelen bij de ambtelijke coördinatie van de aanpak van grensoverschrijdende veiligheidsvraagstukken.¹⁹²

Onder de dimensie 'problemen' is onder meer gekeken naar de ontwikkeling van het veiligheidsconcept en op welke wijze gedacht wordt over de 'nexus interne en externe veiligheid'. Er is relatief weinig aandacht in de academische literatuur voor de 'nexus interne en externe veiligheid' of synoniemen daarvan (bijvoorbeeld: *transborder threats, transboundary, inside-out/outside-in threats*). Er is duidelijk nog een zoektocht gaande naar de ontwarring en conceptualisering van de verschillende termen en definities die de dynamiek van veiligheid in een nieuwe fase van globalisering kan vatten. Veel houvast biedt de huidige literatuur hier niet voor. Een nieuwe terminologie en een nieuw

192 J. Eriksson en M. Rhinard, "The Internal-External Security Nexus: Notes on an Emerging Research Agenda", *Cooperation and Conflict* 44 (3) (2009) 243-267.

veiligheidsparadigma lijken nodig om de grenzeloosheid van veiligheidsvraagstukken beter te kunnen omschrijven en bevatten. De relatie tussen globalisering en veiligheid is een zeer hechte. Toch lijkt dit nog niet systematisch onderzocht en is de aard van deze relatie nog onvoldoende in kaart gebracht. Alle parameters wijzen erop dat Nederland een sterk 'geglobaliseerd' land is. Inzicht in hoe de connecties tussen de Nederlandse samenleving in brede zin en globalisering effect hebben op onze veiligheid zou kunnen helpen de weerbaarheid uit te bouwen. Dit leidt tot de volgende suggesties als onderdeel van een onderzoekskader:

- De 'interne en externe veiligheidsnexus' is nog een relatieve black box: verder onderzoek is nodig om te bepalen of het zinvol is het narratief van 'binnen' en 'buiten' in relatie tot veiligheid te behouden. Als dit niet of beperkt het geval is, hoe conceptualiseren we dan het nieuwe veiligheidsparadigma?
- Kennis over '*whole of government*', '*whole of society*' (maatschappijbrede) benaderingen vergroten.
- In de keten belangen-preventie-dreigingen-weerbaarheid, zijn de preventieve maatregelenkant en de weerbaarheidzijde nog onderontwikkeld en behoeven meer conceptualisering. Hierbij moet ook veel meer aan *early warning*, preventieve maatregelen en weerbaarheid in internationale samenwerkingsverbanden worden gedacht.
- Aandacht voor de subjectiviteit van dreigingen en de verschillen in percepties tussen de elite en het brede publiek (draagvlakprobleem).
- Digitalisering, robotisering, kunstmatige intelligentie, de *internet of things* en 3D *printing* zullen verder onze wijze van produceren, werken, mobiliteit en consumeren sterk veranderen. Het is daarom belangrijk beter te begrijpen op welke wijze deze nieuwe fase van globalisering onze veiligheid in brede zin verder gaat beïnvloeden.
- Verder ontwikkelen van een ordeningskader (bijvoorbeeld in termen van een 'transportband') om de belangrijkste connecties tussen interne en externe veiligheid inzichtelijk te maken. Met een dergelijk ordeningskader kan de Nederlandse kwetsbaarheid voor dreigingen die deze connecties met zich meebrengen in kaart worden gebracht zodat de weerbaarheid kan worden versterkt.

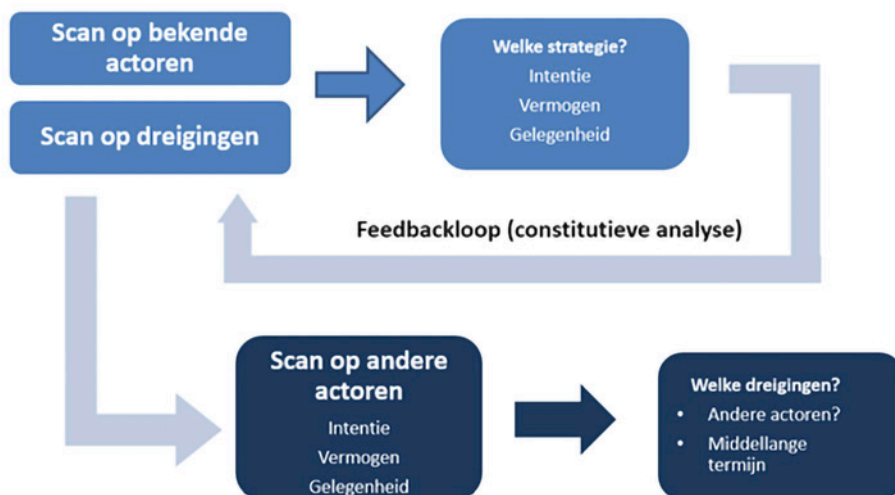
In hoofdstuk twee is een overzicht gegeven van de belangrijkste grensoverschrijdende dreigingen die genoemd worden in Nederlandse risicoanalyses, beleidsnota's en strategieën. In de meeste gevallen wordt uitgegaan van de dreiging, en niet van (specifieke) dreigingsactoren. De recent verschenen Kamerbrief Tegengaan statelijke dreigingen uit april 2019 is hierop een belangrijke uitzondering. Hierin worden, zonder expliciet bepaalde staten te noemen, de dreigingen en risico's benoemd die uitgaan van statelijke actoren en die potentieel een ondermijnend effect kunnen hebben op de rechtstaat en op de openheid en stabiliteit van de Nederlandse samenleving. Denk hierbij aan: digitale dreigingen, economische dreigingen, ongewenste buitenlandse beïnvloeding en afhankelijkheid van nieuwe technologieën. Ook binnen andere risicoanalyses (in bijvoorbeeld de GRA en het Meerjarig perspectief krijgsmacht) is er een verandering zichtbaar, in de zin dat de dreigingsactor vaker expliciet wordt

benoemd. In deze documenten wordt bijvoorbeeld verwezen naar Rusland en China als dreigingsactoren. Dit is echter wel iets anders dan een (volledige) actoranalyse, omdat hier niet naar de actor in zijn geheel wordt gekeken, met de daarbij behorende capaciteiten, intenties en gelegenheid.

Ditzelfde geldt ook voor de risicoanalyses voor de overzeese gebieden, waarin met name de dreigingen worden benoemd. Als er al een actor wordt benoemd (bijv. Venezuela), dan wordt niet naar het volledige palet aan dreigingen gekeken dat van deze actor uitgaat. Het is tot slot belangrijk om te melden dat er geen complete risicoanalyse voor het Caribisch gedeelte van het Koninkrijk bestaat, terwijl deze gebieden te stellen hebben met een heel ander pakket aan grensoverschrijdende dreigingen dan het Europese deel.

Het volgende hoofdstuk (3) heeft een beknopt overzicht gegeven van hoe in Nederland risicoanalyses worden gedaan ten behoeve van de nationale veiligheid. De gebruikte methoden zijn in een beperkt internationaal perspectief geplaatst en een aantal problemen van de huidige methodiek zijn geïdentificeerd. Een gecombineerde actor- en dreigingscentrische benadering kan een aantal van deze problemen adresseren en is een interessante richting waarnaar meer onderzoek benodigd is. Het vertrekpunt van de analyse is hierbij niet alleen de dreiging, ook niet alleen de actor, maar **beide**. Door de onderstaande stappen te doorlopen wordt *actorbias* voorkomen en worden ook dreigingen waarvan de oorsprong onduidelijk is, voldoende verdisconteerd.

Figuur 5 De gecombineerde actor- en dreigingsanalyse



Daarnaast blijven er een aantal vragen over:

- Hoe kunnen we de complexe dreigingsomgeving zo weergeven dat het onderzoekbaar en repliceerbaar is, maar dat ook de complexe dwarsverbanden en verwevenheid goed in beeld worden gebracht?
- Welke lessen zijn er te leren van de praktijk van risicoanalyses van andere landen?
 - Een comparatieve landenstudie naar *best practices* op het gebied van methoden van risico-analyses. Het interessantst zou zijn om toonaangevende veiligheidspartners te onderzoeken, zoals het VK, VS, en Frankrijk, maar ook landen van vergelijkbare grootte, zoals bijvoorbeeld Canada, Finland, Zweden en Australië.
- Hoe kan weerbaarheid ten opzichte van een dreiging worden gedefinieerd en hoe gaan we om met leereffecten van dreigingen op de calculatie van weerbaarheid?
- Op welke wijze kunnen we zinvol prioriteren tussen dreigingen en gevaren (*security- en safety-fenomenen*)?
- Op welke wijze kan Nederland zich beter voorbereiden op '*unknown unknowns*'?
- Nader onderzoek naar de 'internationale rechtsorde' als vitaal belang van Nederland. Is het terecht en verstandig dat dit als vitaal belang wordt bestempeld, wat is precies onderdeel van dit belang (in hoeverre bijvoorbeeld mensenrechten worden meegewogen en of het internationaal-financieel economisch stelsel er ook deel van uitmaakt)? Hoe gaan andere landen hiermee om? Welke gevolgen heeft het besluit van de SNV om het als zesde belang toe te voegen voor de Nederlandse positionering in het internationale krachtenveld? Hoe verhoudt dit vitale belang zich tot de buitenland- en veiligheidsbeleidsagenda van Nederland?

Deze analyse van de dreigingsanalyses wordt in hoofdstuk 4 gevolgd door een test van de 'gecombineerde actor- en dreigingsanalyse' aan de hand van hybride dreigingen. Ten eerste is gebleken dat het moeilijk is om alle verschillende manifestaties met elkaar in verband te brengen en te herkennen als onderdeel van een strategie van één actor, wanneer men alleen redeneert vanuit de dreiging. Daarom is het nodig dieper in te gaan op de intenties, capaciteit en gelegenheid van de dreigingsactor. Een voordeel van de actor-centrische benadering is dat door de bredere intenties en strategie van de actor te kennen, inclusief het patroon van rekruteren en het gebruik van proxies, de overige manifestaties ook beter te herkennen zijn als onderdeel van die strategie. Maar tegelijkertijd is, ten tweede, een pure actorbenadering ook niet afdoende. Sommige bedreigingen zijn niet (direct) te herleiden tot een actor, of manifesteren zich via andere (niet-statelijke) actoren. Door te veel op een bepaalde actor te focussen, bestaat het risico dat andere (statelijke en niet-statelijke) actoren over het hoofd worden gezien.

De gecombineerde actor-dreigingsanalyse ondervangt deze analyseproblemen, door de verschillende manifestaties van de dreiging terug te voeren op een moedwillige actor, en daarvan de intentie, vermogen en gelegenheid te onderzoeken. Door zowel de actor als de dreiging als startpunt te nemen wordt het complete dreigingspalet

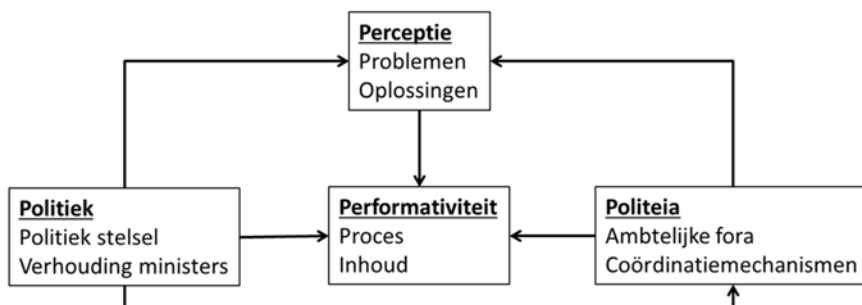
zichtbaar, waarmee de 'loop' weer sluitend wordt gemaakt naar de dreiging en wellicht andere actoren. De gecombineerde actor- en dreigingsanalyse geeft dus niet alleen een completer beeld, maar brengt ook verfijning aan in de dreiging, en de attributie ervan. Ook voorkomt het tot slot een *actorbias*, door eveneens te kijken naar andere actoren die deze dreiging veroorzaken.

Dit geeft uit de hoofdstukken 3 en 4 de volgende elementen voor het onderzoekskader:

- In hoeverre geeft een gecombineerde actor- en dreigingsanalyse een completer beeld ten behoeve van onze nationale veiligheid?
- In hoeverre is er een noodzaak om een actueel overzicht op te stellen van dreigingsactoren, zodat die routinematig in de analyse worden meegenomen?
- Hoe kan dit overzicht op systematische wijze tot stand komen en periodiek geactualiseerd worden, inclusief meeweging van een aantal landen en niet-statelijke actoren die misschien in de toekomst boven de drempel van dreigingsactor uit gaan komen?
- Wat zijn de voor- en nadelen van het openbaar maken van dit soort analyses?

In hoofdstuk 5 zijn tenslotte achtereenvolgens de perceptieverschillen over problemen, de performativiteit van het beleid, de politieke context en de aspecten van verticale en horizontale coördinatie besproken. Met deze vier dimensies, samen te vatten als percepties, performativiteit, politiek en politeia, is het mogelijk een analysekader te maken. In dit analysekader (zie hieronder) zijn door pijlen tussen de variabelen de onderlinge relaties aangegeven. Zij bepalen uiteindelijk in hun onderlinge samenhang hoe effectief nationale overheden reageren op grensoverschrijdende veiligheidsvraagstukken. Het kan daarmee als bril dienen om naar de interdepartementale samenwerking in Nederland te kijken.

Figuur 6 Analyse kader voor het onderzoek naar grensoverschrijdende veiligheidsvraagstukken



Op basis van dit analysekader zijn de volgende deelvragen te formuleren om het onderzoek op het gebied van grensoverschrijdende veiligheidsvraagstukken in de toekomst mee vorm te geven:

- Welke invloed hebben de verschillende percepties over de aard van het probleem, de aanpak ervan en de beleidsdoelstelling op de interdepartementale samenwerking ten aanzien van grensoverschrijdende veiligheidsvraagstukken?
- Wat is de politieke context waarbinnen de interdepartementale samenwerking op het gebied van grensoverschrijdende veiligheidsvraagstukken plaatsvindt en wat is de impact hiervan op de effectiviteit van het beleid?
- Hoe is de aansturing, onderverdeeld in ambtelijk leiderschap en coördinatie-mechanismen, ten aanzien van grensoverschrijdende veiligheidsvraagstukken georganiseerd en wat is de impact hiervan op de doelmatigheid van het beleid? Hoe kan de aansturing, onderverdeeld in ambtelijk leiderschap en coördinatie-mechanismen, ten aanzien van grensoverschrijdende veiligheidsvraagstukken doelmatiger worden georganiseerd?
- Wat zijn de bepalende factoren van de proces- en de inhoudelijke performance van de interdepartementale samenwerking t.a.v. grensoverschrijdende veiligheidsvraagstukken en wat is de impact hiervan op de tijdigheid van het beleid?
- Wat is de invloed van de politieke context, de percepties over de aard van het probleem, de aanpak en de doelstelling, alsmede de ambtelijke aansturing en coördinatie op de proces- en de inhoudelijke performance van de interdepartementale samenwerking op het gebied van grensoverschrijdende veiligheidsvraagstukken?

De hoge complexiteit van de hedendaagse dreigingen en de wijze waarop ze de interne en externe domeinen van nationale veiligheid omspannen, moet zoals gezegd allereerst goed worden begrepen alvorens we de effecten ervan op het beleid, de percepties van beleidsmakers, de politieke context en de wijze van bestuur kunnen onderzoeken. Wij stellen tenslotte nog een aanvullende richting voor die zich leent voor mogelijk toekomstig onderzoek. Dit betreft het geaggregeerde effect van de vijf te onderscheiden dimensies op het gedrag van nationale overheden ten aanzien van *internationale samenwerking*. Afhankelijk van de dynamiek tussen problemen, percepties, performativiteit, politiek en politiea kan dit overheidsgedrag volgens Eriksson en Rhinard vier ideaaltypes aannemen, te weten: inertie, ontkenning, overdrijving en coherentie.¹⁹³ Meer dan ooit vraagt het waarborgen van onze veiligheid om een grensoverschrijdende aanpak. Zoals aangegeven is de oorsprong, het traject en het effect op veiligheid van dreigingen niet of nauwelijks meer aan fysieke grenzen gebonden. Dit vraagt dus een veiligheidsaanpak die ook deze fysieke grenzen kan overstijgen. Elk onderzoekskader van hedendaagse veiligheid moet deze internationale dimensie reflecteren.

193 Eriksson en Rhinard (2009) 258-259.

Bijlagen

Literatuurlijst

- AIVD. (2019). *Jaarverslag 2018*.
- AIVD. (2019). *Iran waarschijnlijk betrokken bij liquidaties in Nederland*.
- Allison, G. & Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis*. (New York: Addison Wesley Longman).
- Andeweg, R.B. (2000). 'Ministers as Double Agents? The Delegation Process Between Cabinet and Ministers'. In: *European Journal of Political Research*, 37, pp. 337-395.
- Analistenennetwerk Nationale Veiligheid (ANV). (2016). *Nationaal Veiligheidsprofiel. Een All Hazard overzicht van potentiële rampen en dreigingen die onze samenleving kunnen ontwrichten*.
<https://www.rivm.nl/sites/default/files/2018-11/Nationaal%20Veiligheidsprofiel%202016.pdf>.
- ANV. (2018). *Horizonscan Nationale Veiligheid 2018*.
- ANV. (2018). *Hybrid Conflict: The Roles of Russia, North Korea and China*. Edited by: F.P. van der Putten, M. Meijnders, S. van der Meer & T. van der Togt.
- ANV. (2019). *Geïntegreerde risicoanalyse Nationale Veiligheid*.
- APSC. (2007). *Tackling Wicked Problems: A Public Policy Perspective*. (Barton: Australian Public Service Commission).
- Arena, M. (2016). *Cyber Threat Intelligence: Comparing the incident-centric and actor-centric approaches*. <https://medium.com/@markarenaau/cyber-threat-intelligence-comparing-the-incident-centric-and-actor-centric-approaches-f20cfba2dea2>.
- AT Kearney. (2017). *Global Cities 2017: Leaders in a World of Disruptive Innovation*.
- Beck, U. (1992). *Risk Society. Towards a New Modernity*, p. 697.
- Bekkers, F., Meessen, R. & Lassche, D. (2018). *Hybrid Conflicts: the New Normal?*
- Benner, T., Gaspers, J., Ohlberg, M., Poggetti, L. & Shi-Kupfer, K. (2018). *Responding to China's Growing Political Influence in Europe*. (Global Public Policy Institute & Mercator Institute for China Studies).
- Besselink, L. 'The Constitutional Duty to Promote the Development of the International Legal Order: the Significance and Meaning of Article 90 of the Netherlands Constitution'. *Netherlands Yearbook of International Law*, nr. 34 (2003): p. 89-138.
- Blagden, D. (2018). 'The flawed promise of National Security Risk Assessment: nine lessons from the British approach'. *Intelligence and National Security*, Vol. 33, No. 5, p. 716-736.
- Bogdanor, V. (2005). *Joined-up Government*. (Oxford: Oxford University Press).
- Bouckaert, G., Peters, B.G. & Verhoest, K. (2010). 'The Coordination of Public Sector Organizations'. In: B.G. Peters & G. Bouckaert (Eds.), *Shifting Patterns of Public Management*. (Hampshire: Palgrave MacMillan).
- Bovens, M.A.P., 't Hart, P. & van Twist, M.J.W. (2007). *Openbaar bestuur: beleid, organisatie en politiek*. (Alphen aan de Rijn: Kluwer).

- Brandao, A.P. (2015). 'The internal-external security nexus in the security narrative of the EU'. In: *JANUS.net, e-journal of International Relations*, 6(1), pp. 1-19.
- Brown, G.G. & Cox Jr., L.A. (2011). 'How Probabilistic Risk Assessment Can Mislead Terrorism Risk Analysis'. In: *Risk Analysis*, 31(2), pp. 196-204.
- Bruijne, de, K. (2018). 'Vitale Belangen'. *Clingendael Policy Brief*. (Den Haag: Instituut Clingendael).
- Buzan, B. (1991). *People, States and Fear*. (Boulder-CO: Lynne-Rienner Publishers).
- Buzan, B., Waever, O. & Wilde, de, J. (1998). *Security: A New Framework for Analysis*. (Boulder-CO: Lynne Rienner Publishers).
- Churchman, C.W. (1967). 'Wicked Problems'. In: *Management Science*, 14(4), pp. 141-142.
- Christensen, T. & Laegreid, P. (2006). *The Whole-of-Government Approach*. (Stein Rokkan Centre for Social Studies).
- Clarke, M. & Steward, J. (1997). *Handling the Wicked Issues: A Challenge for government*. (University of Birmingham: School of Public Policy).
- Coomans, F. & Kamminga, M. 'De Rechten van de Mens'. In: Nathalie Horbach et al (red.), *Handboek Internationaal Recht*, T.M.C. Asser Press, 2007.
- Cox Jr., L.A. (2008). 'Some limitations of "Risk = Threat x Vulnerability x Consequence" for Risk analysis of Terrorist Attacks'. *Risk Analysis*, Vol. 28, No. 6, p. 1749-1761.
- DHL, *DHL Global Connectedness Index 2018: The State of Globalization in a Fragile World*.
- Directie Internationaal Onderzoek en Beleidsevaluatie, het ministerie van Buitenlandse Zaken. 'Vreedzame geschillenbeslechting en het tegengaan van straffeloosheid', nr. 410, 2015.
- Drent, M. & Meijnders, M. (2019). *De Internationale Rechtsorde als zesde nationaal veiligheidsbelang*, ANV.
- Duchateau-Polkerman, E.E. (2016). 'Hoe perceptie ons veiligheidsgevoel beïnvloedt'. In: *Militaire Spectator*, 185(1), pp. 4-18.
- Eriksson, J. & Rhinard, M. (2009). 'The Internal-External Security Nexus: Notes on an Emerging Agenda'. In: *Cooperation and Conflict*, 44(3), pp. 243-267.
- European Commission. (2017). *Reflection Paper on Harnessing Globalisation*. Via: https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-globalisation_en.pdf.
- Evans-Pritchard, A. (2018). 'Leaked EU files show Brussels cover-up and collusion on Putin's Gazprom abuses'. *The Telegraph*. Via: <https://www.telegraph.co.uk/business/2018/04/12/leaked-eu-files-show-brussels-cover-up-collusion-putins-gazprom/>.
- Fox, J. & Godement, F. (2009). *A Power Audit of EU-China Relations*. (London: European Council on Foreign Relations).
- Goldgeier, J. 'The Misunderstood Roots of International Order and Why They Matter Again'. *The Washington Quarterly*, nr.41(3), (2018): p. 9.
- Grashof, R. 'Maak Nederland weer voortrekker'. In: *Internationale Spectator*, nr.70 (2016): p. 2.
- Gray, B. (1985). 'Conditions Facilitating Interorganizational Collaboration'. In: *Human Relations*, 38(10), pp. 911-936.
- Gray, B. (1989). *Collaborating: Finding Common Ground for Multiparty Problems*. (San Francisco: Jossey-Bass).
- Gross Stein, J. (2002). 'Psychological Explanations of International Conflict'. In: W. Carlsnaes, T. Risse-Kappen & B.A. Simmons (Eds.), *Handbook of International Relations*. (Londen: Sage), pp. 292-308.

- Guikema, S.D. & Aven, T. (2010). 'Assessing risk from intelligent attacks: A perspective on approaches'. In: *Reliability Engineering and System Safety*, Vol. 95.
- Hazelbag, L.J. (2015). 'Nationale Veiligheidsraad: politiek wenselijk en staatsrechtelijk haalbaar?'. In: *Militaire Spectator*, 184(4), pp. 184-197.
- Hirsch Ballin, E. 'Ontwikkeling van de internationale rechtsorde'. In: *Christen Democratische Verkenningen*, nr. 34 (2014): p. 136-142.
- Hood, C. (2005). 'The Idea of Joined-up Government: A Historical Perspective'. In: V. Bogdanor (Eds.) *Joined-up Government*. (Oxford: Oxford University Press), pp. 12-37.
- Ioannides, I. & Collantes-Celador, G. (2011). 'The internal-external security nexus and EU police/ rule of law missions in the Western Balkans'. In: *Conflict, Security & Development*, 11(94), pp. 415-445.
- Ioannides, I. (2014). 'Inside-out and outside-in: EU security in the neighbourhood'. In: *The International Spectator*.
- James, P. & Steger, B. (2014). 'A Genealogy of 'Globalization': The Career of a Concept'. In: *Globalizations*, 11(4), pp. 417-434.
- Jore, S.H., Utland, I.F. & Vatnamo, V.H. (2018). 'The contribution of foresight to improve long-term security planning'. In: *Foresight*, 20(1), pp. 68-83.
- Jovanovic, M et al. (2016). 'Non-traditional transnational security challenges in Serbian, British and Dutch discourses: a cross-country comparison'. In: Masys, A.J. (ed). *Exploring the Security Landscape: Non-Traditional Security Challenges*. Springer, pp. 9-30.
- Kaldor, M. (2006). *New and Old Wars: Organized Violence in a Global Era*. (Palo Alto-CA: Stanford University Press).
- Kickert, W.J.M., Klijn, E.H. & Koppenjan, J.F.M. (1997). *Managing Complex Network: Strategies for the Public Sector*. (Londen: SAGE Publications).
- Klein, M. (2019). *Private military companies – a growing instrument in Russia's foreign and security policy toolbox*. (Hybrid Center of Excellence).
- Knops, R. 'Realistisch én waardegedreven'. In: *Internationale Spectator*, nr.70 (2016): p. 2.
- Koppenjan, J.F.M. & Klijn, E.H. (2004). *Managing Uncertainties in Networks*. (Londen: Routledge).
- Krasner, S.D. 'Structural causes and regime consequences: regimes as intervening variables'. *International Organization*, nr. 36(2), (1982): p. 85.
- Kruisbergen, E.W., Bunt, van de, H.G. & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. (Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)).
- Laan, van der, F. (2016). *Het Grenzeloze Werkveld van de Politie. Externe Veiligheidsontwikkelingen en hun Implicaties voor Internationale Samenwerking*. (Clingendael Rapport).
- Laan, van der, F. & M. Drent. (2017). 'Grip op het grenzeloze werkveld van de politie'. In: *Cahier Politiestudies*, 3(44), pp. 13-44.
- Lijphart, A. (1999). *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*. (New Haven: Yale University Press).
- Lindaas, O.A. & Pettersen, K.A. (2016). 'Risk analysis and Black Swans: Two strategies for de-blackening'. In: *Journal of Risk Research*, 19(10), pp. 1231-1245.
- Lund Petersen, K. (2011). 'Risk analysis – a field within security studies?'. *European Journal of International Relations*, Vol. 18, No. 4, p. 693-717.

- Mazarr, M. 'The Once and Future Order: What Comes after Hegemony'. In: *Foreign Affairs*, nr. 96 (2017): p. 25.
- Meijnders, M. & Martens, M. (2019). *Global Security Pulse: Economic Security*. (Den Haag: Clingendael Institute & HCSS).
- Ministerie van Algemene Zaken. (2018). *Geïntegreerde Aanwijzing Inlichtingen en Veiligheid 2019-2022*. Staatscourant Nr. 68088, 4 december 2018.
- Ministerie van Buitenlandse Zaken. (2013). *Internationale Veiligheidsstrategie: Veilige Wereld, Veilig Nederland*.
- Ministerie van Buitenlandse Zaken. (2018). *Investeren in perspectief. Goed voor de wereld, goed voor Nederland* (BHOS-nota).
- Ministerie van Buitenlandse Zaken. (2018). *Kamerbrief over de Nederlandse gasrelatie met Rusland*.
- Ministerie van Buitenlandse Zaken. (2018). *Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022*.
- Ministerie van Buitenlandse Zaken. (2019). *Homogene Groep International Samenwerking (HGIS) – nota 2019*. Tweede Kamer, vergaderjaar 2018–2019, 35 001, nr. 2.
- Ministerie van Buitenlandse Zaken. (2019). *Kamerbrief over sancties tegen Iran*.
- Ministerie van Defensie. (2017). *Houvast in een onzekere wereld – Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gereede en snel inzetbare krijgsmacht*.
- Ministerie van Defensie. (2018). *Defensienota 2018 – Investeren in onze mensen, slagkracht en zichtbaarheid*.
- Ministerie van Justitie en Veiligheid. (maart 2013). *Werken met scenario's, risicobeoordeling en capaciteiten in de Strategie Nationale Veiligheid*.
- Ministerie van Justitie en Veiligheid. (2019). *Kamerbrief Tegengaan statelijke dreigingen*.
- Nollkaemper, A. 'Kern van het internationaal publiekrecht'. (Boom Juridische uitgevers, 2016).
- Weiβ, J., A. Sachs, A. & H. Weinelt. (2018). *2018 Globalization Report. Who Benefits Most from Globalization?* (Bertelsmann Stiftung).
- Mulgan, K. (2005). 'Joined-up Government: Past, Present and Future'. In: V. Bogdanor (Eds.), *Joined-up Government*, (Oxford: Oxford University Press), pp. 175-187.
- Multinational Capability Development Campaign. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*.
- National Security and Risk Assessment, Factsheet. (2015). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf.
- NCTV. (2016). *Nationale Contraterrorisme strategie (2016-2020)*.
- NCTV. (2018). *Kamerbrief Ongewenste buitenlandse inmenging*.
- NCTV. (2019). *Chimaera: Een duiding van het fenomeen 'hybride dreiging'*.
- NCTV. (2019). *Nationale Veiligheid Strategie 2019*.
- NOS. (2018). *Kabinet: Turkse stemoproep Erdogan ongepast*. Via: <https://nos.nl/artikel/2236610-kabinet-turkse-stemoproep-erdogan-ongepast.html>.
- Peters, B.G. (1998). 'Managing Horizontal Government: The Politics of Co-ordination'. In: *Public Administration*, pp. 295-311.
- Pronk, D. (2019). 'The Return of Political Warfare'. In: *Strategic Monitor 2018-2019*. (Den Haag: Clingendael Institute & HCSS).

- Rachman, G. (2018). 'Why Globalism is Good for You', in *Financial Times*.
- Rees, W. (2008). 'Inside Out: the External Face of EU Internal Security Policy'. In: *Journal of European Integration*, 30(1), pp. 97-111.
- Regeerakkoord VVD-CDA, 'Vrijheid en verantwoordelijkheid', 2010.
- Regeerakkoord VVD-PvdA, 'Bruggen slaan', 2012.
- Regeerakkoord VVD, CDA, D66 en ChristenUnie, 'Vertrouwen in de toekomst', 2017.
- Ripsam, N.M. (2010). 'Globalization and the National Security State'. *Foreign Affairs*, pp. 20-21.
- Roberts, N. (2000). 'Wicked Problems and Network Approaches to Resolution'. In: *International Public Management Review*, 1(1), pp. 1-19.
- Rosenboim, O. (2017). 'Globalism and Nationalism. Why interconnectedness does not threaten sovereignty'. In *Foreign Affairs*.
- Rudolph, C. (2003). 'Globalization and Security: Migration and Evolving Conceptions of Security in Statecraft and Scholarship'. In: *Security Studies*, 13(1), pp. 1-32.
- Schein, E.H. (2010). *Organization Culture and Leadership*, 4th edition. (New York: Wiley and Sons).
- Scholte, J.A. (2007). 'Defining Globalization'. In *Clim.economía*, 10, pp. 15-63.
- Schroeder, U.C. (2011). *The Organization of European Security Governance: Internal and External Security in Transition*. (Londen: Routledge).
- Schuurman, B. & Eijkman, Q. (2015), 'Indicators of terrorist intent and capability: Tools for threat assessment'. *Dynamics of Asymmetric Conflict*, Vol. 8, No. 3, p. 215-231.
- Steijn, B., Klijn, E.H. & Edelenbos, J. (2010). 'The Impact of Network Management on Outcomes in Governance Networks'. In: *Public Administration*, 88(4), pp. 1063-1082.
- Stoutenborough, J.W. (2018). *China's Comprehensive Approach: Refining the U.S. Targeting Process to Inform U.S. Strategy*.
- Susel, I., Lasley, T., Montezemolo, M. & Piper, J. (2016). 'Augmenting the Deliberative Method for Ranking Risks'. In: *Risk Analysis*, Vol. 36, No. 1.
- Taleb, N.N. (2007). *The Black Swan: The impact of the highly improbable*. (London: Penguin Books).
- Ten Broeke, H. 'Tien vuistregels voor realistisch buitenlands beleid'. In: *Internationale Spectator*, nr. 70 (2016): p. 2.
- Trauner, F. (2011). 'The Internal-External Security Nexus: More Coherence Under Lisbon?'. In: *SSRN Electronic Journal*.
- Tweede Kamer der Staten Generaal. 'Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van bepalingen inzake de buitenlandse betrekkingen', Kamerstuk II 1979/80, 15049 (R1100), nr. 7 (1979): p. 5.
- Tzevelekos, V. 'Revisiting the Humanisation of International Law: Limits and Potential: Obligations Erga Omnes, Hierarchy of Rules and the Principle of Due Diligence as the Basis for Further Humanisation'. In: *Erasmus Law Review*, nr. 6(1) (2013): p. 62.
- Verenigde Naties. 'Internationaal Verdrag inzake Burgerrechten en Politieke Rechten'. (1966).
- Vlemminx, F. 'Commentaar op artikel 90 van de Grondwet'. In: Ernst Hirsch Ballin en Gert-Jan Leenknecht (red.), *Artikelsgewijs commentaar op de Grondwet*, webeditie 2018.
- Wetenschappelijk Raad voor het Regeringsbeleid (WRR). (2017). *Veiligheid in een wereld van verbindingen: een strategische visie op het defensiebeleid*. (Den Haag: WRR).
- Willis, H.H., et al. (2018). *Homeland Security National Risk Categorization. Risk Assessment Methodology*. (Santa Monica: RAND Corporation).

Zee, van der, S. & Hoebé, D. (2019). *Veiligheidsbeeld BES 2018*. (Kralendijk: Openbaar Ministerie Bonaire, Sint Eustatius en Saba).

<http://www.worldshipping.org/about-the-industry/global-trade/top-50-world-container-ports>.

<https://aci.aero/news/2018/09/20/aci-world-publishes-annual-world-airport-traffic-report/>.

<https://www.nrc.nl/nieuws/2019/05/26/nederland-is-nu-transitland-voor-mensensmokkel-a3961645>.

https://files.taxfoundation.org/20190213134207/ITCI_2018.pdf.

Uit: Margriet Drent en Minke Meijnders, *Internationale Rechtsorde als zesde Nationaal Veiligheidsbelang*, Analistennetwerk Nationale Veiligheid, mei 2019, pp. 17-19.

Belang: Internationale Rechtsorde

Op basis van de bovenstaande criteria kan een definitie worden opgesteld van het belang 'internationale rechtsorde':

Het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, inclusief mensenrechten, een gereguleerd internationaal financieel-economisch bestel en effectieve multilaterale instituties en regimes.

De internationale rechtsorde wordt hier dus begrepen als het stelsel van normen en afspraken, die zijn gericht op het bevorderen van internationale vrede en veiligheid. Wat onlosmakelijk verbonden is met het bereiken van internationale vrede en veiligheid is het bevorderen van fundamentele mensenrechten, een op regels gebaseerd internationaal financieel-economisch bestel en effectieve multilaterale instituties en regimes. Dit is een definitie die zowel de fundamentele (brede stelsel van mensenrechten) als de instrumentele (nauwe belangen) interpretatie van internationale rechtsorde tegemoet komt.

Impactcriteria

Het belang 'functioneren internationale rechtsorde' kan op basis van bovenstaande uitgewerkt worden in vier delen:

1. Waarborgen van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting;
2. Waarborgen van de rechten van de mens;
3. Waarborgen van een op regels gebaseerd internationaal financieel-economisch bestel;
4. Behoud en uitbouw van een effectief multilateraal systeem van goed functionerende multilaterale instituties en internationale regimes.

Deze vier delen van het belang kunnen worden uitgewerkt in vier corresponderende **impactcriteria**:

1. Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting (zoals in het VN-Handvest vastgelegd);
2. Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens;

3. Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel;
4. Aantasting van de effectiviteit en legitimiteit van multilaterale instituties en internationale regimes.

Indicatoren die de impactscore bepalen, zijn als volgt uitgewerkt:

Impactcriterium 1: Aantasting van de normen van staatssoevereiniteit, vreedzame co-existentie en vreedzame geschillenbeslechting (zoals in het VN-Handvest vastgelegd¹⁹⁴):

- A. Blokkades (land, lucht, water) of inperken van het gezag van een soevereine staat (zoals: manipulatie verkiezingen, sabotage, desinformatiecampagnes, infiltratie, ongewenste overname vitale infrastructuur, geweldschantage)
- B. Geweldsconflicten tussen landen zonder grensoverschrijding van militaire landeenheden; inperken van het gezag van een soevereine staat (zie A) voor langere tijd
- C. Geweldsconflicten tussen landen met kortdurende grensoverschrijding; inperken van het gezag van een soevereine staat (zie A) voor langere tijd en van essentiële onderdelen van de staatssoevereiniteit en functioneren van de vitale infrastructuur
- D. Gebruik van massavernietigingswapens door een staat of tijdelijke bezetting van (een deel van de) soevereine staat door middel van geweld (doel bijvoorbeeld grenscorrectie, bewindswijziging)
- E. Permanente bezetting en/of annexatie van een soevereine staat (door geweld bewerkstelligd) en/of gebruik van massavernietigingswapens door meerdere staten.

Toelichting verhoging: Het maakt uit welke staat de norm(en) schendt. Dit leidt ertoe dat de impactscore (Klasse) met +1 wordt gecorrigeerd als één van de permanente leden van de VN-Veiligheidsraad de normbreker is (China, Frankrijk, Rusland, VK, VS).

194 Artikel 1 van het VN-Handvest behelst de volgende eerste doelstelling:

“1. De internationale vrede en veiligheid te handhaven en, met het oog daarop: doeltreffende gezamenlijke maatregelen te nemen ter voorkoming en opheffing van bedreigingen van de vrede en ter onderdrukking van daden van agressie of andere vormen van verbreking van de vrede, alsook met vreedzame middelen en in overeenstemming met de beginselen van gerechtigheid en internationaal recht, een regeling of beslechting van internationale geschillen of van situaties die tot verbreking van de vrede zouden kunnen leiden, tot stand te brengen.”

Impactcriterium 2: Aantasting van de werking, legitimiteit dan wel naleving van de internationale verdragen en normen inzake de rechten van de mens¹⁹⁵:

- A. Ontzeggen of aantasten van economische, culturele, sociale en collectieve rechten (+1 mate van geweldsgebruik bij het ontzeggen van de rechten en +1 omvang van de schending)
- B. Ontzeggen of aantasten van burger- en politieke rechten (+1 mate van geweldsgebruik bij het ontzeggen van de rechten en +1 omvang van de schending)
- C. Zie A en B; oorlogsmisdrijven¹⁹⁶ (+1 omvang misdaden)
- D. Zie B en C

¹⁹⁵ Deze mensenrechten zijn neergelegd in de volgende documenten: de Universele Verklaring van de Rechten van de Mens, het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR), het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), het Internationaal Verdrag inzake economische, sociale en culturele rechten (IVESCR) en het Europees Sociaal Handvest (ESH) alsmede allerlei specifieke verdragen in het kader van de VN en de Raad van Europa.

¹⁹⁶ Handelingen zijn oorlogsmisdrijven en onderdeel van het humanitair oorlogsrecht als zij worden begaan ten tijde van een gewapend conflict. Er zijn twee delen, het Geneefse en Haagse deel. Het Geneve-deel is een geheel van regels dat de slachtoffers beschermt van een gewapend conflict, zoals burgers die niet of niet langer deelnemen aan de vijandelijkheden en gewonde of zieke soldaten die beschouwd worden als buiten strijd. Het 'recht van Den Haag' is een geheel dat regels, rechten en plichten oplegt aan de strijdende partijen in de manier waarop ze oorlog voeren en beperkt de middelen en methoden. Deze twee zijn in 1977 samengevoegd.

E. Misdaden tegen de menselijkheid¹⁹⁷ of ernstige oorlogsmisdrijven (onderdeel van strategie of beleid)¹⁹⁸ en genocide

Toelichting verhoging: De impactscore kan worden gecorrigeerd als er sprake is van geweldsgebruik bij en/of een omvangrijke schending van de rechten van de mens (beide +1). Ook als er sprake is van omvangrijke oorlogsmisdaden, kan de impactscore met +1 worden gecorrigeerd.

197 In artikel 7 van het Statuut van het Internationaal Strafhof worden de volgende handelingen aangemerkt als misdaden tegen de menselijkheid, *"indien gepleegd als onderdeel van een wijdverbreide of stelselmatige aanval gericht tegen een burgerbevolking, met kennis van de aanval"*: moord; uitroeiing; slavernij; deportatie of onder dwang onderbrengen van bevolking; gevangenneming of andere ernstige beroving van de lichamelijke vrijheid, marteling; verkrachting, seksuele slavernij, gedwongen prostitutie, gedwongen zwangerschap, gedwongen sterilisatie, of enige andere vorm van seksueel geweld van vergelijkbare ernst; vervolging van een identificeerbare groep of collectiviteit op politieke gronden, omdat deze tot een bepaald ras of een bepaalde nationaliteit behoort, op etnische, culturele of godsdienstige gronden, of op grond van geslacht of op andere gronden die universeel zijn erkend als ontoelaatbaar; gedwongen verdwijning van personen; apartheid; en andere onmenselijke handelingen van vergelijkbare aard waardoor opzettelijk ernstig lijden of ernstig lichamelijk letsel of schade aan de geestelijke of lichamelijke gezondheid wordt veroorzaakt.

198 In artikel 8 van het Statuut van het Internationaal Strafhof wordt beschreven wat er wordt verstaan onder oorlogsmisdrijven:

- i. opzettelijk doden;
- ii. marteling of onmenselijke behandeling, met inbegrip van biologische experimenten;
- iii. opzettelijk veroorzaken van ernstig lijden, zwaar lichamelijk letsel of ernstige schade aan de gezondheid;
- iv. grootschalige wederrechtelijke en moedwillige vernietiging en toe-eigening van goederen zonder militaire noodzaak;
- v. een krijgsgevangene of andere beschermde persoon dwingen dienst te nemen bij de strijdkrachten van een vijandige mogendheid;
- vi. een krijgsgevangene of andere beschermde persoon opzettelijk het recht op een eerlijke en rechtmatige berechting onthouden;
- vii. onrechtmatige deportatie of verplaatsing of onrechtmatige opsluiting;
- viii. gijzelneming.

Er is sprake van ernstige oorlogsmisdrijven als ze worden gepleegd als *"onderdeel van een plan of beleid of als onderdeel van het op grote schaal plegen van dergelijke misdaden"*.

Impactcriterium 3: Aantasting van een op regels gebaseerd internationaal financieel-economisch bestel¹⁹⁹:

- A. Niet- naleven van de regels of onttrekken aan verplichtingen van het internationaal financieel-economisch verkeer (+ 1 ernst en +1 omvang)
- B. Aanpassing van bestaande instituties en de onderliggende normen en regels (die Nederland niet wenselijk acht)
- C. Verlamming van besluitvorming en processen van bestaande instituties en/of presenteren van alternatieven door unilaterale initiatieven
- D. Het gedeeltelijk ineenstorten van het op regels gebaseerde internationaal financieel-economisch bestel en/of alternatieve instituties en/of netwerken zijn invloedrijker dan die van het bestaand internationaal financieel-economisch bestel (met als gevolg minder invloed voor NL)
- E. Het volledig ineenstorten van het op regels gebaseerde internationaal financieel-economisch bestel (omvallen WTO en alternatieve instituties en netwerken)

Toelichting verhoging: Het maakt uit welke staat de regels niet naleeft of zich onttrekt aan verplichtingen van het financieel-economisch bestel. Het is ernstiger als het gaat om de normdragers van het financieel-economisch bestel, dat wil zeggen de EU, VS of China. De impactscore (Klasse A) wordt gecorrigeerd naar Klasse B als het één van deze normdragers betreft of als het om een omvangrijke schending gaat. Als het gaat om een omvangrijke schending door de (een van de) normdragers, dan wordt de impactscore (Klasse A) gecorrigeerd naar Klasse C.

Impactcriterium 4: Aantasting van de effectiviteit en legitimiteit van multilaterale instituties (waarvan de belangrijkste, maar niet limitatief*: VN, EU, NAVO, Internationale Strafhoven en Tribunalen) en internationale regimes (denk aan wapenbeheersing, klimaatafspraken, terrorismebestrijding etc.).

- A. Onttrekken aan verplichtingen (geen contributie of anderszins actieve bijdrage) en/of niet-naleven van afspraken en/of legitimiteit van institutie staat ter discussie (+1 ernst (normdragers en/of P5-landen) of omvangrijk)
- B. Onderminning van basisbeginselen van de multilaterale instituties en internationale regimes (+1 normdragers of P5-landen)

¹⁹⁹ De WTO met haar geschillenbeslechtsmechanisme staat in dit criterium centraal, maar er wordt ook gekeken naar het IMF, de Wereldbank, De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), en het bredere stelsel van regionale, bilaterale en sectorale akkoorden, maar ook bijvoorbeeld het internationaal zeerecht en waterrecht of andere verdragen, afspraken en regimes die het goed functioneren van het financieel-economisch bestel bevorderen.

- C. Verlamming van besluitvorming en processen van instituties; uittreden leidend(e) land(en) en/of regio's uit multilaterale instituties en/of regimes (als dit uittreding uit de VN, EU, NAVO betreft dan +1)
- D. Het uiteenvallen van multilaterale instituties (anders dan VN, NAVO, EU) en regimes
- E. Uiteenvallen van VN, NAVO, EU

* Financieel-economische instituties en regimes worden meegenomen in criterium 3

Toelichting verhoging: Het maakt uit welke staat de regels niet naleeft of zich onttrekt aan verplichtingen. Het is ernstiger als het gaat om de normdragers of om één van de permanente leden van de VN-Veiligheidsraad (China, Frankrijk, Rusland, VK, VS), de impactscore (klasse) wordt dan met +1 gecorrigeerd. Ook kan er een klasse +1 gecorrigeerd worden als het om een omvangrijke schending gaat. Daarnaast maakt het uit welke instituties worden verlamd of uiteenvallen: vanwege het belang van de VN, NAVO of EU voor Nederland, dan wordt er +1 gecorrigeerd.