Afschrikking als veiligheidsconcept tegen niet-traditionele dreigingen

Frans-Paul van der Putten
Minke Meijnders
Jan Rood

Verdiepingsstudie
Clingendael Monitor 2015

Clingendael
Netherlands Institute of International Relations

Clingendael

Netherlands Institute of International Relations

Afschrikking als veiligheidsconcept tegen niet-traditionele dreigingen

Verdiepingsstudie Clingendael Monitor 2015

Frans-Paul van der Putten
Minke Meijnders
Jan Rood

Juni 2015

Juni 2015

Over de auteurs

Frans-Paul van der Putten is *Senior Research Fellow* bij Instituut Clingendael. Zijn onderzoek richt zich in het bijzonder op de gevolgen van de opkomst van China voor mondiale machtsverhoudingen.

Minke Meijnders is onderzoeks- en projectassistent voor het veiligheidscluster van Clingendael Research. Zij houdt zich bezig met internationale veiligheidskwesties, zoals maritieme veiligheid, terrorisme en vredesoperaties.

Jan Rood is als *Senior Research Fellow* verbonden aan Instituut Clingendael, waar hij zich bezighoudt met mondiale vraagstukken en met Europese integratie. Daarnaast is hij bijzonder hoogleraar Europese Integratie in een Mondiaal Perspectief aan de Universiteit Leiden.

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

Email: info@clingendael.nl
Website: http://www.clingendael.nl/

Inhoud

Afschrikking als veiligheidsconcept tegen niet-traditionele dreigingen

Inleiding

De vraag die in dit deel van de Clingendael Monitor 2015 centraal staat is in hoeverre in de komende 5 tot 10 jaar afschrikking als veiligheidsconcept en –instrument een relevant en effectief middel kan zijn voor de bescherming van de Nederlandse veiligheidsbelangen waar deze door internationale 'niet-traditionele' dreigingen worden bedreigd.[1] Reeds in de Defensieverkenningen van 2010 werd gewezen op de blijvende betekenis van afschrikking als middel tot ontmoediging 'van activiteiten die indruisen tegen de veiligheidsbelangen van het Koninkrijk en de internationale rechtsorde'.[2] Daarbij ging het om afschrikking in de vorm van het in het vooruitzicht stellen van een geloofwaardige vergelding tegen bestaande, in het bijzonder militaire dreigingen, met mogelijke inzet in bondgenootschappelijk verband van conventionele en nucleaire middelen. Maar ook in de Defensieverkenningen werd geconstateerd dat zich mondiaal een diffuser dreigingsbeeld aftekende rond niet-militaire c.q. niet direct militaire dreigingen, wat noopte tot een langetermijnbenadering van afschrikking als instrument, gericht op zowel bestaande militaire als nieuwe en toekomstige dreigingen van andere aard.

Deze niet-traditionele dreigingen onderscheiden zich daarbij van traditionele veiligheidsdreigingen, die gekenmerkt worden door een herkenbare inzet van militaire middelen door buitenlandse statelijke actoren met als doel de nationale veiligheid van Nederland en/of zijn militaire bondgenoten ernstige schade toe te brengen. Niet-traditionele dreigingen ontberen deze kenmerken van herkenbare militaire en statelijke inzet en zijn daardoor hybride en diffuus. Waar het gaat om niet-traditionele dreigingen die in concrete gevallen van statelijke actoren uitgaan kan het van belang zijn om die in samenhang te beschouwen met traditionele dreigingen vanuit dezelfde staten (voor zover daar sprake van is).

De eerder gepubliceerde edities van de Clingendael Monitor bevestigen het beeld van een diffuser palet aan veiligheidsdreigingen voor Nederland en zijn partners en bondgenoten.[3] Naast het blijvend gevaar van een militaire dreiging is sprake van 'nieuwe' dreigingen in o.a. de vorm van cyberdreigingen, religieus geïnspireerd terrorisme, criminaliteit, etc. In het bijzonder dit diffusere dreigingsbeeld is reden om in deze studie de vraag naar de betekenis en effectiviteit van afschrikking als middel tot bezwering van deze dreigingen te bespreken, mede in het licht van toekomstige ontwikkelingen op dit terrein.

---

1 De auteurs danken Nina Jolink en Anne Bakker voor de waardevolle bijdragen die zij hebben geleverd aan dit rapport als onderdeel van hun onderzoeksstages op Clingendael; Bibi van Ginkel, Sico van der Meer, Sander Huisman, Peter van Bergeijk, Rob Hendriks, Margriet Drent, Kees Homan en Dick Zandee voor het schrijven van onderdelen van dit rapport en/of het deelnemen aan voorbereidende sessies; en Franca van der Laan, Luc van de Goor, Ko Colijn en meelezers bij diverse ministeries voor hun waardevolle commentaren op eerdere versies van de tekst.

2 Ministerie van Defensie, Eindrapport verkenningen; houvast voor de krijgsmacht van de toekomst. Den Haag: Ministerie van Defensie, 2010, p. 196.

3 Zie Clingendael Strategische Monitor 2012, 2013, 2014, 2015.

Op basis van de conclusies van de eerdere versies van de Clingendael Monitor is in deze studie een vijftal internationale dreigingsthema's geselecteerd dat nader wordt geanalyseerd op de toepasbaarheid van het instrument van afschrikking. Het gaat bij deze dreigingsthema's met name om de internationale dimensie ervan, dus om dreigingen die Nederland (mede) via het internationale niveau kunnen treffen:

- Terrorisme;
- Dreigingen via het cyberdomein;
- Georganiseerde criminaliteit;
- Dreigingen via het economische domein;
- Ambigue oorlogsvoering.

In de bespreking van deze thema's gaat het om de volgende drie deelvragen:
1. Wat is de huidige situatie op het desbetreffende dreigingsthema?
2. In hoeverre is het betreffende dreigingsthema in de komende 5 à 10 jaar relevant voor de Nederlandse nationale veiligheid?
3. Op welke wijze is afschrikking als veiligheidsconcept relevant voor de bescherming van de nationale veiligheid ten opzichte van dit type dreiging?

Dit rapport vat de belangrijkste bevindingen en conclusies samen van de aan de hand van deze vragen verrichte verkennende analyses op de vijf genoemde thema's, die als bijlagen zijn opgenomen bij deze studie.[4] Gezien de beperkte hoeveelheid literatuur die beschikbaar is over afschrikking in relatie tot niet-traditionele veiligheidsdreigingen, in het algemeen en wat betreft de relevantie voor Nederland in het bijzonder, moet dit rapport gezien worden als een eerste afbakening van het terrein. Daarnaast heeft ook de beperkte beschikbaarheid van praktijkvoorbeelden van het al dan niet succesvol implementeren van afschrikkingsinstrumenten in gevallen die voor Nederland relevant zijn tot gevolg dat deze studie eerder theoretisch van aard is dan gericht op het aanreiken van concrete beleidsopties.

Alvorens de belangrijkste bevindingen en conclusies samen te vatten zal eerst het concept afschrikking zoals gehanteerd in deze studie nader worden omschreven en in historisch perspectief worden geplaatst. Daarna zullen kort de Nederlandse veiligheidsbelangen in kaart gebracht worden, gevolgd door een schets van de mondiale en regionale context waarin deze studie gezien moet worden. Deze inleidende paragrafen worden gevolgd door een bespreking van de actuele dreigingen en de verwachtingen voor de komende 5 à 10 jaar. De afsluitende concluderende paragraaf geeft een indicatie van de relevantie van afschrikking als veiligheidsconcept voor de vijf dreigingsthema's. Of het kosteneffectief en politiek of maatschappelijk wenselijk is om specifieke activiteiten ter afschrikking in praktijk te brengen, blijft in dit rapport buiten beschouwing.

Deze studie vormt samen met het overzichtsrapport 'Een wereld zonder orde?' en een nog te verschijnen studie over 'economische kwetsbaarheid' de Clingendael Monitor 2015.
De Clingendael Monitor wordt jaarlijks gepubliceerd als onderdeel van de Strategische Monitor van de Nederlandse overheid.

4 De bijlagen zijn tot stand gekomen op basis van door thema-experts aangeleverde schriftelijke bijdragen die door de auteurs van dit rapport zijn geredigeerd. De verantwoordelijkheid voor de wijze waarop inzichten uit de bijlagen in de analyse in deze overkoepelende tekst zijn verwerkt ligt bij de auteurs van de hoofdtekst van het rapport.

Afschrikking

Het principe van afschrikking (*deterrence*) wordt al zeer lang toegepast in ordehandhaving en als militaire strategie. De term werd tijdens de Koude Oorlog een centraal begrip in het denken over internationale veiligheid, als reactie op het bestaan van kernwapens. Sindsdien is het concept zowel academisch alsook beleidsmatig verder ontwikkeld.

Afschrikking is gericht op het ontmoedigen van ongewenst gedrag. De definitie van afschrikking die in deze studie wordt gehanteerd is:

Alleen maatregelen die *doelbewust* gericht zijn op het ontmoedigen van potentiële daders en/of hun *facilitators* (personen die, door het geven van steun, het mogelijk maken voor daders om hun aanval of aanslag uit te voeren) maken deel uit van een afschrikkingsstrategie. Afschrikking kan enerzijds gericht zijn op het vergroten van de kosten, anderzijds op het verlagen van de baten voor de dader. Binnen deze vormen kan vervolgens onderscheid worden gemaakt tussen het gebruik van maatregelen die direct dan wel indirect dit doel proberen te bereiken.

‘Een benadering gericht op het voorkomen dat een actor die van plan is ernstige schade toe te brengen aan de nationale veiligheidsbelangen van Nederland tot schadelijk handelen overgaat door beïnvloeding van zijn of haar kosten/baten-afweging.

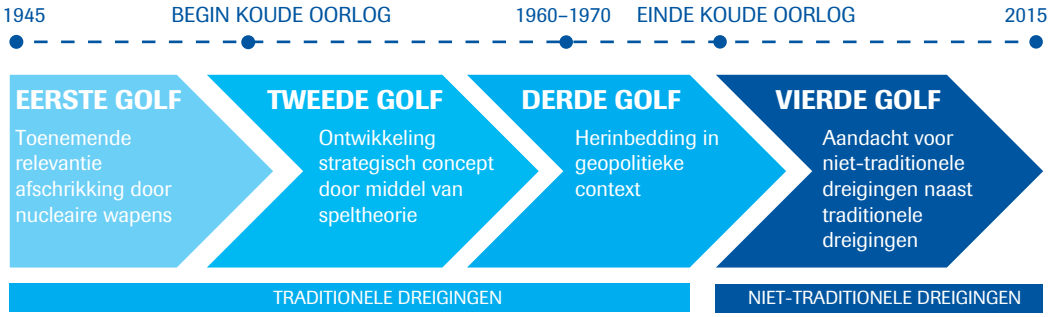
In dit rapport wordt het volgende analysekader gehanteerd met betrekking tot de verschillende mogelijke vormen van afschrikking.

	Maatregelen gericht op het benadrukken/ vergroten van de door de dader ingecalculeerde kosten	**Maatregelen gericht op het benadrukken/ verkleinen van de door de dader ingecalculeerde baten**
Direct	De dader ervan overtuigen dat een aanval (schadelijke handeling, aanslag) tot vergeldings-maatregelen leidt	Verkleinen van de gelegenheid een aanval te doen door het zichtbaar verhogen van de veiligheidsmaatregelen en het vergroten van operationele risico’s voor de dader (kans op succes van de aanval zelf verkleinen).
Indirect	De dader ervan overtuigen dat de voor een aanval benodigde voorinvestering hoog is	De dader ervan overtuigen dat het schadelijk handelen niet bijdraagt aan het beoogde doel (voordelen van/na een succesvolle aanval ver-kleinen).

Bij een effectief afschrikkingsbeleid staat de communicatie met de potentiële dader centraal: het gaat er uiteindelijk om de inschatting die de dader maakt te beïnvloeden, waardoor het minder aantrekkelijk wordt om een schadelijke daad uit te voeren. Belangrijke voorwaarden voor de uitvoering van een afschrikkingsbeleid zijn daarom dat communicatie over de getroffen maatregelen de potentiële dader bereikt en dat deze door hem/haar geloofwaardig worden gevonden. Een afschrikkingsbeleid is gebaseerd op de wetenschap of het vermoeden dat bepaalde actoren het voornemen hebben om handelingen te verrichten die de nationale veiligheid schaden: om het beleid te vormen is het dus noodzakelijk te weten wie de mogelijke daders zijn en wat hun belangen, motivatie en middelen zijn.

Ontwikkelingen in het denken over afschrikking op het terrein van internationale veiligheid

Het huidige denken over afschrikking als instrument voor statelijke actoren tegen veiligheids-dreigingen op internationaal niveau is sterk beïnvloed door de ontwikkeling van kernwapens sinds de jaren '40 van de twintigste eeuw, en is direct gerelateerd aan het ontstaan van het bipolair mondiaal bestel waarbinnen de Sovjet Unie en de Verenigde Staten met het dreigen met wederzijdse vernietiging, *mutually assured destruction (MAD),* een ongemakkelijke vrede overeind hielden. De nucleaire strategie van *second strike capability,* d.w.z. het geloofwaardig vermogen van een mogendheid om een vijandelijke kernaanval te vergelden door middel van een tegenaanval met de eigen nucleaire wapens, stond hierbij centraal.



De politicoloog Robert Jervis spreekt over *drie* golven in het denken over afschrikking.[5] De *eerste* golf in de afschrikkingstheorie begint dan ook na de Tweede Wereldoorlog toen schrijvers als Bernard Brodie tot de conclusie kwamen dat de uitvinding van de atoombom grote gevolgen had voor de wijze van oorlogsvoering. Brodie meende dat er sprake was van een strategische revolutie. Waar het voorheen ging over het winnen van oorlogen, was dit doel nu veranderd in het voorkomen ervan. De reden voor deze strategische revolutie was volgens hem gelegen in het vermogen tot totale vernietiging dat inherent was aan het gebruik van nucleaire wapens, waardoor het verslaan van de tegenstander er niet of nauwelijks meer toe deed. De logische implicatie hiervan was dat, geconfronteerd met een nucleair bewapende tegenstander, een staat zich niet langer kon beschermen met militaire superioriteit.

De *tweede* golf kwam op tegen de achtergrond van de Koude Oorlog. Door onder andere speltheorie te gebruiken werd het strategisch concept van nucleaire afschrikking verder ontwikkeld. Thomas Schelling was een van de eersten die oorlogsvoering typeerde als een onderhandelingsproces, waarin tegenstanders elkaars verwachtingen en intenties met dreigementen, beloftes en acties probeerden te beïnvloeden.[6] Hij zag oorlogsvoering als de kunst van afschrikking, dwang en intimidatie. Nucleaire wapens waren daarbij volgens hem eerder geschikt voor strafoplegging dan om terrein te winnen. Om afschrikking geloofwaardig te maken, moesten de verschillende fasen van de escalatieladder enerzijds volledig duidelijk zijn, om zo een mogelijke oorlog tot een bepaalde fase te beperken. Tegelijkertijd moesten omwille van het bewerkstelligen van een afschrikkend effect de fasen in voldoende mate onbepaald zijn, om zo het risico van een daadwerkelijke oorlog uit te sluiten. Een zekere mate

5 Review Article, Robert Jervis, 'Deterrence theory revisited'. In: *World Politics*. 31(1979)2, p. 289–324.
6 Thomas Schelling, *Arms and influence*. New Haven: Yale University Press, 1966.

van onzekerheid over het escalatieproces is daarmee in deze opvatting noodzakelijk voor effectieve afschrikking.[7]

De *derde* golf kwam op in de jaren zestig en zeventig als kritiek op de afschrikkingstheorie tot dusver. Statistische gegevens en case studies werden gebruikt om de theorie empirisch te testen. Daarnaast werd afschrikking van de tweede golf te apolitiek bevonden. De derde golf denkers meende dat afschrikking niet los van de (geo-)politieke context waarbinnen het concept werd toegepast gezien diende te worden. Het afschrikkingsdenken uit de vorige golf ging volgens hen te weinig in op wat de achterliggende problemen waren die tot een crisis hadden geleid en hoe de crisis kon worden vermeden. Ook werd er geen aandacht besteed aan het sluiten van compromissen, terwijl de meeste conflicten juist eindigden in het sluiten van een compromis tussen betrokken partijen. Tot slot betwistten zij de aanname dat actoren rationeel handelen; een aanname die centraal stond bij de tweede golf denkers. Men vroeg zich af hoe rationeel leiders in het heetst van de strijd nog konden handelen.

In de daaropvolgende decennia bleef aanvankelijk de aandacht in het afschrikkingsdenken voornamelijk gericht op het traditionele interstatelijke conflict. Geleidelijk ontstond echter een nieuwe zienswijze op de toepasbaarheid van afschrikking,[8] waarin in tegenstelling tot de eerdere theorieën niet-traditionele dreigingen in relatie tot afschrikking centraal stonden. Deze benadering maakt deel uit van de vierde golf, die tegen de achtergrond van het einde van de Koude Oorlog in 1991 en de terroristische aanslagen in de VS op 11 september 2001 was opgekomen. Afschrikking werd niet langer uitsluitend in het licht van nucleaire wapens en conventionele oorlog bezien, maar vanuit een veel breder palet aan dreigingen, waaronder ook gewelddadige niet-statelijke actoren en asymmetrische oorlogvoering. De vraag die nu centraal stond was of afschrikking ook ingezet kan worden tegen niet-traditionele dreigingen als terrorisme, piraterij en cyberaanvallen.

Volgens Jeffrey Knopf en andere auteurs uit de vierde golf is afschrikking ook in deze context relevant, maar als slechts één van diverse instrumenten die beschikbaar zijn. Afschrikking heeft daarmee niet meer de centrale rol die het tijdens de Koude Oorlog had. Knopf meent dat afschrikking voortdurend moet worden aangepast aan de specifieke dreiging waartegen het moet beschermen en gebaseerd moet zijn op een gedetailleerd onderzoek naar de tegenstander. Strategisch cultureel besef over de tegenstander is hierbij essentieel.

Veel beschikbare literatuur over afschrikking en niet traditionele dreigingen is gerelateerd aan de Verenigde Staten, of aan het internationale niveau in het algemeen. Deze studie verkent hoe afschrikking relevant kan zijn tegen niet-traditionele dreigingen in het specifieke geval van Nederland.

Nationale veiligheid en internationale context

Nederlandse veiligheidsbelangen en externe dreigingen

In deze studie wordt bekeken in hoeverre afschrikking relevant is als instrument om de Nederlandse veiligheidsbelangen te beschermen. Wat zijn deze Nederlandse veiligheidsbelangen en in hoeverre worden die (potentieel) bedreigd door de in deze studie besproken externe dreigingen? Een primair c.q. vitaal veiligheidsbelang betreft de handhaving van

7 Ola Tunander, 'The logic of deterrence'. In: *Journal of Peace Research*. 26(1989)4, p. 353–365.
8 Jeffrey Knopf, 'The fourth wave in deterrence research'. In: *Contemporary security policy*. 31(2010)1, p. 1-33.

de territoriale integriteit van Nederland, d.w.z. het waarborgen van het voortbestaan als onafhankelijke staat. Maar naast dit primaire belang worden in de Strategie Nationale Veiligheid nog vier andere vitale veiligheidsbelangen onderscheiden: economische veiligheid, ecologische veiligheid, fysieke veiligheid, en sociale en politieke stabiliteit.[9] Onder economische veiligheid wordt verstaan het vermogen om ongestoord te functioneren als effectieve en efficiënte economie. Ecologische veiligheid heeft betrekking op het verzekeren van een veilige natuurlijke leefomgeving. Fysieke veiligheid betreft het veilig kunnen functioneren binnen de samenleving van individuen en groepen van individuen. Bij sociale en politieke stabiliteit gaat het om het waarborgen van een maatschappelijk klimaat waarbinnen de kernwaarden van de democratie en de rechtsstaat zijn verzekerd.

Nederland als relatief klein land met een open democratisch bestel, en dat in velerlei opzichten, maar vooral financieel en economisch, sterk verweven is met het Europese en mondiale systeem, is per definitie kwetsbaar voor externe ontwikkelingen en dreigingen. De primaire dreiging voor Nederland betreft, zoals ook eerdere versies van de Strategische Monitor laten zien,[10] daarbij niet het risico van een directe aanval van een andere staat op het Nederlands grondgebied. Dat risico wordt nog immer als zeer klein beschouwd. Nederlandse betrokkenheid bij territoriale conflicten elders is tegelijkertijd niet uitgesloten, maar dan uit hoofde van de bondgenootschappelijke verplichtingen in het kader van de NAVO en de bijstandsverplichtingen binnen de Europese Unie. In het bijzonder als gevolg van het Russisch optreden in het oosten van Europa is de kans op een dergelijke betrokkenheid toegenomen. De in deze studie besproken dreigingen laten echter zien dat de belangrijkste gevaren voor Nederland liggen op het niet-militaire of niet-direct militaire vlak. Daar tekent zich een divers palet aan dreigingen af, dat diffuus en hybride is, transnationaal van aard en daarmee grenzeloos, en dat zich uitstrekt over een thematiek die loopt van terugkerende *foreign fighters*, via criminaliteit en cyber, de ontwrichtende effecten van migratie, financieel-economische schokken, tot en met klimaatverandering en het risico van pandemieën. De Monitor 2015 laat bovendien zien dat in het wankele wereldbestel van vandaag als gevolg van vooral toenemende instabiliteit in de directe omgeving van de EU en daarmee van Nederland, een aantal van deze dreigingen aan urgentie heeft gewonnen.

In deze studie zijn binnen dit diverse palet in het bijzonder dreigingen die uitgaan van terrorisme, internationale criminaliteit, kwetsbaarheden via het cyberdomein, economische kwetsbaarheid en ambigue oorlogsvoering onderzocht. Duidelijk is dat deze verschijnselen een bedreiging kunnen vormen voor de benoemde nationale veiligheidsbelangen. Cyber in samenhang met georganiseerde criminaliteit kan de Nederlandse *economische veiligheid* aantasten. Deze is ook kwetsbaar voor internationale spanningen, het gebruik van economische sancties en instabiliteit in voor Nederland belangrijke regio's en gebieden. De *politieke en sociale stabiliteit* en *fysieke veiligheid* kunnen in het geding komen als gevolg van terroristische activiteiten, o.a. via polarisatie binnen de samenleving, en als gevolg van georganiseerde criminaliteit. Tot slot is daar het fenomeen van ambigue oorlogsvoering, dat weliswaar niet direct de Nederlandse territoriale veiligheid bedreigt, maar wel potentieel die van partners en bondgenoten (zie hiervoor), en die waar deze zich bedient van onder-

9 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Strategie Nationale Veiligheid. Den Haag, 2007, p.11. Zie ook: Ministerie van Buitenlandse Zaken, Veilige wereld, veilig Nederland; Internationale Veiligheidsstrategie. Den Haag, 21 juni 2013; WRR, Aan het buitenland gehecht; over verankering en strategie van Nederlands buitenlandbeleid. Amsterdam: Amsterdam U.Pr., 2010.

10 Clingendael Monitor 2012, 2013, 2014.

mijnende activiteiten via propaganda, cyber, etc. wel degelijk een gevaar voor de politieke en sociale stabiliteit kan vormen.

Het beschermen van de nationale veiligheid is primair een verantwoordelijkheid van de Nederlandse overheid. Tegelijkertijd laten de dreigingen zien dat deze door hun aard en oorsprong in veel gevallen slechts door samenwerking met anderen effectief kunnen worden bestreden en geneutraliseerd. In die zin kan in het geval van de onderscheiden Nederlandse veiligheidsbelangen worden gesproken over verlengde belangen, d.w.z. belangen die Nederland met andere landen deelt, maar die Nederland niet op eigen kracht, maar alleen in samenwerking met anderen kan behartigen. Dat geldt voor het meest primaire nationale belang: de bescherming van de territoriale integriteit, waar Nederland afhankelijk is van de bereidheid van de bondgenoten. Maar het geldt ook voor de andere benoemde veiligheidsbelangen in relatie tot de beschreven dreigingen.

Behartiging van deze belangen veronderstelt derhalve van Nederlandse kant een actieve inzet op internationale samenwerking in Europees, bondgenootschappelijk, VN- of ander verband en idealiter een internationale rechtsorde die mondiale veiligheid en stabiliteit waarborgt en die borging van door Nederland gepropageerde waarden en beginselen verzekert. Alleen met een dergelijke actieve inzet zal Nederland ook invloed kunnen uitoefenen.

De mondiale en regionale context

De verwachtingen ten aanzien van de in deze studie besproken bedreigingen voor de Nederlandse samenleving voor de komende 5 à 10 jaar moeten mede bezien worden in het licht van bredere ontwikkelingen zowel mondiaal als regionaal op het vlak van internationale veiligheid, stabiliteit en samenwerking. Zoals in de voorgaande paragraaf is aangegeven, is Nederland kwetsbaar voor externe ontwikkelingen en gebeurtenissen. Dit betekent dat het Nederlands belang bij een stabiel mondiaal bestel waarbinnen samenwerking overheerst, groot is.

De Clingendael Monitor 2015 ‘Een wereld zonder orde?’ laat zien dat op zowel mondiaal als regionaal niveau sprake is van ontwikkelingen die (potentieel) een bedreiging vormen voor de internationale veiligheid en stabiliteit en voor het functioneren van de bestaande kaders voor internationale samenwerking.[11] Mede als gevolg van het voortgaande proces van *mondiale machtsspreiding* is er sprake van toenemende spanningen tussen de grote mogendheden, ook wel de ‘terugkeer van de geopolitiek’ genoemd. Dit plaatst het bestaande multilaterale bestel van samenwerking en de daarmee verbonden internationale orde onder grote druk. Tegelijkertijd is er sprake van een sterke onderlinge afhankelijkheid van de belangrijkste spelers, in het bijzonder op financieel-economisch terrein. Een belangrijke vraag voor de komende periode is daarom of op mondiaal niveau de geopolitiek de relaties zal domineren of dat de wederzijdse interdependentie een matigend effect zal hebben op het gedrag van partijen. Het meest waarschijnlijke scenario voor de komende 5 à 10 jaar is dat van een *versmelting* van een meer multipolaire wereld met elementen van een multilateraal bestel. Met andere woorden, een wereld, waarin samenwerking sterker afhankelijk zal zijn van de relaties tussen de grote mogendheden – de VS en China in het bijzonder – en vaker ad hoc zal zijn en aldus buiten de formele kaders van de bestaande internationale

11 Zie: Jan Rood, Frans-Paul van der Putten en Minke Meijnders, Een wereld zonder orde?; Clingendael Monitor 2015. Den Haag: Instituut Clingendael, februari 2015.

organisaties. Kortom, de wereldorde zal gekenmerkt worden door een mix van rivaliteit en van samenwerking voor zover dat laatste de belangen van de grote spelers dient.

Onder dit mondiale niveau tekent zich een complex *regionaal* patroon van verhoudingen af. Drie '*hot spots'* zijn daarbij waar het (potentiële) dreigingen betreft, in het bijzonder relevant. Allereerst, de veiligheidspolitieke ontwikkelingen in Oost-Azië, waar de regionale ambities van China botsen met de rol van de VS als '*security provider'* voor een aantal landen in deze regio (o.a. Japan, Zuid-Korea en Taiwan) en daarmee met de Amerikaanse rol als '*balancer*', d.w.z. als tegenwicht tegenover de machtspolitieke aspiraties van China. De dynamiek in deze regio en in het bijzonder de verdere ontwikkeling van de Amerikaans-Chinese relatie zal in belangrijke mate de aard van het *mondiale* bestel bepalen.

Ten tweede, de veiligheidspolitieke ontwikkelingen de komende jaren in de MENA-regio en Sub-Sahara Afrika. Binnen deze regio is sprake van een ernstige destabilisering, die sterk aan kracht heeft gewonnen met de vestiging van Islamitische Staat in delen van Syrië en Irak, het optreden van Boko Haram in Nigeria en de activiteiten van Al Shabaab in de Hoorn van Afrika. In combinatie met de desintegratie van landen als Jemen, Libië, Mali en de Centraal-Afrikaanse Republiek en een internationale gemeenschap die niet in staat is om adequaat het hoofd te bieden aan deze groeperingen, biedt dit het vooruitzicht van verdere destabilisering, o.a. als gevolg van het verder uitwaaieren van ondermijnende en terroristische activiteiten naar andere landen in deze regio en daarbuiten. In de mate dat dit plaatsvindt, zal dit via de nexus externe-interne veiligheid gevolgen hebben voor Nederland en de Europese partners, o.a. in de vorm terroristische dreiging, vluchtelingenstromen, criminaliteit, etc.

Ten derde, het ambigue conflict dat zich afspeelt in het oosten van Europa, met op dit moment de vijandelijkheden tussen Rusland en Oekraïne als belangrijkste ijkpunt voor de toekomstige verhoudingen op het Europese continent. Voor die toekomstige verhoudingen is bepalend dat de Russische opstelling wordt ingegeven door de weigering om nog langer de uitgangspunten van de naoorlogse Europese orde zoals die ten tijde van de Koude Oorlog en in het bijzonder daarna, zijn uitgekristalliseerd – territoriale integriteit en erkenning van soevereiniteit – nog langer te accepteren. Daarnaast is sprake van afkeer van het westerse, in het bijzonder door de EU gepropageerde waardepatroon; dat is immers potentieel bedreigend voor de machthebbers in Moskou. In samenhang met de al dan niet gemanipuleerde gevoelens van frustratie en vernedering en de waarschijnlijkheid van een voortgaand economisch verval, wijst dit op een blijvend risico van instabiliteit in het oosten van Europa. De reikwijdte en intensiteit van de Russische agressie is daarbij moeilijk te voorspelen en zal mede afhangen van de westerse/Europese opstelling. Maar de huidige vorm van ambigue oorlogsvoering en ondermijning biedt de Russische machthebbers ruime mogelijkheid om indien gewenst onrust te veroorzaken in omringende gebieden. Hoe dan ook zal het vinden van een nieuwe *modus vivendi* met Moskou voor de EU/het Westen één van de grote uitdagingen voor de komende jaren worden.

De bredere context laat derhalve een wankele wereldorde zien, met het grondgebied van de EU omringd door een gordel van instabiliteit of, in de woorden van *The Economist*, *'a ring of fire'*.[12] Het hiermee samenhangende dreigingsbeeld is bovenal diffuus, waarbij dreigingen vaak met elkaar samenhangen en elkaar versterken. Voorbeelden hiervan zijn criminaliteit en

12 Zie: Jan Rood, Een wankele wereldorde; Clingendael Strategische Monitor 2014. Den Haag: Instituut Clingendael, juni 2014; Charlemagne, 'Europe's ring of fire'. In: The Economist (20 september 2014).

misbruik van het cyberdomein, economische oorlogsvoering met inzet van cyber en spionage, en de financiering van terroristische activiteiten met criminele middelen. Dit onderstreept dat effectieve bestrijding c.q. afschrikking een integrale benadering vereist; d.w.z. de beschikbaarheid en inzet van een breed palet aan middelen. Daarnaast zal in veel gevallen optreden in samenwerking met andere landen, in bondgenootschappelijk of EU-verband, noodzakelijk zijn; dit onverlet de noodzaak om waar mogelijk zelfstandig te handelen. Internationale samenwerking is vereist omdat in veel gevallen dreigingen zich via het grondgebied van andere landen manifesteren, Nederland zich via afspraken gecommitteerd heeft aan de bescherming van partners, en omdat Nederland in de wereld van vandaag en morgen een maatje te klein is om effectief tegenspel te kunnen bieden aan statelijke actoren als Rusland en China.

De vijf dreigingsthema's

De Nederlandse samenleving ziet zich direct of indirect geconfronteerd met verschillende dreigingen. In deze studie is, zoals reeds aangegeven, ervoor gekozen de dreigingen via het cyberdomein, het economisch domein, terroristische dreigingen, het gevaar van georganiseerde criminaliteit en door middel van ambigue oorlogsvoering te bestuderen. Elk van deze dreigingen is op zichzelf niet nieuw, maar de manier waarop de dreiging zich manifesteert is wel veranderd. Op elke individuele dreiging zal in de aparte bijlages verder worden ingegaan. In deze paragraaf volgt in vogelvlucht een schets van de actuele situatie en de verwachtingen voor de komende 5 à 10 jaar: wat is de aard van de dreigingen en hoe komen deze vijf verschillende dreigingen tot uiting? Wat zijn de verwachtingen wat betreft de toekomstige ontwikkelingen? Het gaat bij elk van de thema's om dreigingen die Nederland (gedeeltelijk) vanuit het buitenland kunnen treffen.

Ten eerste heeft Nederland te maken met *terroristische dreigingen*. Als gevolg van de recente gebeurtenissen in o.a. Parijs wordt de dreiging van terroristisch geweld ook vrij direct gevoeld in Nederland. De kans op een aanslag in Nederland of op Nederlandse belangen in het buitenland is door de Nederlandse overheid al enige tijd vastgesteld op substantieel. Tegelijkertijd is de aard van terroristische dreigingen de afgelopen jaren veranderd. Het religieus extremisme als drijfveer van terroristisch geweld heeft de laatste jaren aan kracht gewonnen. Terrorisme is bovendien sterk transnationaal van karakter geworden. Groeiende internationale (en grensoverschrijdende) terroristische netwerken als Al Qaida, de Taliban, Boko Haram, Al Shabaab, Al Nusra en ISIS leiden tot toenemende dreiging. Het groeiend aantal uitreizigers naar instabiele gebieden in het Midden-Oosten en Noord-Afrika en het risico dat deze zich aansluiten bij jihadistische groeperingen vormt, zodra deze *foreign fighters* terugkeren naar Nederland, een reëel risico voor de Nederlandse veiligheid. Met name de burgeroorlog in Syrië en de opkomst van ISIS trekt wereldwijd *foreign fighters* aan. De NCTV schat het aantal Nederlandse strijders dat is uitgereisd naar jihadgebieden op zo'n 190, waarvan er zo'n 35 zijn teruggekeerd en 30 zijn gesneuveld.[13] Het *International Centre for the Study of Radicalisation and Political Violence* (ICSR) schat dat aantal zelfs hoger: zo'n 200-250 strijders.[14] De kans dat teruggekeerde strijders uit oorlogsgebieden, al dan niet in georganiseerd verband, een aanslag plegen op Nederlands grondgebied is groter

13 NCTV, Beleidsimplicaties Dreigingsbeeld Terrorisme Nederland 38, Den Haag: NCTV, 7 april 2015.

14 Peter R. Neumann, 'Foreign fighter total in Syria/Iraq now exceeds 20,000', International Centre for the Study of Radicalisation and Political Violence, 26 januari 2015, http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/ (geraadpleegd 23 februari 2015).

geworden. Daarbij moet worden opgemerkt dat er ook vanuit thuisblijvende sympathisanten een dreiging uitgaat, zoals o.a. de aanslagen in Parijs en Canada hebben laten zien, waarbij niet alle daders teruggekeerde strijders waren.

Terrorisme vormt aldus niet alleen een fysieke dreiging voor burgers in Nederland en in het buitenland, maar het gevaar zit vooral in de maatschappelijke onrust die een aanslag kan veroorzaken, hetgeen zich kan uiten in verdere maatschappelijke polarisatie tussen en radicalisering van bevolkingsgroepen. In het licht van de blijvende instabiliteit en voortgaande conflicten in de MENA-regio en de uitwaaiering ervan naar andere gebieden is een blijvende en mogelijk toenemende terroristische dreiging voor Nederland en de Europese partners zeer waarschijnlijk. De MENA-regio, inclusief Sub-Sahara Afrika, West-Afrika en de Hoorn van Afrika, blijft een belangrijk operatiegebied voor terroristische groeperingen en in sommige gevallen daarmee een voedingsbodem voor het ondernemen van terroristische activiteiten op Europees grondgebied. Bestrijding in de regio zelf zal moeilijk blijven als gevolg van enerzijds onenigheid en onwil binnen de internationale gemeenschap, en anderzijds als gevolg van het vermogen van deze groeperingen om zich te nestelen binnen samenlevingen c.q. een georganiseerd, quasi-statelijk karakter te verwerven (zoals bijvoorbeeld ISIS en Boko Haram). Onzeker is of de terroristische dreiging zich tot deze regio zal beperken. Een heropleving van een dreiging uit de regio Afghanistan/Pakistan is bij een terugval in dit gebied niet uitgesloten. Tevens is gebruik van terrorisme als instrument van ambigue oorlogsvoering door Rusland niet ondenkbaar.

Twee additionele risico's onderstrepen de toekomstige dreiging die in het bijzonder van de MENA-regio uitgaat: de aantrekkingskracht van deze bewegingen op *foreign fighters*, met een toenemend gevaar van geweldgebruik door teruggekeerde jihadisten, en daarnaast het mobiliserende effect dat radicalisering en polarisatie binnen westerse/Europese samenlevingen kan hebben op *foreign fighters* en *home-grown* terroristen. Een gevaar dat mede moet worden bezien in het licht van het effectieve gebruik door terroristische groeperingen van propaganda via internet en sociale media als middel tot ronselen, ondermijning en radicalisering.

Ten tweede ziet Nederland zich in toenemende mate geconfronteerd met *dreigingen via het cyberdomein*. Digitale dreigingen worden door de AIVD gezien als één van de grootste dreigingen waar Nederland op dit moment mee te maken heeft.[15] De intensiteit en het gebruik van informatie- en communicatietechnologie (ICT) in allerlei sectoren is in de afgelopen jaren drastisch toegenomen, maar de beveiliging ervan loopt sterk achter. Daarmee neemt de mogelijke impact van een cyberaanval sterk toe. Volgens het Nationaal Cyber Security Centrum (NCSC) komt de grootste dreiging momenteel voort uit staten (in de vorm van cyberspionage) en van de kant van criminelen (door diverse vormen van cybercriminaliteit).[16] Van terroristen, cybervandalen, hackers en *scriptkiddies*[17] gaat op dit moment een minder grote dreiging uit. In het geval van cyberspionage gaat het om het blootleggen van gevoelige informatie van bedrijven, burgers of van de overheid, zoals over het defensie-, buitenland, economisch of energiebeleid. Aanvallen gepleegd door andere staten zijn in aantal sterk toegenomen volgens het NCSC, evenals hun intensiteit en impact. Cyberspionage

15 AIVD, Jaarverslag 2013, Den Haag: AIVD, april 2014.
16 Cybersecuritybeeld Nederland: CSBN-4. Nationaal Cyber Security Centrum, juli 2014, p. 7.
17 Personen die zich op het internet misdragen en daarbij gebruik maken van technieken die door anderen zijn ontwikkeld.

en cybercriminaliteit zijn in belangrijke mate gericht op het bedrijfsleven en vormen daarmee, hoewel het zeer lastig blijft de exacte omvang ervan vast te stellen, een grote economische schadepost. Begin dit jaar kwam bijvoorbeeld nog een omvangrijke digitale bankroof op internationaal niveau aan het licht, waarbij 100 banken uit 30 verschillende landen het slachtoffer werden en internetcriminelen ruim 260 miljoen euro wisten buit te maken.[18] Ook kunnen aanvallen via het cyberdomein direct gericht zijn op sabotage van de maatschappelijke en economische infrastructuur, wat mogelijk tot ernstige verstoring kan leiden. Met belangrijke economische knooppunten als de haven van Rotterdam en Schiphol, en met AMS-IX als één van de belangrijkste internetknooppunten ter wereld, is Nederland extra kwetsbaar voor dergelijke aanvallen. Het is ook niet ondenkbaar dat in ambigue oorlogs- en conflictsituaties er misbruik gemaakt zal worden van deze kwetsbaarheden. Tenslotte heeft het internet ook nieuwe mogelijkheden gecreëerd die de dreiging door criminelen en terroristen kunnen vergroten, zoals nieuwe mogelijkheden om handelswaar aan te bieden of om sympathisanten te rekruteren.

Voor Nederland geldt dat de cyberdreiging samen met georganiseerde criminaliteit, hoewel diffuus, waarschijnlijk aan kracht zal winnen. Dit laatste is primair een gevolg van de snelle ontwikkelingen op het terrein van ICT, de steeds gemakkelijker toegang tot deze technologie en de toegenomen afhankelijkheid van samenlevingen van een ongestoorde toepassing van ICT. Deze factoren maken moderne samenlevingen als de Nederlandse steeds kwetsbaarder voor misbruik van cyber. Daarbij hoeft dit misbruik zich niet tot Nederland te beperken. Een adequaat functioneren van Nederlandse instellingen is gegeven de internationale vervlechting van allerlei systemen (satellieten, financieel verkeer, etc.) ook kwetsbaar voor cyberaanvallen op andere landen of niet-Nederlandse instanties.

De twee belangrijkste dreigingen van het cyberdomein, cybercriminaliteit en cyberspionage, zullen naar alle waarschijnlijkheid in de toekomst verder aan kracht winnen. Toenemende cybercriminaliteit is mede een gevolg van de geringe pakkans en de gemakkelijke toegang tot ICT. Cyberspionage zal waarschijnlijk vaker voorkomen, ook door bevriende naties. Enerzijds hangt dit samen met de behoefte/noodzaak om in antwoord op een dreiging als terrorisme inlichtingen te verzamelen. Anderzijds past dit in een wereld waarin sterker sprake is van geopolitieke spanningen en economische wedijver. Hiermee is ook gezegd dat de inzet van cyber niet beperkt zal blijven tot traditionele bedrijfsspionage, maar op economisch terrein '*state-sponsored'* zal zijn. Gebruik van cyber in het kader van ambigue oorlogsvoering zal waarschijnlijk ook aan kracht winnen.

Ten derde heeft Nederland te maken met dreigingen die uitgaan van (internationale) *georganiseerde criminaliteit*. Georganiseerde criminaliteit komt in vele verschillende verschijningvormen voor. In het Nationaal Dreigingsbeeld van de Korps Landelijke Politiediensten worden drie categorieën van criminele verschijnselen onderscheiden: verschillende illegale markten met o.a. handel in drugs, mensen of kinderporno; witwassen en fraude; en vermogenscriminaliteit (hieronder verstaat de politie criminaliteit uit het zogenaamde middensegment, zoals inbraak en diefstal).[19] De aard van de georganiseerde misdaad is nauw verbonden met de geografische positie en fysieke en digitale infrastructuur van

18 'Digitale bankrovers stelen zeker 260 miljoen euro'. In: *NRC Handelsblad*, 16 februari 2015.

19 F. Boerman, M. Grapendaal, F. Nieuwenhuis en E. Stoffers, Nationaal Dreigingsbeeld 2012: Georganiseerde Criminaliteit. Zoetermeer: KLPD. December 2012, p. 30-31.

Nederland en laat zich het best omschrijven als 'transitcriminaliteit'.[20] Georganiseerde criminaliteit concentreert zich op internationale handel. Nederland speelt een dominante rol op de internationale misdaadmarkt, vooral als het gaat om drugs, mensenhandel, fraude, witwassen en cybercrime. Het is echter heel lastig – zo niet onmogelijk – de totale schade van georganiseerde misdaad vast te stellen, omdat het bijvoorbeeld ook gaat om immateriële zaken als reputatieverlies, zo stelt de meest recente Monitor Georganiseerde Criminaliteit.[21]

Gezien zijn geografische positie blijft Nederland ook voor de komende 5 à 10 jaar aantrekkelijk voor internationaal opererende criminelen. Daarbij zal georganiseerde criminaliteit, ten eerste, vooral een bedreiging vormen voor de maatschappelijke en politieke stabiliteit. Zo kan het de marktwerking verstoren, leiden tot het verlies van vertrouwen in het handelsverkeer en de financiële sector, maar ook bijvoorbeeld de reputatie aantasten van belangrijke economische knooppunten als Schiphol en de Rotterdamse haven als veilige doorvoerpunten. Dit effect zal sterker zijn naarmate criminelen er in slagen zich middels corruptie en omkoping in de bovenwereld te nestelen. Daarnaast zal georganiseerde criminaliteit ook negatieve economische effecten kunnen bewerkstelligen, waarbij het gaat om tal van activiteiten, waaronder in het bijzonder cybercriminaliteit, witwassen en allerlei vormen van illegale transacties die het vertrouwen in de economie ondermijnen.

Ontwikkelingen buiten Nederland zijn hierbij een belangrijke katalysator. Gegeven de eerder beschreven instabiliteit in de MENA-regio is er een groter gevaar dat vluchtelingenstromen worden misbruikt door mensenhandelaren als kanaal voor de 'export' van criminele activiteiten. Hoe dan ook brengt het ontstaan van gebieden waarin het ontbreekt aan effectieve vormen van overheidsgezag het risico met zich mee dat deze bronnen van criminaliteit worden, van waaruit ook activiteiten op Europees grondgebied worden ontplooid. Gegeven de instabiliteit in de MENA-regio neemt dit gevaar toe, waarbij zij opgemerkt dat ook in delen van Latijns-Amerika en Midden-Amerika overheden in delen van het eigen grondgebied plaats hebben moeten maken voor criminele groeperingen.

Ten vierde ziet Nederland zich geconfronteerd met *dreigingen via het economisch domein*. De aard van deze dreigingen hangt nauw samen met de open, internationaal georiënteerde economie van Nederland. De dreiging komt van verschillende actoren (staten, criminele organisaties en terroristen) en valt uiteen in verschillende types. Ten eerste valt te denken aan expliciete of impliciete economische druk, zoals de sancties die afgelopen zomer door Rusland zijn ingesteld als reactie op het Europese en Amerikaanse pakket aan sancties naar aanleiding van de annexatie van de Krim. Sancties worden vaker ingezet als politiek drukmiddel en zijn omvangrijker en doeltreffender dan in het verleden, vooral dankzij de sterke verwevenheid van Nederland met de internationale markt. Ten tweede kan het strategisch-economisch beleid van andere staten, bijvoorbeeld als onderdeel van hybride oorlogsvoering, potentieel gevolgen hebben voor de Nederlandse nationale veiligheid, bijvoorbeeld als dat leidt tot beperkte toegang tot voor Nederland belangrijke grondstoffen. Ten derde kan instabiliteit in voor Nederland belangrijke gebieden nadelige gevolgen hebben, bijvoorbeeld ook hier voor de toevoer van essentiële grondstoffen. Deze dreigingen hebben vooral effect op de economische veiligheid van Nederland. Tot slot zijn er dreigingen waarbij

20 E.W. Kruisbergen, H.G. van de Bunt en E.R. Kleemans, Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit. Den Haag/Rotterdam: WODC/ Erasmus Universiteit. 2012, p. 16.

21 Idem, p. 34

het economische en het cyberdomein overlappen, en die economische kernprocessen kunnen verstoren. Hierbij valt te denken aan energieproductie, communicatie, transport, geldverkeer, etc. Dit kan dan niet alleen gevolgen hebben voor de economische veiligheid van Nederland, maar tast potentieel ook de maatschappelijke stabiliteit aan.

De dreigingen op het economisch vlak zullen naar verwachting ook niet afnemen in de toekomst. Allereerst niet vanwege de eerder geschetste bredere mondiale context, die duidt op een wereld die de komende jaren minder geordend en stabiel zal zijn. Dit betekent dat waar Nederland economisch belang heeft bij een open en stabiel mondiaal bestel, in het bijzonder financieel en economisch, dit belang verder onder druk zal komen te staan. In deze vooral op regionaal niveau instabielere wereld is er een groter risico dat het directe Nederlandse belang bij vrije toegang tot markten, vrije doorvoer over water en door de lucht, en een ongestoorde aanvoer van energie en grondstoffen in het geding komt als gevolg van economische wedijver en politieke spanningen (inclusief sancties), van regionale instabiliteit en conflicten, dan wel van binnenlandspolitieke onrust. Hierbij zij opgemerkt dat in het bijzonder waar het de aanvoer van grondstoffen en energie betreft, Nederland in samenwerking met de Europese partners afhankelijk is van landen/regio's waarmee de relatie gespannen is (Rusland), die instabiel zijn (MENA-regio), dan wel landen waarvan de langere termijn stabiliteit allerminst zeker is (Saoedi-Arabië). Deze situatie zal op de voorzienbare termijn niet in gunstige zin veranderen.

Tot slot is daar een verschijnsel dat recent sterk in de aandacht is gekomen, namelijk *ambigue oorlogsvoering*. Oorlogsvoering is ambigu wanneer een betrokken partij in de context van het gewapende conflict handelingen verricht waarbij zij dit heimelijk doet, haar identiteit verborgen houdt, zich voordoet als een andere partij of ten onrechte ontkent dat deze handelingen erop gericht zijn de tegenstander te treffen. Zulke handelingen zijn vaak gericht op het creëren van verwarring en onzekerheid, waarbij de ontkenbaarheid van de verantwoordelijkheid voor het betreffende handelen voor de dader een centraal element is.[22] Juist door de inzet van geavanceerde, moderne middelen en door de sterke verwevenheid van landen onderling, is dergelijke oorlogsvoering tegenwoordig makkelijker en effectiever en is het effect mogelijk ook groter. De ambigu optredende staat kan gebruik maken van geanonimiseerde militaire middelen, al dan niet in combinatie met niet-militaire middelen, zoals impliciete economische druk en cyberaanvallen. Grootschalige informatie- en propagandacampagnes en heimelijke steun aan lokale (*'proxy'*) groeperingen kunnen bijdragen aan het creëren van onzekerheid over welke actor verantwoordelijk is voor bepaalde acties. Kenmerkend voor dit type oorlogsvoering is dat er ontkenbaarheid voor de eigen betrokkenheid wordt nagestreefd, waardoor een tegenactie moeilijk te rechtvaardigen is. Een actueel voorbeeld van het gebruik van ambigue oorlogsvoering, is het Russische militaire optreden in Oekraïne (zie box 1). Dit dreigingsthema is relevant voor Nederland wat betreft het functioneren van de internationale rechtsorde, de geloofwaardigheid van de NAVO en de EU als organisaties die cruciaal zijn voor onze nationale veiligheid en voor het gevaar van directe of indirecte schade aan voor ons vitale infrastructuur door ambigue militaire acties.

22 Ambigue oorlogsvoering is niet hetzelfde als hybride oorlogsvoering. Bij ambigue oorlogsvoering gaat het om de ontkenbaarheid, bij hybride oorlogsvoering gaat het om oorlogsvoering met alle mogelijke middelen, dus ook economisch, diplomatiek, via propaganda, cyberaanvallen etc. Deze twee vormen van oorlogsvoering kunnen als combinatie voorkomen.

Russische militairen op de militaire basis in Perevalne, Oekraïne tijdens de annexatie van de Krim in maart 2014. *Foto: Anton Holoborodko/Wikimedia Commons.*

Waar het Nederland en de Europese bondgenoten betreft, zal de dreiging in de toekomst voornamelijk vanuit Rusland komen. Het lijkt waarschijnlijk dat Rusland zal volharden in de huidige opstelling en met inzet van alle middelen zal proberen invloed uit te oefenen op zijn omgeving. Dit impliceert ook pogingen om het Westen te verdelen door landen tegen elkaar uit te spelen c.q. de publieke opinie voor het Russische standpunt te winnen. Daarom zal rekening moeten worden gehouden met een variatie aan activiteiten die passen binnen deze vorm van ambigue oorlogsvoering, lopend van subtiele economische sancties c.q. steun, via propaganda, desinformatie en politieke manipulatie en beïnvloeding tot en met direct ondermijnende activiteiten, via cyber en anderszins. Voor Nederland en de EU ligt de dreiging voor de komende periode primair in de relatie met Rusland. De kans dat ook andere landen de 'voordelen' van deze vorm van oorlogsvoering gaan onderkennen en dit dus vaker zal gaan voorkomen is reëel.

Box 1 De crisis in Oekraïne en ambigue oorlogsvoering

De vijandelijkheden in het oosten van Oekraïne en de annexatie van de Krim door Rusland in maart 2014 hebben de aandacht gevestigd op ambigue oorlogsvoering. Rusland speelt volgens westerse analisten een grote rol in Oost-Oekraïne en op de Krim. Zo bleken de zogenoemde 'groene mannetjes' op de Krim Russische speciale eenheden en eenheden van de marine infanterie te zijn. Met coördinatie en steun vanuit Moskou werden daarnaast de Oekraïense separatisten van een arsenaal aan wapens voorzien. Zowel de aanwezigheid van artillerie en tanks als geavanceerde anti-vliegtuig raketsystemen in het oosten van Oekraïne lijken deze betrokkenheid van Russische

troepen te bevestigen. Ook de toename van luchtruimschendingen bij EU- en NAVO-lidstaten door Russische militaire vliegtuigen,[23] de cyberaanvallen op en ontvoeringen in de Baltische staten en de mogelijke aanwezigheid van een Russische onderzeeër in Zweedse wateren passen binnen dit beeld en hebben tot oplopende spanningen tussen Rusland en het Westen geleid.

Deze militaire acties en betrokkenheid zijn onderdeel van een bredere strategie waarbij gebruik wordt gemaakt van een breed palet aan middelen, zoals indirecte interventies, geheime operaties, politieke beïnvloeding van de tegenstander, economische chantage, cyberaanvallen, propaganda en misleiding. Daarbij beperkt het Russische optreden zich niet tot de omringende landen, maar heeft het ook tot doel om verdeeldheid te zaaien binnen het kamp van EU- en NAVO-lidstaten, met onder andere als doel om steun voor zwaardere sancties tegen Rusland te ondermijnen. Dit gebeurt door zowel linkse als rechtse populistische politieke partijen binnen de EU financiële steun te bieden, door het omkopen van politici en zakenlieden, en door landen die voor hun energie van Rusland afhankelijk zijn onder druk te zetten. In Rusland zelf wordt daarnaast een desinformatiecampagne gevoerd door de door het Kremlin gecontroleerde Russische media strak in de greep te houden. Volgens sommigen is het denkbaar dat gegeven het Russische optreden ook andere staten deze wijze van oorlogsvoering zullen gaan toepassen. Zo zouden ook Aziatische landen die betrokken zijn bij territoriale geschillen in de Zuid-Chinese Zee met ambigue oorlogsvoering nieuwe spanningen kunnen creëren. Datzelfde geldt ook voor landen in het Midden-Oosten. Een belangrijke vraag voor het Westen is hoe hierop te reageren.

Relevantie van afschrikking als veiligheidsconcept

Hieronder wordt aangegeven op welke manier afschrikking als veiligheidsconcept relevant is voor de vijf dreigingsthema's die centraal staan in dit rapport. De inzichten zijn geordend aan de hand van het analysekader dat in paragraaf 2 werd geïntroduceerd en gebaseerd op de verkennende analyses per dreigingsthema die als bijlagen bij dit rapport zijn gevoegd.

Afschrikking met betrekking tot alle vijf dreigingsthema's

Het doel van afschrikking is potentiële daders te ontmoedigen door beïnvloeding van hun kosten/baten-inschatting. Wanneer de verwachte kosten verbonden aan een voor Nederland schadelijke handeling omhoog gaan en/of de verwachte baten afnemen wordt het minder aantrekkelijk voor de dader om deze handeling uit te voeren. De meest effectieve benadering omvat daarom, waar mogelijk, maatregelen die zowel op de kosten- als de batenzijde gericht zijn.

Er zijn wat betreft de in dit rapport besproken dreigingsthema's drie vormen van afschrikking die in veel gevallen toepasbaar lijken. Ten eerste is er aan de kostenzijde de dreiging van vergelding door middel van juridische, economische of militaire middelen. Wanneer een dader weet dat zijn actie zeer waarschijnlijk tot onwenselijke vergeldingsmaatregelen leidt wordt het minder aantrekkelijk om deze daad uit te voeren. Ten tweede is er aan de

23 Lizzie Dearden, 'Full list of incidents involving Russian military and Nato since March 2014'. In: *The Independent*, 10 november 2014.

batenzijde de mogelijkheid om de eigen weerbaarheid te vergroten, bijvoorbeeld door middel van crisisbeheersingsmaatregelen of andere maatregelen die het vertrouwen van de bevolking versterken. Aanvallen die tot doel hebben om maatschappelijke onrust te veroorzaken worden daardoor minder snel effectief en dus minder aantrekkelijk voor de potentiële aanvaller. Ten derde is er de mogelijkheid om extra beveiligingsmaatregelen te treffen door investeringen in bewaking en in fysieke of technologische barrières. Dit kan zowel de kosten- als de bateninschatting beïnvloeden omdat ze enerzijds daders tot grotere voorinvesteringen dwingen (hogere kosten) en anderzijds hun kans op succes verkleinen (lagere baten). Doorslaggevend bij alle vormen van afschrikking is de *perceptie* bij de dader van de balans tussen kosten en baten. Een essentieel onderdeel van alle mogelijke afschrikkingsmaatregelen is daarom de zichtbaarheid ervan, en dus de wijze waarop ze gecommuniceerd worden. Maatregelen die voor potentiële daders onzichtbaar zijn hebben immers voor die specifieke doelgroep geen afschrikkende functie.

Wat betreft de relevantie van afschrikking voor de verschillende typen actoren kan worden gesteld dat een betere beveiliging op alle actoren van toepassing is, maar dat de relevantie van vergelding en van een grotere weerbaarheid verschillend is per actor. Zoals hieronder en in de bijlagen nader wordt aangegeven is vergelding beperkt toepasbaar tegen terroristen, en heeft het versterken van de eigen weerbaarheid geen afschrikkende werking tegen criminelen. Verschillen in motivatie bij de actoren zijn hierbij de voornaamste variabele. Actoren die vergelding niet vrezen (terroristen) kunnen niet worden afgeschrikt door de dreiging ervan, en hetzelfde geldt voor investeringen in weerbaarheid tegen actoren die niet naar maatschappelijke ontwrichting streven (criminelen). In het geval van statelijke actoren hangt het af van hun motieven welke vormen van afschrikking relevant kunnen zijn.

Tenslotte moet worden opgemerkt dat veel van de hieronder genoemde middelen meerdere veiligheidsdoelen kunnen dienen: naast afschrikking kunnen ze ook op andere wijzen bijdragen aan een grotere veiligheid. Dit geldt bijvoorbeeld voor investeringen in betere beveiliging of crisisbeheersing. Ook als deze geen afschrikkende werking hebben kunnen ze helpen om de schade door aanvallen of aanslagen te beperken. Wat daarbij verschillend is ten opzichte van de afschrikkingsfunctie is dat de nadruk dan verschuift van de perceptie bij de daders (*heeft de zichtbaarheid van extra beveiliging een ontmoedigend effect?*) naar de concrete werking van dergelijke maatregelen (*is een daadwerkelijke aanslag moeilijker uit te voeren?*).

TERRORISME

Relevante actoren
- Individuele terroristen/terroristische organisaties;
- *Facilitators*.

Beïnvloeding kostenperceptie
De werking van vergeldingsdreigingen is in veel gevallen beperkt omdat terroristen vanwege hun religieuze of politieke overtuiging vergelding vaak niet vrezen.
De inzet van vergeldingsmaatregelen kan zelfs contraproductief werken doordat het tot bredere steun kan leiden voor terroristen onder bevolkingsgroepen waaruit de terroristen afkomstig zijn. Waarneembare versterking of grotere zichtbaarheid van verdedigingsmechanismen zoals de fysieke aanwezigheid van beveiligers of surveillancemiddelen draagt bij aan afschrikking tegen terrorisme, omdat daders daarmee genoodzaakt worden grotere investeringen te doen in de voorbereiding tot een aanslag.

Beïnvloeding batenperceptie
Maatregelen gericht op het verkleinen van de gelegenheid tot het uitvoeren van een terreurdaad of de kans op succes daarvan zijn een relevant afschrikkingsmiddel. Daarom kunnen zichtbare investeringen in verdedigingsmechanismen ook aan de batenkant een belangrijk middel zijn. In dit geval gaat het niet, zoals aan de kostenzijde, om grotere voorinvesteringen door daders maar om de inschatting dat de kans op succes kleiner wordt. Ook capaciteiten die zichtbaar bijdragen aan vroegtijdige ontdekking van pogingen tot aanslagen (inlichtingendiensten) kunnen daarom terroristen afschrikken. Het overtuigen van terroristen dat terreurdaden niet bijdragen aan het doel dat ze nastreven draagt eveneens bij aan afschrikking. *Counter-narratives* zijn hierbij een middel om terroristen tot deze overtuiging te brengen of steun uit hun sociale omgeving te verminderen. Een ander relevant middel is het zichtbaar vergroten van de eigen weerbaarheid binnen de samenleving, bijvoorbeeld wat betreft het goed voorbereid zijn op noodsituaties en het publieke vertrouwen in het functioneren van de overheid. Immers een meer weerbare samenleving is minder snel ontwricht en dus zijn terreurdaden dan minder zinvol. Ook een hoge maatschappelijke weerbaarheid in de zin van het niet ontvankelijk zijn voor extremistisch of terroristisch gedachtengoed kan van invloed zijn op de bateninschatting door terroristen.

Categorieën van mogelijk relevante instrumenten
- Strafrecht;
- Fysieke en digitale beveiliging;
- Communicatie;
- Crisisbeheersing;
- Deradicaliseringsbeleid;
- *Counter-narratives*;
- Versterken signalering.

CYBERDREIGINGEN

Relevante actoren
- Staten (inclusief door staten aangestuurde *hackers*);
- Individuele criminelen/criminele organisaties;
- Individuele terroristen/terroristische organisaties.[24]

Beïnvloeding kostenperceptie
De tegendreiging van vergelding is beperkt toepasbaar doordat het lastig kan zijn om de dader achter een cyberaanval te identificeren (als die verborgen wil blijven), of zelfs de aanval zelf te signaleren (als het om spionage gaat). Voor de identificatie van daders en het nemen van vergeldingsmaatregelen is het vaak van belang dat het land waar de dader zich bevindt meewerkt. In het geval dat statelijke actoren de aanval uitvoeren is die mogelijkheid er dus niet. Vergelding tegen cyberdreigingen kan onder andere de vorm hebben van vervolging en straf (bij criminele actoren) of economische sancties (bij statelijke actoren). Een zwaardere tegendreiging tegen statelijke actoren kan bovendien worden gecreëerd met militaire middelen (conventioneel dan wel op

24 Hier zijn 'kleinere' actoren als *scriptkiddies*, hacktivisten e.d. niet inbegrepen. CSBN-4 geeft aan dat de grootste dreiging uitgaat van staten, terroristen en beroepscriminelen: Cybersecuritybeeld Nederland: CSBN-4. Nationaal Cyber Security Centrum, juli 2014.

het gebied van cyberoorlogsvoering). Zo heeft de Amerikaanse regering in april 2015 bijvoorbeeld bekend gemaakt dat zij bij ernstige aantasting van de nationale veiligheid door cyberacties van andere staten gebruik zal maken van vergelding, indien nodig met militaire middelen.[25] De moeilijkheid om een geschikte mate van proportionaliteit te bepalen is echter een complicerende factor bij vergelding. Waarneembare verbetering van verdedigingsmechanismen draagt bij aan afschrikking tegen cyberdreigingen wanneer dit tot hogere kosten wat betreft geld of tijd aan de kant van de dader leidt.

Beïnvloeding batenperceptie
Het overtuigen van politiek gemotiveerde actoren (staten of terroristen) dat cyberaanvallen niet bijdragen aan het doel dat ze nastreven draagt bij aan afschrikking. Een relevant middel hiertoe is het zichtbaar vergroten van de eigen weerbaarheid, ook wel *cyberresilience* genoemd, bijvoorbeeld door het zorgen voor redundantie. Cyberaanvallen door staten die op ontwrichting zijn gericht kunnen op deze wijze mogelijk worden ontmoedigd. Dit geldt niet voor cyberaanvallen die op spionage of illegale vermogensvergaring zijn gericht omdat eventueel ontwrichtende effecten voor de dader niet direct relevant zijn. Verder zijn zichtbare investeringen in een betere verdediging zoals veelgelaagde *firewalls,* geavanceerde encryptie- en authenticatiemiddelen en zogenaamde *'honeypots'* relevant wanneer deze tot gevolg hebben dat daders hun kans op succes lager inschatten.

Categorieën van mogelijk relevante instrumenten
- Strafrecht;
- Digitale beveiliging (encryptie e.d.) ofwel cybersecurity;
- Vermogen tot ontmaskering;
- Vergroten van *cyberresilience*.

CRIMINELE ORGANISATIES

Relevante actoren
- Individuele criminelen/criminele organisaties;
- *Facilitators*.

Beïnvloeding kostenperceptie
Afschrikking door middel van het dreigen met vergelding (vervolging en straf) is relevant als veiligheidsconcept tegen criminelen. Daarnaast kan de dreiging van een beperkte vergelding tegen personen in de sociale omgeving van criminelen (*facilitators*) relevant zijn om de steun die zij vanuit deze omgeving ontvangen te verzwakken. Deze steun is vaak essentieel voor criminelen omdat ze hun reputatie en status erop baseren. Het kan hierbij gaan om maatregelen gericht tegen de financiële belangen van deze *facilitators*, bijvoorbeeld door het beslagleggen op goederen die op naam van vertrouwelingen en familieleden van veroordeelde criminelen staan. Vergelding kan ook doeltreffend zijn tegen *facilitators* die achter een legale façade werken om daarmee een illegaal doel te ondersteunen. Zij hebben een reputatie te verliezen en zijn af te schrikken door de dreiging dat ze openlijk met criminaliteit geassocieerd worden. Toepassing van afschrikking door vergelding op internationaal

25 US Department of Defense, 'Carter Unveils New DoD Cyber Strategy in Silicon Valley', 23 april 2015, http://preview.defenselink.mil/news/newsarticle.aspx?id=128659; 'Preparing for Warfare in Cyberspace'. In: *The New York Times*, 28 april 2015.

niveau vereist veelal medewerking van het land waarin de criminelen of hun *facilitators* zich bevinden. Het versterken van verdedigingsmechanismen leidt tot een hogere kosten-inschatting en is daarom ook in het geval van criminelen een relevant aanvullend afschrikkingsmiddel.

Beïnvloeding batenperceptie
Het lijkt niet waarschijnlijk dat criminelen ervan kunnen worden overtuigd dat het door hen nagestreefde achterliggende doel bij schadelijk handelen onhaalbaar is. Afschrikking door middel van het versterken van de eigen weerbaarheid lijkt daarom in dit geval niet van toepassing te zijn. Aan de batenzijde zijn daarom alleen maatregelen gericht op het verkleinen van de gelegenheid tot het uitvoeren van criminele activiteiten of de kans op succes een relevant afschrikkingsmiddel: zichtbare investeringen in verdedigingsmechanismen vormen een belangrijk middel daartoe.

Categorieën van mogelijk relevante instrumenten
- Strafrecht;
- Fysieke beveiliging;
- Digitale beveiliging/cybersecurity;
- Vermogen tot ontmaskering.

DREIGINGEN VIA HET ECONOMISCHE DOMEIN

Relevante actoren
- Staten;
- Individuele criminelen/criminele organisaties;
- Individuele terroristen/terroristische organisaties.

Beïnvloeding kostenperceptie
Afschrikking door middel van het dreigen met vergelding (economische sancties) is relevant als veiligheidsconcept tegen statelijke actoren die een dreiging via het economische domein vormen. Ook waar het gaat om criminele organisaties die dit doen is deze vorm van afschrikking relevant. De effectiviteit van de dreiging met sancties als vergeldingsmiddel neemt sterk toe als dit in multilateraal verband wordt gedaan. Gerichte sancties (*smart sanctions*) kunnen effectiever zijn, dan wel minder schadelijke neveneffecten hebben, dan brede sancties. Het lijkt echter onwaarschijnlijk dat de dreiging van een buitenlandse consumentenboycot kan worden afgeschrikt door middel van vergelding als tegendreiging als deze boycot spontaan is ontstaan vanuit maatschappelijke organisaties en individuele initiatiefnemers en niet geregisseerd is door statelijke actoren. Evenals bij de overige dreigingsthema's is ook bij dreigingen via het economische domein een betere verdediging relevant waar het gaat om aanvallen door criminelen of terroristen. Ook het vergroten van de kans op reputatieschade bij de dader kan afschrikkend werken tegen statelijke actoren. Voorwaarde hierbij is dat er duidelijke normen zijn die door staten overtreden worden wanneer ze via het economische domein de veiligheid van andere staten zoals Nederland bedreigen.

Beïnvloeding batenperceptie
Wanneer staten streven naar het uitoefenen van druk via economische of sociale ontwrichting door middel van acties via het economische domein kan het ondermijnen van de gedachte dat dit doel haalbaar is bijdragen aan afschrikking. Het beschikken over alternatieven is hiervan een voorbeeld. Een relevant middel

hiertoe is het zichtbaar vergroten van de eigen weerbaarheid. Zichtbare investeringen in verdedigingsmechanismen, zoals betere internetbeveiliging in het geval van (economische) cyberdreigingen, kunnen de batenperceptie van daders beïnvloeden.

Categorieën van mogelijk relevante instrumenten
- Economisch beleid;
- Beleidsvermogen tot sancties;
- Vermogen tot ontmaskering;
- Fysieke en digitale beveiliging.

AMBIGUE OORLOGSVOERING

Relevante actoren
- Staten.

Beïnvloeding kostenperceptie
De tegendreiging van vergelding is in dit geval beperkt toepasbaar doordat het bij ambigue oorlogsvoering per definitie lastig of zelfs onmogelijk is de dader te identificeren, of – in het geval van heimelijke acties – zelfs het betreffende ambigue handelen te signaleren. In combinatie met een zichtbaar vermogen om de actor achter een ambigue actie te identificeren kan de dreiging van vergelding wel afschrikkend zijn. Het is daarbij noodzakelijk dat dit vermogen mede inhoudt dat de identiteit van de verantwoordelijke dader op overtuigende wijze kan worden aangetoond en als zodanig wordt geaccepteerd door derden (publieke opinie, internationale media e.d.). Als het voorgaande het geval is dan omvatten mogelijke vergeldingsmiddelen de inzet van militaire middelen of economische sancties, waarbij inzet in multilateraal verband een aanzienlijk grotere mate van effectiviteit heeft. In dit geval heeft vergelding dezelfde werking als bij afschrikking tegen klassieke militaire dreigingen (zie box 2). Daarnaast is vergelding door middel van ambigue tegenacties ook een mogelijkheid, die echter als nadeel op de langere termijn heeft dat daarmee de werking van normen die ambigue oorlogsvoering moeten voorkomen ondermijnd worden. Afgezien van vergeldingsmiddelen kunnen ook betere verdedigingsmechanismen bijdragen aan afschrikking tegen ambigue oorlogsvoering als ze kunnen worden gecombineerd met een zichtbaar vermogen om de identiteit van de betreffende ambigue actor overtuigend aan te tonen. Ook het vergroten van de kans op reputatieschade bij de dader – door ontmaskering in combinatie met de aanwezigheid van breed geaccepteerde normen tegen ambigue oorlogsvoering – kan de kosten-inschatting verhogen.

Beïnvloeding batenperceptie
Wanneer staten ambigue oorlogsvoering toepassen om daarmee ontwrichting te veroorzaken van een samenleving of een internationale coalitie kan het ondermijnen van de gedachte dat dit doel haalbaar is bijdragen aan afschrikking. Een relevant middel hiertoe is het zichtbaar vergroten van de weerbaarheid van de betreffende samenleving of coalitie, bijvoorbeeld door te laten zien over een adequate crisisbeheersing te beschikken waardoor het vertrouwen van de bevolking in het functioneren van de samenleving niet snel ondermijnd wordt. Bij ambigue oorlogsvoering die gericht is op meer beperkte doelen zoals territoriale winst is deze vorm van afschrikking niet van toepassing. Tenslotte kan ook een groter vermogen tot verdediging, in de eerste plaats met militaire middelen, bijdragen aan afschrikking als dit de gepercipieerde kans op succes aan de kant van de aanvaller verkleint.

Categorieën van mogelijk relevante instrumenten
- Vermogen tot hybride tegenoffensief;
- Militaire middelen;
- Economische middelen/beleidsvermogen tot sancties;
- Diplomatie, fysieke en digitale beveiliging;
- Vermogen tot ontmaskering;
- Crisisbeheersing;
- Communicatie/*counternarratives*.

Box 2 Afschrikking als middel tegen klassieke militaire dreigingen

Dit kader hanteert als definitie van klassieke militaire dreiging 'de openlijke bedreiging met reguliere strijdkrachten van de integriteit van het grondgebied óf de belangen van een staat, in potentie leidend tot aantasting van de soevereiniteit van de bedreigde staat.' In tegenstelling tot bij ambigue oorlogsvoering gaat het hier om een zichtbare militaire bedreiging waarbij de verantwoordelijke staat identificeerbaar is.

De territoriale integriteit van Nederland lijkt niet actueel bedreigd. Zelfs bij beschouwing van het gehele Koninkrijk der Nederlanden kunnen we stellen dat, met het meer normaliseren van de regionale opstelling van Venezuela, er geen directe bedreiging is. Als we echter ook rekening houden met bondgenootschappelijke verplichtingen en de deelname aan militaire vredes- en stabilisatiemissies, dan is de kans dat de Nederlandse krijgsmacht te maken krijgt met klassieke militaire dreigingen aanzienlijk groter. Dreigingen die niet direct tegen Nederland gericht zijn, en waartegen de Nederlandse krijgsmacht in multinationaal verband optreedt lijken daarom voorlopig het meest te zullen voorkomen. Afschrikking wordt van oudsher toegepast als veiligheidsconcept tegen klassieke militaire dreigingen en blijft in de geschetste context dus ook voor Nederland relevant.

Een eerste optie om afschrikking ten opzichte van klassieke militaire dreigingen te creëren is door een sterk militair potentieel in huis te hebben. Een actor zal niet overgaan tot klassieke inzet van zijn militaire machtsmiddel wanneer de tegenpartij naar inschatting militair sterk genoeg is om te voorkomen dat die inzet het beoogde doel bereikt. Wanneer het niet haalbaar is om afdoende macht voor afschrikking te creëren met conventionele troepen en bewapening, kunnen onconventionele inzetmiddelen[26] wellicht hetzelfde doel bereiken. Nederland heeft de keuze gemaakt om niet te beschikken over nucleaire, chemische of biologische wapens. Een tweede mogelijkheid – waar Nederland ook inderdaad gebruik van maakt – is om aansluiting te zoeken bij een bondgenootschap.

26 CBRN: Chemisch, Biologisch, Radiologisch/Nucleair, maar ook cyber bijvoorbeeld.

Een dergelijk bondgenootschap kan als geheel in staat zijn om voldoende militair potentieel te onderhouden voor afschrikking van mogelijke opponenten. Een derde optie om afschrikking te creëren is het vermogen tot beslissende inzet van niet-militaire machtsmiddelen van de staat,[27] vooral economische middelen. Het vermogen van Nederland om hiermee op eigen kracht afschrikking te bereiken is echter beperkt. De vierde mogelijkheid is dan ook internationale samenwerking te zoeken waarmee economische druk kan worden gecreëerd. Nederland heeft deze optie gevonden door zijn lidmaatschap van de EU. De gezamenlijke economie van de EU zou in voorkomend geval van inzet als machtsmiddel een zeer significante factor zijn en vormt derhalve een potentiële afschrikking.

Nederland beschikt over conventioneel-militaire en economische middelen die ter afschrikking kunnen worden ingezet, bij voorkeur in een internationaal verband. Beide kunnen (ook) in het geval van klassieke militaire dreigingen worden onderverdeeld in afschrikking door het vergroten van de kosten-inschatting bij de aanvaller (met name door de vergeldingsdreiging), en afschrikking door het verkleinen van de baten (met name door betere weerbaarheid).[28] Nederland beschikt niet over een eigen capaciteit tot nucleair-militaire afschrikking, het middel dat ten tijde van de Koude Oorlog centraal stond bij het denken over afschrikking. Maar net als tijdens de Koude Oorlog bevindt Nederland zich onder de nucleaire 'paraplu' van de NAVO, en kan nucleaire afschrikking dus indirect nog altijd relevant zijn als middel tegen klassieke militaire dreigingen. Nucleaire afschrikking is na het einde van de Koude Oorlog naar de achtergrond verdwenen, mede doordat het maar beperkt van toepassing was tegen niet-traditionele dreigingen,[29] maar nu lijkt die situatie weer enigszins te veranderen. De huidige geopolitieke ontwikkelingen zorgen ervoor dat er met hernieuwde aandacht wordt gekeken naar de rol van nucleaire afschrikking. Dit is met name het geval voor wat betreft de betrekkingen tussen de VS, Rusland, China en India, maar als gevolg hiervan wordt nucleaire afschrikking mogelijk ook voor veel andere landen een punt van grotere aandacht.

Conclusies

Deze studie verkent het mogelijke nut voor de Nederlandse overheid van afschrikking als veiligheidsconcept met betrekking tot een aantal niet-traditionele veiligheidsdreigingen: terrorisme, criminaliteit, dreigingen via het cyber- en economische domein, en ambigue oorlogsvoering. Het uitgangspunt is daarbij dat afschrikking kan worden bereikt door de kosten/baten-afweging bij potentiële daders (of hun *facilitators*) zodanig te beïnvloeden dat het on- of minder aantrekkelijk wordt om tot schadelijk handelen over te gaan (of daar steun aan te geven).

27 DIME: Diplomatie, Informatie, Militair en Economie.

28 Over conventionele militaire afschrikking zie Jon Solomon, 'Conventional deterrence requires forward presence'. In: *Information dissemination*, 14 oktober 2014; 'Conventional deterrence in the second nuclear age'. In: *Carnegie endowment for international peace*, 17 november 2010; Maren Leed, 'The role of conventional forces in deterrence'. In: *Global Forecast 2015*, Center for Strategic & International Studies, 2014.

29 Adam Lowther, 'Framing Deterrence in the Twenty first century: Conference summary'. In: Anthony C. Cain (ed.), *Deterrence in the Twenty first century: proceedings*. Maxwell Air Force Base: Air University Press, 2010.

De ***hoofdconclusies*** van deze studie zijn ten eerste dat afschrikking als veiligheidsconcept relevant is voor alle vijf hier besproken dreigingsthema's, en ten tweede dat het per dreigingsthema en daarbinnen per actor verschilt op welke wijze afschrikking de beste mogelijkheden biedt om te kunnen worden ingezet. Een effectief afschrikkingsbeleid moet daarom zijn afgestemd op een specifiek dreigingsthema en waar mogelijk op specifieke groepen van actoren. Over de effectiviteit van concrete afschrikkingsinstrumenten bestaat vooralsnog weinig inzicht.

Dit rapport komt daarnaast ook tot de volgende ***aanvullende conclusies***.

- Het in dit rapport toegepaste analysekader levert de volgende inzichten op. De meest effectieve wijze om afschrikking te bewerkstelligen is door zowel aan de kosten- als aan de batenzijde in te grijpen:
  a. *Beïnvloeding van de kosten-inschatting* door daders is op directe wijze mogelijk door middel van de tegendreiging van vergelding. Deze methode lijkt het meest van toepassing als afschrikking tegen criminele acties (bijvoorbeeld via vervolging en straf) en economische dreigingen vanuit statelijke actoren (bijvoorbeeld via tegensancties). De effectiviteit van de vergeldingsdreiging neemt af naarmate het moeilijker is de daders te identificeren. Hierdoor is de toepasbaarheid van dit middel tegen cyberdreigingen en ambigue oorlogsvoering beperkt. Bovendien is het in beide gevallen lastig te bepalen welke mate van proportionaliteit moet worden gehanteerd bij vergeldingsmaatregelen. Ook in het geval van terreurdreigingen is de werking van deze methode beperkt, met name bij terroristen die de vergelding niet vrezen. Daarbij kan de inzet van vergeldingsmaatregelen zelfs contraproductief werken doordat het tot bredere steun kan leiden onder bevolkingsgroepen waaruit de terroristen afkomstig zijn. Ook in het geval van criminelen kan de dreiging van een beperkte vergelding tegen personen in hun omgeving relevant zijn om de steun vanuit deze sociale omgeving voor misdadigers te verzwakken. Indirecte beïnvloeding van de kosten-inschatting door daders kan worden bereikt door ze ervan te overtuigen dat benodigde voorinvesteringen hoog zijn. De belangrijkste manier om dit te bereiken is door de eigen verdedigingsmechanismen zichtbaar te verbeteren of door deze meer te benadrukken. Dit is van toepassing op alle vijf dreigingsthema's in deze studie.
  b. *Beïnvloeding van de baten-inschatting* kan op directe wijze door ervoor te zorgen dat de gelegenheid tot schadelijk handelen of de kans op succes daarvan kleiner wordt of in elk geval lijkt. Ook hier zijn zichtbare investeringen in verdedigingsmechanismen een belangrijk middel. Dit middel is relevant voor alle vijf dreigingsthema's. Bij ambigue oorlogsvoering kan het dan gaan om investeringen in bijvoorbeeld defensieve (collectieve) militaire of cybercapaciteiten maar ook om het zichtbaar versterken van het vermogen tot identificeren (ontmaskeren) van de dader. Capaciteiten die zichtbaar leiden tot vroegtijdige ontdekking van pogingen tot aanslagen kunnen terroristen afschrikken. Indirecte beïnvloeding van de baten-inschatting kan worden bereikt door de dader ervan te overtuigen dat schadelijk handelen niet bijdraagt aan het nagestreefde doel. Dit is waarschijnlijk niet toepasbaar als afschrikking tegen criminelen, maar wel tegen politiek gemotiveerde actoren (terroristen en staten). Een belangrijk middel hierbij is het zichtbaar vergroten van de weerbaarheid van de samenleving waardoor ontwrichting door terreurdaden of statelijke bedreigingen moeilijker bereikt kan worden.

- Voor alle hier besproken afschrikkingsmiddelen geldt dat internationale samenwerking het Nederlandse vermogen tot afschrikking aanzienlijk versterkt. In veel gevallen is effectieve afschrikking waarschijnlijk zelfs niet mogelijk zonder internationale samenwerking. In het geval van het instellen van diplomatieke en economische vergeldingsmaatregelen kan Nederland een stuk effectiever optreden als dit in internationaal verband gebeurt. Internationale samenwerking is ook van belang als het gaat om het verkrijgen van een goede informatiepositie, waarmee kan worden voldaan aan een belangrijke voorwaarde voor het uitvoeren van afschrikkingsbeleid: het identificeren (ontmaskeren) van een (potentiële) dader.

- Ook is het van belang op te merken dat afschrikking gericht op het vermijden dat *Nederlandse* belangen worden getroffen minder ver gaat, en dus mogelijk gemakkelijker te realiseren is, dan vormen van afschrikking die tot een verminderde dreiging leiden *tegen welk land dan ook*. De benadrukte noodzaak voor gezamenlijk optreden in internationaal verband als voorwaarde voor een effectief afschrikkingsbeleid impliceert echter dat afschrikking gericht op het strikt beschermen van de Nederlandse nationale veiligheid niet afdoende is.

- Naast *internationale samenwerking* is er nog een aantal andere voorwaarden voor effectieve afschrikking. Het gaat om de *geloofwaardigheid* van de genomen maatregelen, het overbrengen van de afschrikkingsboodschap aan de potentiële dader (*communicatie*), het kennen van de dreiging en de actoren waar deze uit voortkomt (*inlichtingen*), het beschikken over de *capaciteiten* waarop de afschrikking is gebaseerd en het toepassen van een *integrale benadering* (zowel op kosten- als batenzijde gericht, via meerdere beleidsdomeinen en typen van capaciteiten).

Bijlagen

Bijlage 1
Afschrikking als veiligheidsconcept tegen terrorisme

Bibi van Ginkel

Huidige situatie

De ontwikkelingen in de afgelopen periode - 2014/begin 2015 - liggen in lijn met de trends die in de recent uitgebrachte *Global Terrorism Index* 2014 werden geconstateerd. Daarin wordt over de periode 2012-2013 een sterke toename van het aantal dodelijke slachtoffers van terrorisme vastgesteld (+61%), waarbij ruim 80% van deze slachtoffers in vijf landen vielen: Irak, Afghanistan, Pakistan, Nigeria en Syrië. In totaal kwamen in 2013 17.958 mensen om als gevolg van ongeveer 10.000 terroristische aanslagen. Naast de vijf genoemde landen valt op dat de OESO-landen relatief weinig getroffen worden. Daar was in 2013 sprake van 113 slachtoffers bij ruim 300 incidenten.

De vijf meest getroffen landen staan tegelijkertijd model voor de afgelopen periode meest actieve terroristische organisaties en netwerken: Al Qaida (Irak/Syrië), de Taliban (Afghanistan), Boko Haram (Nigeria) en ISIS (Irak/Syrië). Hierbij moet worden opgemerkt dat naast de vijf genoemde landen ook elders sprake is van blijvende en deels toenemende terroristisch activiteiten. Dit geldt in het bijzonder voor Jemen, Somalië/Kenia, Libië, Mali en de CAR, waar aan de genoemde organisaties verwante bewegingen actief zijn en soms met elkaar rivaliseren.

Kenmerkend voor de huidige golf aan terrorisme is dat religieus extremisme als drijfveer de afgelopen jaren sterk aan kracht gewonnen heeft; dit in vergelijking met politiek terrorisme of nationaal separatistisch terrorisme. Er wordt daarbij onderscheid gemaakt tussen *dawa salafisme* en *jihadi salafisme*. Daarnaast zijn de '*hot spots*' van deze terroristische activiteiten vooral landen of regio's waar sprake is van etnische en religieuze tegenstellingen, sociaal-economische achterstelling van bepaalde groeperingen en van willekeurig staatsgeweld. Er is niet zondermeer sprake van een direct causaal verband, maar het onderstreept dat vooral regio's die gekenmerkt worden door instabiliteit, en door fragiele, autoritaire en falende staten, kwetsbaar zijn voor terrorisme dan wel een aantrekkelijke locatie vormen voor het ontplooien van terroristische activiteiten.

De afgelopen periode scherpt dit algemene beeld op een aantal punten aan. Ten eerste, de manifestatie van de Islamitische Staat als een op 'statelijke' basis georganiseerde terroristische beweging, die met geweld en aanslagen het Kalifaat probeert te vestigen in Syrië en Irak (maar verdergaande ambities o.a. tegen het Westen heeft). Deze ontwikkeling moet geplaatst worden in een breder palet, waarbij in het bijzonder, zoals benadrukt werd in de Clingendael Strategische Monitor 2014, de gehele MENA-regio een brandhaard van instabiliteit en daarmee een bron van terrorisme dreigt te worden.

Ten tweede, als gevolg van het geweld in Syrië en de opkomst van ISIS is er sprake van een sterke toename van het aantal *foreign fighters* vanuit de OESO-landen, West-Europese landen in het bijzonder, richting Syrië en Irak, om daar deel te nemen aan de strijd. Deze ontwikkeling is mede een gevolg van en gaat gepaard met een toenemende radicalisering van jonge Moslims in westerse landen ten opzichte van de afgelopen jaren. De uitreis richting Syrië en Irak betreft bovendien al lang niet meer enkel jonge mannen, maar betreft tevens (jonge) vrouwen en in enkele gevallen hele gezinnen. De AIVD spreekt van zwermdynamieken van jihadisme als het gaat over de wijze waarop jihadisten zich organiseren.

Ten derde, als gevolg hiervan is het risico dat de vertrokken jihadisten bij terugkeer een gevaar opleveren voor de Nederlandse en andere westerse samenleving, toegenomen. Dat dit niet enkel een theoretisch gevaar is, blijkt uit de recente aanslagen in Brussel op het Joods museum (mei 2014), en in Parijs op het satirisch blad Charlie Hebdo en op een Joodse supermarkt (begin januari 2015) een duidelijk voorbeeld. Tevens tonen deze aanslagen aan dat er ook een risico volgt uit jihadisten die nog niet eerder uitreisden, maar desondanks een aanslag uitvoeren in eigen land uit naam van jihadistische organisaties. De aanslagen passen ook binnen een ontwikkeling waarbij naast burgers, ook politieagenten en militairen doelwit van terroristen vormen.

Het voorgaande onderstreept, ten vierde, de sterke relatie tussen externe en interne veiligheid en de kwetsbaarheid van westerse, open samenlevingen. Die kwetsbaarheid is in de afgelopen periode in het geval van Nederland, maar dat geldt ook voor andere westerse landen, toegenomen als gevolg van de deelname aan de internationale coalitie in de strijd tegen ISIS. Daarnaast is in veel Europese landen sprake van een sterkere polarisatie inzake de islam en de integratie van migranten, wat radicalisering in de hand kan werken, en tevens een toename van het risico op '*lone wolf*' terrorisme laat zien.

Tot slot, het doel van terroristen is het veroorzaken van maatschappelijke en politieke ontwrichting en het creëren van angst. Bij de ingezette middelen werd al steeds vaker gebruik gemaakt van sociale media en internet, o.a. als middelen voor het ronselen van medestanders en als propaganda-instrument. Die tendens lijkt met het optreden van ISIS en het gebruik van video's bij het doden van gegijzelden, een nieuwe dimensie te hebben verkregen. Communicatie is nog meer het veld geworden waarop de strijd wordt gestreden.

Verwachting voor de komende 5 à 10 jaar

Sinds begin 2013 is het dreigingsniveau in Nederland verhoogd tot 'substantieel', maar de overheid erkent dat het binnen de bandbreedte van deze kwalificatie opschuift naar de bovengrens. De samenleving wordt zich meer en meer bewust van de risico's en kan bovendien waarnemen dat veiligheidsmaatregelen worden opgeschroefd. Militairen mogen vanwege de risico's momenteel niet in uniform met het openbaar vervoer reizen. De Koninklijke Marechaussee heeft extra capaciteit ingezet ter ondersteuning van de nationale veiligheid door hoog risico objecten te beveiligen en bewaken. De samenleving staat bovendien onder druk, en het gevaar van polarisatie in de samenleving als gevolg van aan de ene kant reactie en verzet uit islamitische hoek op de stevige taal die de overheid bezigt en de maatregelen die worden getroffen, en aan de andere kant een sterkere behoefte binnen anti-islamitische groeperingen om zich tegen de 'islamisering van Nederland' te keren, is zeker aanwezig. Signalen die voor de komende jaren op een blijvende en mogelijk toenemende terroristische dreiging voor Nederland en andere westerse samenlevingen wijzen betreffen primair de blijvende instabiliteit in de MENA-regio en het uitwaaieren van de

verspreiding van terroristische activiteiten binnen deze regio en naar andere gebieden; een beeld dat o.a. in de Clingendael Monitor 2014 en de update van 2015 wordt onderstreept. De MENA-regio is en blijft instabiel en daarmee een bron van terrorisme.

Het feit dat daarbij de terroristische dreiging, met name van *foreign fighters*, op dit moment grotendeels gerelateerd lijkt te zijn aan de strijd die gaande is in Irak en Syrië, neemt immers niet weg dat er duidelijke onderlinge relaties en verbanden bestaan tussen jihadistische (Al Qaida achtige) groeperingen in het Midden-Oosten, Noord-Afrika, Oost-Afrika, het Sahel-gebied en de Zuid-Aziatische regio. Het risico van verspreiding naar andere instabiele landen of regio's is onder deze omstandigheden groot, ook al omdat de kans bestaat dat uit alle windhoeken afkomstige jihad-strijders uitwaaieren naar andere brandhaarden. Het beeld wordt daarbij gecompliceerd doordat ook sprake is van onderlinge verdeeldheid tussen groeperingen (zie Syrië) en externe mogendheden van groeperingen als 'proxy' gebruik maken om hun onderlinge conflicten uit te vechten, met als gevolg een groter gevaar van onrust in en betrokkenheid van andere, aangrenzende landen.

Gegeven de belangen die voor Europa en het Westen op het spel staan, in het bijzonder op de nexus extern-interne veiligheid, zal er bovendien sprake zijn van een noodzaak tot blijvende betrokkenheid, in welk verband dan ook (ad hoc, EU, VN, etc.) van westerse landen, waaronder Nederland, bij deze regio en bij de brandhaarden aldaar. Dit in combinatie met binnenlandse radicalisering en polarisatie maakt Nederland ook voor de komende jaren een potentieel doelwit voor aanslagen, extern dan wel intern geïnitieerd en georganiseerd.

Wat betreft de aard van de terroristische dreiging zullen tendensen die al langer gaande zijn waarschijnlijk aan kracht winnen. Dit betreft o.a. de versmelting tussen terrorisme en criminele activiteiten als middel om het optreden te financieren, het gebruik van sociale media en internet o.a. als instrument tot ronselen, en het inspelen op gevoelens van frustratie en onvrede waarbij met name jonge moslims de doelgroep vormen, zowel in het Westen als in de regio. In het bijzonder van invloed is tevens het verschijnsel waarbij in essentie niet-statelijke terroristische beweging een meer statelijk karakter krijgen (ISIS, Boko Haram) en grote delen van het grondgebied van landen weten te beheersen. Niet uitgesloten is dat dit verschijnsel aan kracht zal winnen.

Angst zaaien blijft een belangrijk doel van terroristen, waarbij rekening moet worden gehouden met een toenemende inzet van communicatie als middel in de strijd. Naast angst zal ook het tegen elkaar opzetten van bevolkingsgroepen binnen westerse samenlevingen een belangrijk oogmerk zijn. In hoeverre deze bewegingen daarin zullen slagen, hangt sterk af van de weerbaarheid van westerse samenlevingen en het vermogen van politiek en overheid om een adequaat antwoord te vinden op een dergelijke ondermijning van de samenleving. Het voorgaande onderstreept het beeld dat ook uit de analyse in de Strategische Monitor 2014 naar voren komt. De terroristische dreiging is en blijft diffuus en daarmee onvoorspelbaar. De verschillen in grondoorzaken, drijfveren, communicatiemethoden, modus operandi en de verschillende niveaus waarop dit verschijnsel zich openbaart –nationaal, regionaal, internationaal- zullen het komen tot gericht beleid lastig maken, zeker als dit 'afschrikkingsmaatregelen' betreft.

Relevantie van afschrikking als veiligheidsconcept

In de literatuur wordt door de meeste auteurs 'afschrikking' als instrument om terrorisme tegen te gaan afgewezen als een effectief middel. Terroristen zouden niet vatbaar zijn voor

afschrikking.[1] Het instrument 'afschrikking' is vooral bekend uit de wijze waarop het tijdens de Koude Oorlog effectief werkte doordat de nucleaire machtsblokken elkaar wisten te weerhouden van een nucleaire aanval door zelf te dreigen met nucleaire tegenaanvallen. Het risico van catastrofale vernietiging werd zo groot geacht dat geen van de machtsblokken tot inzet van deze wapens overging. Waar het deze klassieke interpretatie van afschrikking betreft, is duidelijk dat dit niet op vergelijkbare wijze geldt voor de afwegingen die terroristen maken, en is zelfs het standpunt te verdedigen dat dit in zijn geheel niet effectief zal werken. Tegelijkertijd is het nuttig om de verschillende aspecten van 'afschrikking' en de wijze waarop dit middel ingezet kan worden nader te analyseren, en af te zetten tegen de doelstellingen en werkwijze van terroristen en terroristische organisaties. Van belang is primair om onderscheid te maken tussen aan de ene kant 'afschrikking' als middel om terrorisme te voorkomen, en aan de ander kant om de kans op het slagen van een terroristische aanslag of de impact ervan te verminderen. Met name met betrekking tot deze laatste categorie kan geconcludeerd worden dat 'afschrikking' in bepaalde toegepaste vormen effect kan bewerkstelligen. Als men het risico van een terroristisch aanslag calculeert als de kans dat het gebeurt maal het effect dat het kan berokkenen, dan biedt het verkleinen van deze elementen aanknopingspunten voor 'afschrikking' als instrument tegen terrorisme.

Terroristen – of ze nu alleen of namens een organisatie opereren – zijn uit op maximaal effect van hun aanslag. Dat effect uit zich in de fysieke schade (slachtoffers, destructie van gebouwen, infrastructuur), economische schade, en het creëren van angst en sociale onrust in een maatschappij. De kans beperken dat dit zich voordoet, dan wel het effect van een aanslag beperken, zijn belangrijke doelstellingen van counter terrorisme beleid.

Terroristen plegen aanslagen om aandacht te genereren voor de politieke boodschap die ze voorstaan, en verantwoorden deze aanslagen als noodzakelijk om dit politieke doel te bereiken. De ideologische motivatie kan gebaseerd zijn op extremistisch religieus gedachtengoed, maar ook op een extreem linkse of rechtse politieke ideologie, of kan separatistisch van aard zijn. Een belangrijk kenmerk is dat terroristen in tegenstelling tot de meeste statelijke actoren in hun strijdplan niet op dezelfde rationele wijze als staten een afweging maken of de gemaakte offers het waard zijn in relatie tot de te verwachten resultaten. Zo geldt voor extremistisch jihadistische strijders dat zij een grotere bereidheid hebben om te sterven omdat binnen hun geloofsovertuiging hen na hun dood het paradijs wacht. Tegelijkertijd geldt dat soms een dreiging van een aanslag op zich of relatief kleine aanslag al genoeg is om een samenleving te ontwrichten, en dat dus met weinig middelen al een optimaal resultaat kan worden behaald. Op basis van deze kenmerken stellen vele auteurs dat 'afschrikking' als middel niet effectief is. Het kan zelfs een tegengesteld effect creëren, als de inzet van middelen ter afschrikking gericht is op de '*support*' omgeving van terroristische organisaties, met als resultaat dat in een dergelijke omgeving mensen zich verenigen en zich tegen een gezamenlijke vijand keren, met meer radicalisering als gevolg. Dit probleem doet zich onder meer voor als gevolg van de aanvallen met gewapende drones in Pakistan en Jemen.

1 "*After September 11, many observers dismissed the applicability of traditional concepts of deterrence to non-state actors. They pointed to the difficulties of finding effective threats both against individual terrorists who may care more about heavenly than earthly rewards and are willing to commit suicide for their cause, and against terrorist organizations that lack 'a return address' against which to retaliate.*" In: Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research'. In: Contemporary Security Policy. 31(2010)1.

Alvorens in te gaan op de verschillende afschrikkingsmiddelen en hun effectiviteit bij het tegengaan van terrorisme, is het van belang onderscheid te maken tussen de verschillende actoren en hun rol binnen een terroristische organisatie, en hun tactieken en werkwijzen. Grote wereldwijde terroristische netwerken hebben over het algemeen een geavanceerde organisatiegraad. Binnen die organisatie spelen verschillende actoren een rol. Deze spelers hebben allemaal andere drijfveren en overtuigingen ten aanzien van hun sneuvelbereidheid. Dat kan gaan om het hogere kader, waar de strategie wordt uitgedacht, en van waaruit een infrastructuur wordt uitgerold, maar het kan ook het middenkader betreffen, de voetsoldaten, en het ondersteunend netwerk. Bovendien is de ene terroristische organisatie *nietsontziender* dan de ander organisatie. De bereidheid om – in de ogen van gewone burgers of staten – onevenredige offers te brengen zal derhalve verschillend zijn voor iedere organisatie, maar tevens voor de verschillende categorieën actoren binnen zo'n netwerk. Dit onderscheid is van belang voor de potentiële effectiviteit van de inzet van de verschillende beschikbare 'afschrikkingsinstrumenten'.

Deze instrumenten kunnen zich richten op het netwerk dat in de breedte door de doelstellingen en de werkwijzen van de organisatie te steunen support verleent aan een terroristische organisatie. Uit deze groep van volgelingen worden ook strijders gerekruteerd. De 'afschrikkingsinstrumenten' kunnen zich ook richten op de 'facilitaire dienstverleners', de infrastructuur en de aanvoerroutes voor wapens en explosieven, en voor technische en financiële ondersteuning. De 'afschrikkingsinstrumenten' die effectief kunnen zijn ten aanzien van deze groep zullen afwijken van de instrumenten die effect kunnen sorteren bij de eerste groep. En de noodzaak van op maat gesneden afschrikking geldt ook ten aanzien van de uitvoerders en het hogere kader.

Ook de gebruikte tactieken en werkwijzen van terroristische organisatie en de gekozen doelwitten, dwingen ertoe om 'afschrikkingsmiddelen' gericht in te zetten wil het middel effectief kunnen zijn. Qua werkwijzen en soorten aanslagen kunnen we onderscheid maken tussen: zelfmoordaanslagen, inzet van *improvised explosive devices* (eventueel ingebracht in voertuigen waarmee op gebouwen of menigtes wordt ingereden), shootings, kapingen, ontvoeringen, onthoofdingen, bomaanslagen, etc. Vaak gaan deze methodes gepaard met maatschappelijke ontwrichting, dreiging en angst onder de bevolking. Hier wordt door de terroristische organisaties of de individuele terrorist op ingespeeld door mediacampagnes in te zetten en allerhande communicatiestrategieën toe te passen om dit effect mogelijk te versterken. Sommige tactieken worden bij uitstek ingezet om politieke eisen te stellen of afkoopsommen te regelen. Naast de vraag wat voor afschrikkingsmiddelen men tegen wie inzet, is tevens een belangrijke vraag wanneer deze ingezet worden, om het meest effectief zijn. Het mag duidelijk zijn dat als iemand al aan boord van een vliegtuig zit met een explosief, met de intentie het vliegtuig op te blazen, afschrikkingsmiddelen geen effect meer berokkenen.

Wanneer 'afschrikking' als middel wordt ingezet tegen terrorisme, hoeft dat niet per se militair of repressief van aard te zijn. Glenn Snyder maakt onderscheid tussen afschrikking aan de batenkant (*deterrence by denial*) en afschrikking aan de kostenkant (*deterrence by punishment*). Bij de laatste categorie gaat het er om de 'kosten' van een aanslag zodanig te verhogen dat het niet opweegt tegen de baten. Deze indeling correspondeert deels met de afbakening van begrippen zoals in het algemene hoofdstuk van deze studie wordt gehanteerd. Waar het afschrikking aan de kostenkant betreft die zicht richt op een vorm van vergelding of bijvoorbeeld strafvervolging kan conform de in deze studie gehanteerde categorisering ook gesproken worden van directe vorm van afschrikking aan de kostenkant.

Dit is een strategie die met name door Israël wordt gepropageerd, maar weinig steun vindt in de literatuur of bij beleidsmakers in andere landen. Probleem is dat dit middel wordt ingezet als vergelding tegen de families of de gemeenschappen waar de terroristen uit voortkomen, en uitgaat van een noodzaak om de inzet van de tegenmaatregelen excessief en disproportioneel te laten lijken om de *hard core* terroristen te overtuigen dat de kosten/baten analyse verkeerd uitpakt.

Bij afschrikking aan de batenkant gaat het om maatregelen die er op gericht zijn potentiele daders te ontmoedigen door de succeskans – d.w.z. de baten - te verkleinen of door hen te overtuigen van andere manieren om hun politieke doelen te bereiken. Volgens Davis en Jenkins zouden zelfs de meest geharde terroristen operationele risico's willen vermijden, en zou het vergroten van onzekerheid omtrent het slagen van een aanslag en het verhogen van de risico's op voortijdige opsporing een afschrikwekkende werking hebben. Tot deze categorie van afschrikking kan ook de nieuwste methode zoals door Knopf geïntroduceerd, worden gerekend die zich richt op het ontkrachten van de door extremistische organisaties gebruikte rechtvaardiging voor het gebruik van geweld door middel van counterpropaganda.

James Smith en Brent Talbot maken onderscheid tussen de verschillende niveaus waarop afschrikking aan de batenkant kan worden ingezet. Ze maken daarbij onderscheid tussen het tactische, het operationele en het strategische niveau. Bij het tactische niveau is de afschrikking vooral gericht op het verkleinen van de gelegenheid om een aanslag te plegen door het verhogen van veiligheidsmaatregelen en het vergroten van de operationele risico's die terroristen lopen in de aanloop naar een aanslag. Volgens de categorisering die in deze studie wordt gehanteerd, zouden dergelijke maatregelen ook wel geduid kunnen worden als indirecte afschrikking aan de kostenkant waarbij het gaat om het verhogen van de kosten van de benodigde voorinvestering. Ook de maatregelen die zich richten op het afsnijden van logistieke ondersteuning en financiële geldstromen vallen in die categorie. Smith en Talbot plaatsen deze maatregelen eerder in de categorie van maatregelen die zich op het operationele niveau richten, daar het gaat om het verkleinen van capaciteiten. Dit kan hand in hand gaan met afschrikkingsmaatregelen aan de kostenkant, zoals bijvoorbeeld strafvervolging. Knopf spreekt in dit verband ook wel van afschrikking op indirecte wijze als de maatregelen zich richten op de *support* groep. Tenslotte is op het strategisch niveau de afschrikking gericht op het verkleinen van het beoogde doel. Dutter en Seliktar menen dat dit het belangrijkste niveau is voor de inzet van afschrikkingsmiddelen. Hierbij gaat het onder andere om het overtuigen dat met de terroristische methodes nooit de politieke doelen zullen worden bereikt, maar ook om het vermijden van overreactie bij overheden, het vergroten van de maatschappelijke weerbaarheid om paniek te voorkomen onder meer door angst management en het vergroten van de acceptatie dat onveiligheid nu eenmaal bestaat. Er is sprake van een succesvolle inzet als de steun vanuit de gemeenschap voor terroristen wegvalt.

In sommige gevallen is er sprake van een overlap van de verschillende afschrikkings-methodes. Zo is een beleid dat duidelijk stelt dat geen losgeld betaald wordt om gijzelaars vrij te kopen en dat ook in praktijk wordt gebracht een combinatie van het verkleinen van het beoogde doel en het verhogen van de kosten van de benodigde voorinvestering.

Gezien de grote nadruk die momenteel gelegd wordt op de aanpak van jihadisme en de problematiek van de *foreign fighters*, is het belangrijk om afschrikkingsmaatregelen te beoordelen op de mate waarin de verwachting bestaat dat de genomen of beoogde maatregel vanuit het oogpunt van afschrikking op effectieve wijze zal bijdragen aan een

heroverweging door een terrorist van een geplande aanslag of wel het verminderen van het risico dat deze aanslag plaatsvindt of van de impact die een aanslag heeft op een samenleving.

Literatuur

Nationaal Coördinator Terrorismebestrijding en Veiligheid, Samenvatting Dreigingsbeeld Terrorisme Nederland 36. 30 juni 2014.

Nationaal Coördinator Terrorismebestrijding en Veiligheid, Samenvatting Dreigingsbeeld Terrorisme Nederland 37. 12 november 2014.

Actieprogramma Integrale Aanpak Jihadisme; Overzicht maatregelen en acties. TK 29754, nr. 253. 29 augustus 2014.

Algemene Inlichtingen en Veiligheidsdienst, Transformatie van het jihadisme in Nederland: zwermdynamiek en nieuwe slagkracht. Juni 2014.

Benjamin Darnell, *Deterrence in Counter Terrorism*. 19 mei 2010. Beschikbaar op: http://www.e-ir.info/2010/05/19/deterrence-in-counter-terrorism/.

Matthew Kroenig and Barry Pavel, 'How to Deter Terrorism'. In: *The Washington Quarterly*, 35(2012)2.

Jeffrey W. Knopf, 'The Fourth Wave in Deterrence Research'. In: *Contemporary Security Policy*. 31(2010)1.

Glenn Snyder, 'Deterrence by Denial and Punishment'. In: *Research Monograph*. Princeton University Center of International Studies. (1959)1.

Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*. Princeton, NJ: Princeton University Press, 1961.

Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda*. Santa Monica, CA: RAND, 2002.

James Smith and Brent Talbot, 'Terrorism and Deterrence by Denial'. In: Paul R. Viotti, Michael A. Opheim en Nicholas Bowen (eds). *Terrorism and Homeland Security: Thinking Strategically about Policy*. Boca Raton, FL: CRC Press, 2008.

Lee E. Dutter and Ofira Seliktar, 'To Martyr or Not to Martyr: Jihad Is the Question, What Policy Is the Answer?'. In: *Studies in Conflict & Terrorism*. 30(2007)5.

Gerald M. Steinberg, 'Rediscovering Deterrence after September 11, 2001'. In: *Jerusalem Letter/ Viewpoints* 467. Jerusalem Center for Public Affairs, 2 december 2001. Beschikbaar op: www.jcpa.org/jl/vp467.htm.

International Centre for the Study of Radicalism, ICSR Data. ICSR Insight: Up to 11,000 Foreign Fighters in Syria; Steep Rise Among Western Europeans. Beschikbaar op: http://icsr.info/2013/12/icsr-insight-11000-foreign- fighters-syria-steep-rise-among-western-europeans/ ; Govt. Agency Data. Foreign Fighters in Syria, The Soufan Group. Beschikbaar op: http://soufangroup.com/wp-content/uploads/2014/06/TSG-Foreign-Fighters-in-Syria.pdf.

Institute for Economics and Peace. Global Terrorism Index 2014. Beschikbaar op: http://www.visionofhumanity.org/sites/default/files/Global%20Terrorism%20Index%20Report%202014_0.pdf.

Bijlage 2
Afschrikking als veiligheidsconcept tegen dreigingen via het cyberdomein

Sico van der Meer

Huidige situatie

Cyberdreigingen, ook wel digitale dreigingen genoemd, vormen één van de grootste dreigingen waar Nederland op het moment mee wordt geconfronteerd.[1] Cyberdreigingen beslaan een breed spectrum; gedacht kan worden aan bijvoorbeeld digitale oorlogsvoering, digitaal terrorisme, digitale spionage, digitaal activisme en digitale criminaliteit. Waar het doel van deze activiteiten verschilt, is de gebruikte techniek hetzelfde: gebruikmaken van zwakke plekken binnen het cyberdomein.

Dat het aantal cyberaanvallen sterk toeneemt is duidelijk. Het is echter zeer lastig om een juiste inschatting te maken van het aantal gevallen. De meeste gevallen worden nooit gemeld of zijn niet eens bekend bij de aangevallen personen of organisaties; vaak gaat het immers om het inbreken op computers of computernetwerken waarbij het bij uitstek de bedoeling is dat niemand dat doorheeft. Inbreuken op cyberveiligheid hebben zoveel verschijningsvormen en typen daders, dat het moeilijk is om ze op één hoop te vegen. Het varieert letterlijk van een studentikoze hacker die voor de lol rondsnuffelt op andermans computers, via grootschalige industriële spionage, tot aan werkelijke digitale oorlogsvoering met als doel het ontwrichten van de gehele samenleving. Binnen de beperkingen van deze publicatie wordt niettemin een voorzichtige poging ondernomen om een algemeen beeld te schetsen.

De grootste cyberdreiging voor Nederland gaat momenteel uit van cyberspionage en cybercriminaliteit, aldus het meest recente Cybersecuritybeeld Nederland (CSBN) van het Nationaal Cyber Security Centrum (NCSC).[2] Dit is vooral het geval omdat deze twee vormen van cyberaanvallen veruit het meeste voorkomen in Nederland. Tegelijk constateert het NCSC dat de voortdurend toenemende digitalisering van de Nederlandse maatschappij tevens de risico's van grootschaligere cyberaanvallen, gericht op maatschappelijke ontwrichting, doet toenemen. Hoe meer persoonlijke en maatschappelijke veiligheid afhankelijk worden van digitalisering, hoe groter de gevolgen als kwaadwillenden die digitalisering misbruiken voor eigen doeleinden. Cyberspionage en cybercriminaliteit zijn met name een grote economische schadepost. Vooral cyberspionage heeft naast economische gevolgen (zoals aantasting van de Nederlandse concurrentiepositie) ook een belangrijk veiligheidsaspect: potentiële vijanden van Nederland (statelijke dan wel niet-statelijke actoren) kunnen via cyberspionage veel te weten komen over de Nederlandse nationale veiligheid en mogelijke zwakke plekken daarin. Gestolen gegevens over bijvoorbeeld vitale infrastructuur of militaire operaties zouden misbruikt kunnen worden om via digitale dan wel niet-digitale wegen kwaad uit te richten.

1 AIVD, Jaarverslag 2013. Den Haag: AIVD, april 2014.
2 Nationaal Cyber Security Centrum (NCSC), Cybersecuritybeeld Nederland: CSBN-4. Juli 2014, p. 7.

Waar cyberaanvallen op organisaties, bedrijven en personen wereldwijd inmiddels vrij normaal zijn, blijven cyberaanvallen met als doel grootschalige maatschappelijke verstoring te veroorzaken tot nu toe beperkt. De meest bekende voorbeelden zijn cyberaanvallen in Estland in 2007 (cyberaanval op overheid, banken en media), de Verenigde Staten in 2012 (cyberaanval op diverse banken) en Zuid-Korea in 2012 (cyberaanval op banken en media). Er zijn ook voorbeelden van grootschalige cyberaanvallen die niet in eerste instantie maatschappelijke ontwrichting ten doel hadden: Georgië in 2008 (ter ondersteuning van conventionele militaire operatie door Rusland), Iran in 2010 (gericht op sabotage nucleair programma), Saoedi-Arabië in 2012 (cyberaanval op staatsoliemaatschappij Saudi Aramco, mogelijk om olie-export te saboteren), en de Verenigde Staten in 2014 (cyberaanval op film-producent Sony, wellicht om het uitbrengen van een film over de Noord-Koreaanse leider Kim Jong-Il tegen te houden). Hoewel de economische schade in een aantal van deze gevallen aanzienlijk was, zijn grootschalige cyberaanvallen op werkelijk vitale infrastructuur van een land, bijvoorbeeld energie- en drinkwatervoorzieningen of (in Nederland van belang) waterbouwkundige werken, nog niet bekend.

Weliswaar is de alertheid op cyberdreigingen de afgelopen jaren aanzienlijk toegenomen in Nederland, tegelijkertijd verlopen de technologische ontwikkelingen in het cyberdomein zo razendsnel dat cyberbeveiligingsmaatregelen voortdurend gemoderniseerd moeten worden om de strijd tegen kwaadwillenden niet te verliezen. Het zijn momenteel vooral cyberexperts van gespecialiseerde bedrijven en overheidsdiensten (bijvoorbeeld het Nationaal Cyber Security Centrum en het Defensie Cyber Commando) die actief zijn in de voortdurende strijd tegen cyberdreigingen. De gebruikers van cybertechnologie, zowel organisaties als particulieren, blijven ondanks het toegenomen bewustzijn van risico's een zwakke schakel bij het tegengaan van cyberdreigingen. Om slechts één voorbeeld te noemen: het Cybersecuritybeeld Nederland memoreert dat ongeveer 35 procent van alle gebruikers geen antivirussoftware heeft geïnstalleerd op zijn of haar computer, terwijl dat toch de meest basale eerste stap richting cyberveiligheid is.[3]

Verwachtingen voor de komende 5 à 10 jaar

Hoewel het beeld van het aantal cyberincidenten momenteel diffuus is, valt met zekerheid vast te stellen dat de cyberdreiging voor Nederland in de nabije toekomst alleen maar verder zal toenemen. Dit komt voornamelijk doordat de digitalisering van de Nederlandse maatschappij verder zal doorgroeien, ook in vitale sectoren. Het aantal apparaten (inclusief medische apparatuur, huishoudelijke apparaten, voertuigen etc.) dat met elkaar en met het internet verbonden is, zal wereldwijd exponentieel toenemen tot zo'n 25 miljard in 2020.[4] Hoe groter deze afhankelijkheid, hoe kwetsbaarder de maatschappij is voor cyber-dreigingen. Doordat steeds meer processen digitaal verlopen en steeds meer apparaten met cybernetwerken zijn verbonden, neemt het risico dat processen en apparaten door onbevoegden worden gemanipuleerd navenant toe.[5]

Terwijl aan de kant van de beveiliging van het cyberdomein veel vorderingen worden gemaakt, variërend van vergroting van het bewustzijn van de dreiging tot en met het

3 Nationaal Cyber Security Centrum (NCSC), Cybersecuritybeeld Nederland: CSBN-4. Juli 2014, p. 43.
4 Idem, p. 77.
5 Idem ; Jan Rood, Een wankele wereldorde; Clingendael Strategische Monitor 2014. Den Haag: Instituut Clingendael, 2014, p. 110-119 en 126-128.

technologische beveiligingsniveau van (vitale) cyberinfrastructuur, staan ook andere partijen niet stil. In veel landen (waaronder Nederland zelf) wordt geïnvesteerd in offensieve cyberoorlog-capaciteiten, en ook niet-statelijke actoren investeren daar voortdurend in – er wordt in dit verband regelmatig gesproken over een internationale cyberwapenwedloop.[6] Doordat cyberaanvallers zodra een gat in de veiligheid is gedicht meteen zoeken naar nieuwe zwakheden, zijn zij vrijwel altijd in het voordeel. Het is namelijk onmogelijk om alle zwakke plekken van cyberinfrastructuur te dichten, dus cyberveiligheid zal altijd een wedstrijd blijven tussen aanvallers die een nieuwe zwakte exploiteren en verdedigers die dat gat zo snel mogelijk proberen te dichten.

De belangrijkste toekomstige dreigingen zullen blijven voortkomen uit cybercriminaliteit en cyberspionage en deze blijven daarmee een gevaar voor de nationale veiligheid. Cybercriminelen worden steeds professioneler, de cyberaanvallen steeds complexer en omvangrijker. Ook cyberspionage zal toenemen, zowel door staten als door private organisaties (bedrijfsspionage). Het is niet ondenkbaar dat in de toekomst ook bondgenoten spionageactiviteiten zullen ondernemen via het cyberdomein. Ook het risico dat cyberterroristen hun slag slaan blijft een mogelijk nachtmerriescenario. Cyberterroristen die bijvoorbeeld energievoorzieningen, waterbouwkundige werken, ziekenhuizen, chemische fabrieken, lucht- of spoorverkeersleiding, of betalingssystemen saboteren, kunnen veel schade veroorzaken, wat ook tot maatschappelijke onrust kan leiden. Wat dat betreft geldt voor cyberterrorisme hetzelfde als voor terrorisme in het algemeen: de kans dat een aanslag plaatsvindt is statistisch relatief gering, maar als zo'n aanslag zich voordoet zal de impact aanzienlijk zijn.

Werkelijke cyberoorlogsvoering gericht tegen Nederland ligt niet direct voor de hand, hoewel een diplomatiek conflict tussen Nederland en een willekeurige andere staat wellicht ook zou kunnen leiden tot verstoring van bepaalde cyberdiensten – zie de bovengenoemde buitenlandse voorbeelden.

Niet onbelangrijk is dat ook cyberincidenten in het buitenland gevolgen voor Nederland kunnen hebben. Om slechts enkele voorbeelden te schetsen: als het Amerikaanse GPS-systeem verstoord wordt, zal dit ook in het Nederlandse verkeer ontregelende gevolgen (kunnen) hebben. Indien een cyberterrorist erin zou slagen een nucleaire ramp bij een kerncentrale elders in Europa te veroorzaken, kan Nederland ook te maken krijgen met radioactieve *fall-out*. Ook een cyberaanval op de Europese Centrale Bank kan het Nederlandse betalingsverkeer schade berokkenen. Wat dat betreft maakt de toenemende digitalisering ook de verwevenheid tussen Nederland en het buitenland alleen nog maar groter.

Relevantie van afschrikking als veiligheidsconcept

Over de verdediging- en afschrikkingsmogelijkheden wordt nog volop gediscussieerd door onderzoekers en beleidsmakers. Hoewel het zeer de vraag is of inbreuken op cyberveiligheid volledig te voorkomen zijn, kan afschrikking mogelijk een deel van de cyberaanvallen voorkomen.

6 Zie bijvoorbeeld: Michael Riley en Ashlee Vance, 'Cyber weapons: the new arms race'. In: *Businessweek*, 20 juli 2011.

Wat betreft de kostenzijde van de afweging van potentiële daders en aanvallers, valt te denken aan vergeldingsmaatregelen binnen het cyberdomein zelf (cyberaanval door getroffene op de aanvaller), diplomatieke en/of economische sancties, of zelfs conventionele militaire actie tegen de aanvaller. De NAVO, waarvan Nederland lid is, heeft in 2014 bijvoorbeeld besloten dat een cyberaanval op een van de lidstaten onder artikel 5 van het NAVO Handvest valt, waarmee de weg is vrijgemaakt voor een militaire operatie van het bondgenootschap tegen cyberaanvallers.[7] Tot op bepaalde hoogte zal de drempel voor cyberaanvallers door dergelijke afschrikking ongetwijfeld een tikje hoger zijn dan zonder enige vorm van afschrikking het geval zou zijn geweest. Door verschillende specifieke eigenschappen van het cyberdomein is afschrikking tegen cyberaanvallers echter relatief moeilijk toepasbaar.

Het belangrijkste obstakel om dergelijke afschrikkingsmaatregelen effectief te laten zijn binnen het cyberdomein is het attributieprobleem. Het is bijzonder lastig om onomstotelijk vast te stellen welke dader(-s) verantwoordelijk zijn voor een (onopgeëiste) cyberaanval. In tegenstelling tot conventionele wapens zijn cyberwapens en hun oorsprong niet duidelijk zichtbaar en traceerbaar. Aanvallers kunnen bijvoorbeeld gebruikmaken van een keten van gehackte of geïnfecteerde computers waarvan de eigenaren zich van geen kwaad bewust zijn. Hoewel het technisch mogelijk is om via IP-adressen de bron van een cyberaanval te achterhalen, is altijd het risico aanwezig dat deze geïdentificeerde bron ook slechts een schakel in de aanval is geweest en de eigenaar er niet bewust mee te maken heeft gehad. Daarnaast kunnen statelijke actoren hun betrokkenheid verbergen door de cyberaanval door zogenaamde niet-statelijke actoren (bijvoorbeeld hackersgroepen) te laten uitvoeren, en andersom: niet-statelijke aanvallers kunnen zich verbonden verklaren met staten, terwijl dit niet zo is. Bovendien kunnen cyberaanvallers binnen zeer korte tijd hun slag slaan en direct daarna de eigen sporen wissen, terwijl het onderzoek naar de bronnen van de aanval ingewikkeld en tijdrovend is – vergelding tijdens of direct na de aanval is daarmee al vrijwel uitgesloten. Omdat het vrijwel onmogelijk is om met honderd procent zekerheid vast te stellen wie verantwoordelijk is voor een cyberaanval, zeker als de beschuldigde partij ontkent, bestaat het risico dat een vergeldingsactie tegen een onschuldige partij wordt ingezet. In de praktijk zullen weinig statelijke actoren dit risico willen nemen, en dat beseffen de cyberaanvallers op hun beurt.[8] Er valt wellicht te argumenteren dat in sommige gevallen geen onbetwistbaar sluitend bewijs nodig is, maar dat men ook zou kunnen vergelden indien een (statelijke) partij ofwel vrijwel zeker direct betrokken is, ofwel de aanvallers geen strobreed in de weg heeft gelegd.[9] Los van de wenselijkheid hiervan, inclusief het risico van onterechte beschuldigingen, is het de vraag of het internationale recht dit toestaat – ook wat dat betreft is het cyberdomein nog volop in ontwikkeling.[10]

Om ervoor te zorgen dat de schuldige van een cyberaanval wel aangewezen kan worden, is het voorhanden hebben van sterke forensische capaciteit op cyberterrein uiterst belangrijk. Zodra er een grotere kans bestaat dat een dader ontmaskerd kan worden, zal dit ook een

7 David E. Sanger, 'NATO set to ratify pledge on joint defense in case of major cyberattack'. In: *The New York Times*, 31 augustus 2014.

8 Emilio Iasiello, 'Is cyber deterrence an illusory course of action?'. In: *Journal of Strategic Security*. 7(2013)1, p. 58; Adviesraad Internationale Vraagstukken, Digitale Oorlogvoering. 77(2011), p. 13.

9 Jason Healy, 'Beyond attribution: seeking national responsibility for cyber attacks'. In: *Atlantic Council Issue Brief* (2012).

10 Voor een discussie over internationaal recht en cyberaanvallen, zie: Adviesraad Internationale Vraagstukken, Digitale oorlogvoering, p. 19-27.

afschrikwekkend effect hebben op potentiële daders. Hierbij is internationale samenwerking, zoals informatie-uitwisseling over geconstateerde cyberwapens en cyberkwetsbaarheden, eveneens essentieel.

Naast de moeilijkheid om de schuldige van een cyberaanval overtuigend aan te wijzen, zijn er ook andere problemen verbonden aan afschrikking van dergelijke aanvallen. Een belangrijk vraagstuk vormt de geloofwaardigheid van afschrikking in combinatie met escalatiegevaar. Afschrikking via vergelding werkt alleen als de afschrikkende partij duidelijk communiceert wat eventuele vergeldingsmaatregelen bij een cyberaanval zullen zijn. Wanneer wordt iets beschouwd als een te vergelden cyberaanval? Wordt via digitale weg teruggeslagen, of kan een aanvaller conventionele militaire vergelding verwachten? Worden de vergeldingsmaatregelen niet duidelijk gecommuniceerd, dan zal een potentiële aanvaller hier wellicht geen rekening mee houden en zich niet laten weerhouden van de cyberaanval. Afschrikking werkt immers alleen als de tegenstander weet waarvoor hij moet terugschrikken. De moeilijkheid is dat het trekken van 'rode lijnen' in het cyberdomein ook averechts kan werken. Cyberaanvallers kunnen bewust net een stapje over de rode lijn heengaan om escalatie te veroorzaken, wellicht zelfs terwijl ze zich onder de dekmantel van het attributieprobleem voordoen als een andere partij dan ze in werkelijkheid zijn. Als de afschrikkende partij de afschrikking geloofwaardig wil houden, is deze wel gedwongen om te vergelden, hoe onwenselijk dat op dat moment ook is. Houdt men zich niet aan de gecommuniceerde afschrikkingsmechanismen, dan verwatert die afschrikking ook meteen. Blijkbaar vallen de getrokken rode lijnen in de praktijk wel mee, zullen potentiële tegenstanders denken.[11]

Een derde probleem met afschrikking via vergelding in het cyberdomein vormt de proportionaliteit van de maatregelen. Wanneer de vergeldingsactie met conventionele middelen verloopt is dit meestal wel redelijk in te schatten, maar wanneer een cyberaanval eveneens via het cyberdomein wordt beantwoord, is er minder greep op de gevolgen. Een cyber(vergeldings)aanval kan immers eenvoudig onbedoelde consequenties hebben, juist omdat in het cyberdomein alles met elkaar verbonden is. Een cyberaanval op, bijvoorbeeld, overheidsnetwerken, kan per ongeluk ook effect hebben op netwerken van, eveneens bijvoorbeeld, ziekenhuizen, drinkwaterinstallaties, en dergelijke. Het risico bestaat dat een vergeldingsaanval via het cyberdomein grotere effecten heeft dan bedoeld, waardoor de vergeldende partij zelf in het internationale beklaagdenbankje belandt.[12] Tevens blijft het een probleem wanneer en in welke mate vergeldingsmaatregelen kunnen worden ingezet; waar liggen in het cyberdomein de grenzen tussen het aanrichten van economische schade, verstoring, ontwrichting, en evidente oorlogshandelingen? Over dergelijke vraagstukken bestaat nog volstrekt geen duidelijkheid.

Tot slot, maar zeker niet onbelangrijk, is afschrikking in het cyberdomein lastig door de diversiteit aan actoren. Statelijke aanvallers hebben meestal belangen genoeg die bij een vergeldingsactie in het geding kunnen komen. Maar niet-statelijke groeperingen, bijvoorbeeld een hackers- of terreurgroep, hebben soms geen belangen of goederen van waarde waar een vergeldingsaanval zich op zou kunnen richten, hetgeen meteen de geloofwaardigheid van de vergelding teniet doet. Bovendien is het de vraag of dergelijke niet-statelijke groeperingen,

11 Martin C. Libicki, Cyberdeterrence and cyberwar (RAND Research Report). RAND Corporation, 2009, p. 65-73.
12 Emilio Iasellio, 'Is cyber deterrence an illusory course of action?', p. 59-60.

die ondanks beperkte middelen krachtige cyberaanvallen kunnen uitvoeren, zich altijd rationeel gedragen en zich überhaupt laten afschrikken.[13]

Er zijn ook andere – meer passieve – manieren om de kosten te verhogen voor potentiële daders, in het bijzonder door het versterken van beveiligingsmaatregelen; te denken valt aan veelgelaagde *firewalls* en geavanceerde encryptie- en authenticatiemiddelen. Om de beveiliging te versterken kan ook gebruik worden gemaakt van zogenaamde '*honeypots'.* Dit lijken kwetsbare plekken in een systeem, waarnaar cyberaanvallers op zoek zijn. In feite zijn deze bewust opgezet om informatie te verzamelen over de werkwijze van cyberaanvallers. In praktijk blijkt dat cybercriminelen wegens deze gebruikte methode Nederland en Nederlandse servers mijden. Dit middel brengt daarmee een afschrikwekkend effect met zich mee.[14]

Het verbeteren van de beveiliging verhoogt zowel de kosten die een aanvaller moet maken voor een succesvolle aanval, alsook het risico dat ondanks die kosten de aanval niet het gewenste effect sorteert en dus niet de gewenste baten tot gevolg heeft. Om een dergelijke vorm van afschrikking te bereiken, dient de cyberinfrastructuur van het potentiële slachtoffer zodanig beveiligd te zijn dat eventuele aanvallers tegen barrières zullen aanlopen die de kans op succes van hun aanval aanzienlijk verminderen. Als overheden, organisaties en particulieren zich bewust zijn van de gevaren van cyberaanvallen en voortdurend de modernste beveiligingsmethoden geïnstalleerd hebben op hun computer(netwerken), is al een grote stap richting passieve afschrikking gezet. Daarbij dienen netwerken ook voortdurend gemonitord te worden, zodat bij tekenen van een aanval direct tegenmaatregelen kunnen worden genomen.

Het verhogen van beveiliging, ofwel passieve afschrikking, is met minder potentiële valkuilen verbonden dan actieve afschrikking.[15] Het grootste probleem is dat deze vorm van afschrikking kostbaar en ingewikkeld is en voortdurend nieuwe investeringen blijft vragen – in het technologisch supersnel veranderende cyberdomein betekent stilstand achteruitgang. Daarnaast is het lastig om het bewustzijn bij honderd procent van de betrokkenen te vergroten, terwijl dit tot op bepaalde hoogte noodzakelijk is omdat cyberaanvallers altijd gebruik zullen maken van de zwakste schakel die zij kunnen vinden – bij wijze van spreken die ene onoplettende werknemer die besmette bestanden downloadt zodat de aanvaller een voet tussen de deur heeft. Zoals al eerder opgemerkt, heeft circa 35 procent van de computergebruikers niet eens antivirussoftware geïnstalleerd, dus er valt nog veel te verbeteren qua bewustzijn. Daarnaast zijn cyberaanvallers altijd in het voordeel: waar zij alle tijd hebben om naar kwetsbare punten in cyberinfrastructuur te speuren, moet het slachtoffer onmiddellijk reageren zodra zo'n (tot dan toe onbekend) kwetsbaar punt bij verrassing wordt gebruikt voor een cyberaanval.

Het is belangrijk te beseffen dat Nederland in het cyberdomein geen geïsoleerd gebied vormt; welke methoden ook worden ingezet om cyberdreigingen te verminderen, internationale samenwerking zal altijd noodzakelijk zijn. Afschrikking als methode om de cyberdreigingen te verminderen zal veelal ook verlopen via internationale samenwerkingsverbanden, zoals de

13 Clorinda Trujillo, 'The limits of cyberspace deterrence'. In: *Joint Forces Quarterly*, 75(2014)4, p. 49 ; Emilio Iasellio, 'Is cyber deterrence an illusory course of action?', p. 64.65.

14 KPN (in samenwerking met TNO, Politie en NCSC), European Cyber Security Perspectives 2015, p. 49-51.

15 David Elliot, 'Deterring strategic cyberattack'. In: *IEEE Security & Privacy*, 9(2011), p. 38-39.

EU en de NAVO. In het cyberdomein is afschrikking voorlopig nog een concept dat met veel vragen en problemen omgeven is. Duidelijk is in elk geval dat investeren in beveiliging zonder meer een bepaalde afschrikwekkende werking heeft. Goede cyberbeveiliging verhoogt niet alleen de kosten die een aanvaller moet maken voor een succesvolle aanval, maar ook het risico dat ondanks die kosten de aanval niet het gewenste effect sorteert en dus niet de gewenste baten tot gevolg heeft.

Bijlage 3
Afschrikking als veiligheidsconcept tegen georganiseerde criminaliteit

Sander Huisman[1]

Huidige situatie

De aard van de zogenaamde georganiseerde misdaad in Nederland is onlosmakelijk verbonden met de aard van de Nederlandse maatschappij en economie, evenals de geografische positie en de fysieke en digitale infrastructuur. Zo constateert Europol dat Nederland als draaischijf fungeert voor diverse vormen van grensoverschrijdende misdaad, zoals de handel en smokkel in drugs, sigaretten, en cybercrime.[2] Al decennialang speelt Nederland een dominante rol op diverse internationale misdaadmarkten, met name in relatie tot drugs, fraude, witwassen en cybercrime.[3] Het kent (1) met de internationale oriëntatie van de open Nederlandse economie en met (2) het goed ontwikkelde financiële stelsel met zijn specialistische dienstverleners nu eenmaal een goede handelsomgeving. Bovendien blijft (3) door het volume en de enorme diversiteit van het legale handelsverkeer het risico van onderschepping van illegale goederen klein. Deze mogelijkheden worden verder vergroot door de open grenzen met andere Europese landen. Het heeft (4) een uitstekende infrastructuur over weg, water, spoor en door de lucht. Nederland ligt (5) gunstig ten opzichte van diverse afzetmarkten en is een Europees distributiepunt en logistiek knooppunt, wat zich uit in de rol van Schiphol en andere vliegvelden, de Rotterdamse haven en andere logistieke overslagpunten. Er bestaan (6) door de aanwezigheid van diverse migrantengemeenschappen vele bruggenhoofden, met daarbinnen een (al dan niet passief) netwerk van helpers. Het heeft (7) met Amsterdam een aantrekkelijke internationale ontmoetingsplaats. Dit geldt vooral voor buitenlandse criminelen, die volgens enkele ervaren opsporingsambtenaren doorgaans onder de radar van politie en inlichtingendiensten blijven. Ten slotte heerst er (8) een beeld van een mild strafklimaat, waardoor misdaadondernemers graag in Nederland hun zaken blijven of komen doen.

De AIV[4] (2013) identificeert BTW-fraude in de EU en internetcriminaliteit als de voor Nederland meest omvangrijke en snelgroeiende onderwerpen op het terrein van grensoverschrijdende criminaliteit. Het door politieonderzoekers opgestelde Nationaal Dreigingsbeeld[5] constateert dat het criminele bedrijf momenteel het meest beïnvloed wordt door ontwikkelingen in de digitale technologie en het gebruik van het internet.

1 De auteur schrijft deze bijdrage op persoonlijke titel.
2 Europol/SOCTA, EU serious and organized crime threat assessment 2013. Den Haag: Europol, 2013.
3 Korps Landelijke Politiediensten, Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010. Driebergen: KLPD, 2010.
4 Adviesraad internationale veiligheid, criminaliteit, corruptie en instabiliteit, Een verkennend advies 85. Den Haag, 2013.
5 F. Boerman en M. Grapendaal, Nationaal Dreigingsbeeld Georganiseerde Criminaliteit 2012. Driebergen: KLPD, 2012.

Dat geldt voor verschillende vormen van georganiseerde misdaad, waar meerdere personen samenwerken die primair het verdienen van geld als doel hebben. Wanneer de kern van criminele organisaties[6] moet worden gekenschetst, kan de volgende driedeling worden gemaakt. Allereerst zijn er de beroepscriminelen die dominante posities innemen op de mondiale en Europese drugsmarkt. Ten tweede zijn er de individuen die zich met behulp van rechtspersonen verrijken door middel van milieumisdrijven, fraude, oplichting en witwasmethoden (zoals Palm Invest en Easy Life of de Bouwfraude en Vastgoedfraude). Ten derde zijn er de cyber-saboteurs die met geavanceerde digitale technieken burgers en bedrijven duperen en vaak ook een bedreiging vormen voor vitale infrastructuren (zoals de Bredolab-zaak uit 2012).

Gezien de geografische en logistieke sleutelpositie van Nederland in de internationale drugsmarkt, is het niet verwonderlijk dat Nederland voor misdaadondernemers uit diverse bronlanden en afzetlanden een logisch verblijfsoord is. Het anonieme verblijf van buitenlandse criminelen wordt gefaciliteerd door o.a. bereidwillige makelaars en de (vooralsnog) beschikbare anonieme prepaid telefoons en de afwezigheid van legitimatieplicht in sommige internetcafés. De laatste jaren is er steeds meer zicht gekomen op het bestaan van verschillende buitenlandse individuen en misdaadgroepen. Vele clusters of subculturen zijn al decennialang in Nederland aanwezig, zoals Britten, Colombianen, Italianen, ex-Joegoslaven en Hongkong-Chinezen. In talloze onderzoeken wordt waargenomen dat misdaadondernemingen in het topsegment van de drugsmarkt per definitie een brede internationale spreiding hebben. Naast de geografische reikwijdte is er bij de meest dominante netwerken ook sprake van een degelijke inbedding in legale sectoren en van contacten naar overheidsinstanties in het Midden-Oosten, West-Afrika en Zuid-Amerika.

De beroepscriminelen die in een bepaalde misdaadmarkt een dominante positie innemen, beschikken meestal ook over wijdverbreide internationale contacten. Dat is zeker het geval in de internationale drugsmarkt, waarin Nederland en Nederlandse beroepscriminelen een dominante positie vervullen. Vrijwel elk groot opsporingsonderzoek in dit circuit heeft internationale vertakkingen. België wordt vanuit crimineel oogpunt eerder als een soort achterland beschouwd dan als een ander land. Landen of regio's die in Nederlandse opsporingsonderzoeken veelvuldig naar voren komen zijn Spanje, Marokko, Turkije, verschillende landen in Zuid-Amerika, Oost-Europa, Oost-Azië en West-Afrika en de stadstaat Dubai.[7] Dat heeft soms te maken met de herkomst van de verdachten, soms met de rol van het land in een smokkeltraject, als bronland voor goederen of als schakel in financiële trajecten. De ervaring uit diverse onderzoeken is dat nieuwe relaties veelal ontstaan tijdens (buitenlandse) detentieperiodes (want: nieuwe handelsmogelijkheden).

6 De term 'criminele organisaties' is in de academische wereld omstreden omdat deze de nadruk legt op het bestaan van 'organisaties', terwijl in de ondoorzichtige wereld van misdaadbestrijding deze entiteit meestal niet waarneembaar is. Bovendien geeft 'organisatie' een betekenis van een bepaalde duur aan, terwijl de ervaring leert dat de meeste partnerschappen in het criminele circuit nogal vluchtig zijn (Kleemans e.a., 2002). In strafrechtelijk opzicht bestaan criminele organisaties, wanneer er sprake is van "deelneming aan een organisatie die tot oogmerk heeft het plegen van misdrijven". De veroordeling richt zich echter vrijwel altijd op een persoon, en zelden op een rechtspersoon. Om die reden wordt er hier gekozen voor het perspectief van het individu dat zich (met anderen) bezighoudt met het organiseren van winstgevende misdaad. Het zijn misdaadondernemers (Van Duyne, 1995), in de volksmond vaak betiteld als 'beroepscriminelen' die actief zijn in 'de georganiseerde misdaad'.

7 Korps Landelijke Politiediensten, Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010.

In milieucriminaliteit, diverse vormen van grootschalige fraudes en witwastrajecten speelt het gebruik van rechtspersonen een cruciale rol. Deze geven een beeld van legitimiteit en zorgen voor afscherming van organiserende personen. Zij zorgen met boekhoudkundige handelingen – zoals taxatierapporten en valse declaraties – voor een papieren (schijn)werkelijkheid, zodat alles lijkt te kloppen: “het kapitaal moet op zodanige wijze in het zicht van toezichthouders komen, dat het een stempel van goedkeuring krijgt en daarmee aanwending in de legale economie”.[8]

Het palet aan verdachten in de hoek van cybercriminaliteit is zeer divers: dat varieert van 16-jarige schoolgaande whizzkids tot 38-jarige informatica-cracks uit een voormalige Sovjetrepubliek. Ook de motieven variëren, van hacken vanuit een ideologisch doel tot het saboteren voor de lol en het geldelijk gewin (bv. door afpersen van slachtoffers). De grootste dreiging gaat uit van aanvallen op vitale infrastructuren. Hoewel overheidsinstanties hier het meest toe in staat lijken (zie bv. de destructieve kracht van het Stuxnet of het Regin-virus), kunnen ook individuen grote schade aanrichten. Politieonderzoekers zien dat de aanvallen – die zich vooral richten op het financiële systeem – technisch steeds geavanceerder worden. Een veel gebruikte techniek is de inzet van een botnet: een netwerk van vaak miljoenen geïnfecteerde computers, waarmee de eigen identiteit wordt afgeschermd en veel aanvalskracht kan worden ingezet. Tegen deze achtergrond kan gesteld worden dat de dreiging die van internationale criminaliteit uitgaat vooral de volgende nationale veiligheidsbelangen raakt: politiek-maatschappelijke stabiliteit (vertrouwen van burgers in de staat, vitale infrastructuur), economische veiligheid (financiële schade voor overheid en particulieren, het functioneren van het bedrijfsleven) en ecologische veiligheid (milieuschade).

Verwachting voor de komende 5 à 10 jaar

Dreigingen die voortkomen uit georganiseerde criminaliteit zullen ook in de komende 5 à 10 jaar waarschijnlijk onverminderd hoog zijn. Zoals o.a. in de Clingendael Monitor 2014 is beschreven, domineren twee trends het toekomstbeeld. Ten eerste zal grensoverschrijdende criminaliteit gekenmerkt worden door toenemende flexibiliteit (zowel in vorm, samenstelling en werkterrein) en mobiliteit (van personen, geld en goederen). Daarnaast zal er een verdere verschuiving optreden naar de virtuele wereld.[9]

Door de toenemende digitalisering en de vervagende grenzen zal het ook in de toekomst lastiger worden criminele organisaties te bestrijden, in het bijzonder wanneer zij grens-overschrijdend opereren. Niet alleen zal cybercriminaliteit flink in omvang toenemen, ook in traditionele georganiseerde misdaadzaken worden digitale anonimiserings- en versleutelingstechnieken steeds vaker waargenomen.[10] Daarnaast zijn er gevallen bekend waar ‘oude penoze’ de diensten van cybercriminelen inhuurt om het steeds verder gedigitaliseerde logistieke proces onder controle te krijgen, bijvoorbeeld door het hacken van computersystemen in zeehavens. In financiële trajecten is het mogelijk dat er meer gebruik gemaakt gaat worden van zogenaamde *New Payment Methods*, zoals prepaid debitcards waarop grote bedragen kunnen worden gezet zonder dat ze gekoppeld zijn aan herleidbare

8 Korps Landelijke Politiediensten, Criminaliteitsbeeldanalyse Witwassen 2012(b). Driebergen: KLPD, 2012.
9 Jan Rood, Frans-Paul van der Putten en Minke Meijnders, Een wereld zonder orde?; Clingendael Monitor 2015. Den Haag: Instituut Clingendael, februari 2015.
10 Korps Landelijke Politiediensten, Criminaliteitsbeeldanalyse Hightech Crime 2012(a). Driebergen: KLPD, 2012.

rekeninghouders. Daarnaast achten politieonderzoekers het aannemelijk dat *Trade Based Money Laundering* (TBML) vaker zal worden toegepast. Bij TBML worden legale goederen aangeschaft met misdaadgeld, waarna de goederen op de internationale markt worden verhandeld. Hierdoor kunnen grote geldbedragen (in waarde) verplaatst worden, en kunnen illegale legale winsten worden verantwoord (KLPD, 2012b).[11]

Succesvolle misdaadondernemingen hebben tevens een (informatie-)positie in de bovenwereld. Daarmee zijn zij in de gelegenheid om de bovenwereld te beïnvloeden. Zo kunnen posities verkregen worden in lokale gemeenschappen, bv. in horeca, vastgoed of winkelbestanden, waarmee ze een counterpart (gesprekspartner en legale actor) worden voor de lokale overheid. De aanhoudende economische recessie kan tot gevolg hebben dat mensen die in een schuldpositie verkeren sneller bereid zijn om hand- en spandiensten te verlenen. Dat kan op vele vlakken gebeuren. Te denken valt aan de inzet van *money-mules*, het verkopen van informatie binnen overheidsdiensten, banken of logistieke bedrijven (zoals in havens). Op deze wijze kunnen logistieke en financiële schakels gecorrumpeerd raken. Het staat buiten kijf dat afscherming een onlosmakelijk deel blijft van de werkwijze, zowel voor beroepscriminelen als voor financiële rechtspersonen en cyber-saboteurs. De verwachting is dat digitale verhullingstechnieken steeds vaker zullen worden toegepast, en ook steeds eenvoudiger beschikbaar zullen zijn. De laatste jaren is steeds meer waarneembaar dat fysieke misdaad gebruik maakt van TOR-netwerken en anonieme betalingen. Daarnaast zullen beroepscriminelen afhankelijk blijven van de loyaliteit en alertheid in hun goed-gezinde robuuste omgevingen (straten in bepaalde buurten, woonwagenkampen, clubhuizen van *outlaw motorgangs* (OMG's)).

Het toenemende gemak waarmee in het criminele circuit grensoverschrijdende relaties worden aangegaan zal in de toekomst speciale aandacht vragen. De beroepscriminelen die in een bepaalde misdaadmarkt een dominante positie innemen, beschikken meestal ook over wijdverbreide internationale contacten. Redelijk nieuw is de internationale dynamiek rondom de uitdijende OMG's. Waar tot 2009 de Hells Angels de enige internationale OMG in Nederland was, is dat vijf jaar later uitgebreid naar de Satudarah, No Surrender en de Bandidos. Ook het aantal leden en afdelingen is in vijf jaar tijd enorm gegroeid.[12] Meerdere beroepscriminelen hebben zich aangesloten bij een OMG. Een plausibele reden daarvoor is dat een internationale OMG extra relaties en handelsmogelijkheden oplevert, maar ook bescherming. Naarmate deze OMG's zich verder uitbreiden, zullen er met het doorkruisen van elkaars invloedssferen en belangen vaker onderlinge spanningen ontstaan. Dit zal vermoedelijk met geweldsincidenten gepaard gaan, zowel in Nederland als in landen waar andere afdelingen worden bestierd.

Een ontwikkeling die het criminaliteitsbeeld in de komende jaren mogelijk nog meer zal bepalen, is de toepassing van de nieuwste technologische innovaties. Er zullen steeds meer illegale goederen en diensten verhandeld worden verborgen online handelsmarkten (via TOR-netwerken). Voorbeelden hiervan zijn de (met inzet van het *Team Hightech Crime* van de Nederlandse politie) ontmantelde sites *Silkroad 2.0* en *Black Market Reloaded*. Innovaties als de 3D-printer en zgn. drones worden ook gebruikt in het criminele circuit, voornamelijk om de afscherming en contra-observatie richting concurrenten en de autoriteiten te verbeteren. De gebruikte hardware wordt steeds kleiner (dus goed te verhullen), steeds slimmer (bijvoor-

11 Korps Landelijke Politiediensten, Criminaliteitsbeeldanalyse Witwassen 2012(b).
12 Politie, Outlaw Bikers in Nederland. Woerden: Politie Landelijke Eenheid, 2014.

beeld op afstand te besturen) en steeds krachtiger. Zo zullen nanotechnologie en robots op termijn ongetwijfeld ook in het criminele circuit een toepassing vinden. Ook een 'traditioneel' delict als identiteitsfraude (dat de basis vormt voor vele criminele handelingen) zal door technologische innovaties mogelijk nieuwe dimensies krijgen. Verwacht mag worden dat deze wedloop zal continueren.

Relevantie van afschrikking als veiligheidsconcept

Afschrikking op basis van vergelding is een belangrijk instrument bij het tegengaan van dreigingen die voortkomen uit (internationale) criminele activiteiten. Onderzoek heeft aangetoond dat juist preventieve maatregelen het meeste effect hebben in de brede aanpak van logistieke onderdelen van misdaadmarkten.[13] Wanneer de autoriteiten concrete verdachten op het oog hebben, kunnen bestuurlijke of fiscale interventies ook zeer effectief zijn in de misdaadbestrijding. Dergelijke aanpakken kunnen alleen in een multidisciplinaire benadering tot wasdom komen, waarbij meerdere partijen zich probleemeigenaar voelen en daardoor afstemming zoeken over een aanpak waarin allen eigen capaciteit inzetten. Nederland is vanuit dit opzicht in Europees en in breder internationaal verband een voorloper. Los van de ontwikkeling naar een bredere aanpak die de laatste jaren is geïnitieerd, is het echter niet duidelijk welke aanpak door criminele organisaties of door afzonderlijke beroepscriminelen als afschrikwekkend wordt ervaren. Een strafrechtelijke aanpak leidt veelal tot een detentie of een ontneming, een bestuurlijke aanpak tot een bestuurlijke maatregel (bv. intrekken van een vergunning of het sluiten van een woning), een fiscale aanpak tot een financiële sanctie (bv. een naheffing of een aanslag). Het is aannemelijk dat een gecombineerde (of beter: integrale) aanpak als meest doeltreffend wordt ervaren, en daarmee ook als meest afschrikwekkend wordt beleefd.

Misdaadondernemingen reageren daarbij snel op veranderingen in hun omgeving. Wanneer overheidsinterventies plaatsvinden, zullen activiteiten tijdelijk worden stilgelegd of worden verplaatst. Wanneer de autoriteiten wetswijzigingen doorvoeren, zal de bedrijfsvoering waar mogelijk worden aangepast om de schijn van legaliteit op te kunnen houden. Wanneer bepaalde branches wijzigingen aanbrengen in logistieke processen, zullen logistieke handelingen worden aangepast. De versnippering die de opsporing in Nederland jarenlang kenmerkte was voor subjecten die 'de apenrots' willen beklimmen een ideale voedingsbodem. De bestaande barrières (controles, opsporing, vervolging, detentie, reclassering) zijn voor hen vrij eenvoudig te frustreren, te beslechten of te doorstaan. Wanneer kansen op interventies eerder worden herkend en opgepakt kan de ontwikkeling van een misdaadcarrière worden tegengegaan. Dat betekent wel dat de dreiging van een interventie (zoals een snel beslag of een snelle veroordeling) ook geloofwaardig moet zijn, wat pas kan als er in dit opzicht door autoriteiten een '*track record*' is opgebouwd.

De meest succesvolle beroepscriminelen ontlenen hun macht aan hun reputatie en status in het criminele circuit, maar kunnen deze macht niet behouden zonder een solide sociale omgeving (buurt, familie, criminele 'ploeg'). Duidelijk is dat een tijdelijke detentie bij de zwaardere beroepscriminelen geen effect heeft: dat is een ingecalculeerd bedrijfsrisico dat bovendien ook nog eens nieuwe kansen biedt (nl. het aangaan van nieuwe relaties). De strategische binding vanuit de sociale omgeving is sterk, deze wordt niet tegengegaan

13 Zie o.a.: H.G. van de Bunt en C.R.A. van der Schroot, *Prevention of organised crime: a situational approach*. Den Haag: Boom, 2003.

middels een tijdelijke detentie. De robuustheid (van misdaadgroepen) is daarmee haast onlosmakelijk verbonden met de aanwezigheid van *thick crime habitats* en *community support* .[14] Een solide reputatie is essentieel voor de ontwikkeling van een criminele carrière. Het aanzien van professionele misdaadondernemers is mede gebaseerd op historisch succes, vertrouwen, discipline en bruikbare contacten, zakelijk inzicht, maar ook op zwijgzaamheid naar de autoriteiten en intimiderende vaardigheden.[15] In dit verband hebben zichtbare overheidsdienaren (bv. baliepersoneel van een gemeente, een wijkagent) het meest te duchten. Dit krijgt een extra dimensie wanneer partners of familieleden bij een overheidsdienst werkzaam zijn, en specifieke informatie kunnen inzien. Criminele netwerken kunnen daardoor een robuust karakter krijgen en kunnen daardoor wel wat overheidsinterventies incasseren. Het is geen eenvoudige klus om de *resilience* in het criminele circuit te verminderen.

Er zijn voorbeelden van overheidsinterventies waarbij een crimineel netwerk dusdanig werd ontmanteld, dat ook de nabije (en profiterende) sociale omgeving werd 'berispt'. Zoals in 2010 bij een puissant rijke drugshandelaar die jarenlang onder de radar opereerde en die in het criminele circuit een zeer solide naam had opgebouwd. Een intensief (internationaal) strafrechtelijk en financieel onderzoek leverde niet alleen een jarenlange veroordeling op, maar ook een breed beslag op diverse (roerende en onroerende) goederen die op naam van vertrouwelingen en familieleden waren gezet. Deze interventie had daarmee een signaalwerking die verder ging dan de veroordeelden. Een dermate veelomvattende interventie kan vanuit capaciteitsoogpunt echter maar zeer beperkt worden ingezet. Er zullen dus slimme en weloverwogen keuzes moeten worden gemaakt, waarbij het liefst op basis van een actuele informatiepositie het daadwerkelijk effect ook kan worden ingeschat. Diverse onderzoeken geven aan dat een financiële aanpak van misdaadondernemers (en daarmee ook criminele organisaties) het meest effectief is. Daarbij moet vooral gekozen worden voor een (snel) conservatoir beslag, zodat de verdachte en zijn sociale omgeving direct de gevolgen ervaart.[16] Van dit signaal gaat een afschrikkende werking uit.

Een bijzondere vorm van afschrikking is wanneer voormalige *partners-in-crime* informatie gaan geven aan politie en justitie, teneinde belastende gegevens aan te dragen over de strafbare gedragingen van andere misdaadondernemers. Het is niet voor niets dat strafrechtadvocaten die vooral personen bijstaan die frequent naar voren komen in onderzoeken naar georganiseerde misdaad, felle kritiek uiten op de frequentere inzet van de criminele burgerinfiltrant. Vanuit opsporingsoogpunt is deze inzet op het verkrijgen van *human intelligence* vanuit de onderwereld zelf echter van steeds groter belang. Dit is onlosmakelijk verbonden met de ervaring dat meer traditionele opsporingsmethoden zoals observatie en het onderscheppen van communicatie steeds minder bewijskracht opleveren. Het gaat vaak om zeer gesloten groepen die hun gedragingen en bewegingen structureel afschermen. Dat gebeurt met de inzet van technische middelen, maar ook door het inzetten van stromannen en het intimideren en bedreigen van mogelijke getuigen of ambtenaren. Daardoor worden bronnen uit het criminele circuit steeds belangrijker, zowel als het gaat om de informanten als de (bedreigde) getuigen en in bepaalde gevallen een criminele burgerinfiltrant.

14 J. Ayling, 'Criminal Organizations and Resilience'. In: *International Journal of Law, Crime and Justice*. 37(2009), p. 182-196.

15 Korps Landelijke Politiediensten, Overall-beeld aandachtsgebieden Dienst Nationale Recherche 2010.

16 E.W. Kruisbergen, H.G. van de Bunt en E.R. Kleemans, Vierde monitor georganiseerde criminaliteit. Den Haag/ Rotterdam: WODC/EUR, 2012.

De dreiging van vergelding moet geloofwaardig zijn, alleen dan kan afschrikking effectief zijn.[17] Frappant is dat deze regel ook in het criminele circuit een voorwaarde is voor een solide en geloofwaardige status. Het risico op ontdekking, vervolging en detentie moet groot zijn. Dit vereist een robuuste overheid die snel, flexibel en krachtig intervenieert. Het vereist een goede en dus vooral actuele informatie-positie, en een goede samenwerking tussen betrokken partners (zowel publiek als privaat). Het vereist een solide contingent van *capable guardians* die op basis van actueel inzicht de *willing offenders* kunnen aanpakken. In een wereld waarin nationale grenzen steeds meer vervagen als gevolg van globalisering en het internet is het belang van internationale samenwerking evident. Dit houdt ook in dat buitenlandse rechtshulpverzoeken onverwijld moeten worden opgepakt. Het vereist een snelle opvolging van interventies naar veroordeling en executie van het vonnis, zodat het signaal ook betekenis heeft voor de omgeving. Het vereist niet alleen een goede samenwerking tussen instanties, maar zeker ook een snel handelen door professionals in hun eigen werksetting. Het vereist ten slotte ook een weloverwogen beeldvorming naar de publieke opinie. Mediastrategie is dus van groot belang, omdat met het juiste '*frame*' een groot effect kan worden behaald. Tot op heden leert de ervaring dat dergelijke boodschappen pas betekenis krijgen, wanneer er met de inzet van opsporingsmethoden nieuw en uniek inzicht is verkregen. Onder de juiste omstandigheden kan afschrikking door vergelding dus een effectief instrument zijn tegen criminaliteit, ook met betrekking tot criminele activiteiten vanuit het buitenland. Andere vormen van afschrikking die deel uitmaken van het analysekader in dit rapport (d.w.z. indirecte verhoging van de kosten of de verlaging van de baten voor de dader) lijken echter minder relevant te zijn tegen deze dreiging, behalve waar het gaat om verdedigingsmaatregelen op het gebied van cyberveiligheid die de kosten voor cybercriminaliteit tegen Nederlandse doelen aanzienlijk verhogen.

17 K.H. Hicks, 'The case of deterrence'. In: C. Cohen en J. Gabel (eds.), 2015 Global Forecast: Crisis and Opportunity. Washington: Center for Strategic and International Studies, 2014.

Bijlage 4
Afschrikking als veiligheidsconcept tegen dreigingen via het economisch domein

Peter van Bergeijk

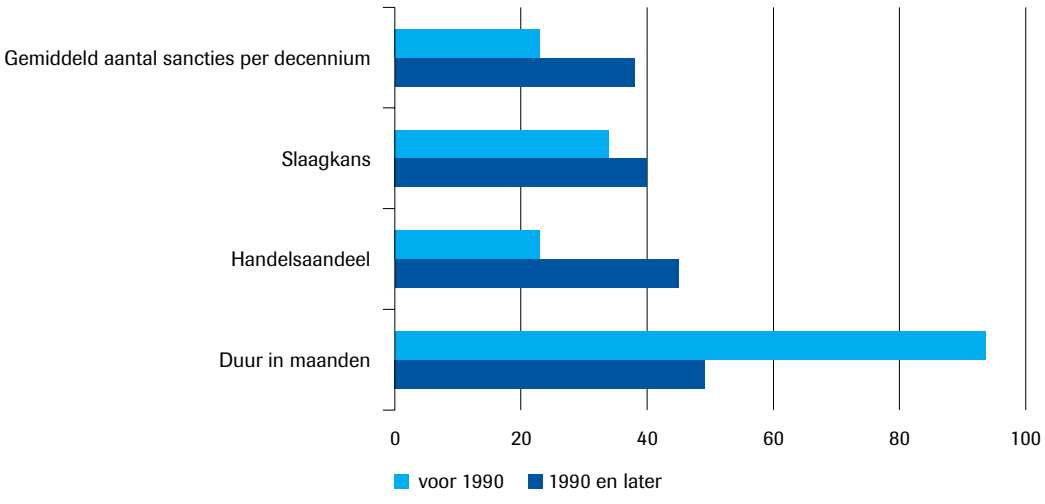
Huidige situatie

Met zijn open en internationaal georiënteerde economie is Nederland potentieel kwetsbaar voor externe veiligheidsdreigingen die ons land via het economische domein bereiken. Deze kwetsbaarheid verdient extra aandacht vanwege de toenemende geopolitieke spanningen in de wereld en door instabiliteit in regio's nabij Europa, zoals geschetst in het overzichtshoofdstuk van de Clingendael Monitor 2015. Het 'economische domein' omvat in deze context alle externe economische contacten van Nederland. De dreiging omvat enerzijds activiteiten die economische kernprocessen, d.w.z. processen die van vitaal belang zijn voor het economisch functioneren (energieproductie, communicatie, transport, geldverkeer, enz.), verstoren. Hierbij kan het gaan om het uitschakelen van een kernproces of het ondergraven van het vertrouwen in dat kernproces bij burgers en bedrijfsleven. Een stabiele aanvoer van energie en andere grondstoffen uit het buitenland is van groot belang voor het functioneren van economische kernprocessen. Zo is een cyberaanval op het Nederlandse betalingsverkeer een voorbeeld van een aanval gericht op een economisch kernproces die tegelijkertijd (ook als deze mislukt) het vertrouwen in het ongestoorde functioneren ervan kan ondergraven. In dezelfde zin kan een fysieke aanval op de energievoorziening (bijvoorbeeld een distributiepunt, al dan niet in Nederland zelf) of een blokkade van de toevoer van bepaalde grondstoffen economische kernprocessen verstoren. Maar naast deze kernprocessen gaat het anderzijds ook om het Nederlandse belang bij vrije handel en toegang tot buitenlandse markten en om het aantrekken van buitenlandse investeringen als basis voor werkgelegenheid en een dynamisch bedrijfsleven. In het bijzonder het verstoren van internationale handel en investeringen kan leiden tot grote macro-economische schade. De impact van de verstoring zal groter zijn naarmate zij onverwachter en langduriger plaatsvindt. Op al deze dimensies is Nederland vanuit handelingen binnen het economisch domein kwetsbaar. Van Bergeijk en Mennen (2014) bespreken een groot aantal economische verstoringen die in het kader van de Nationale Risico Beoordeling zijn geanalyseerd.

Afschrikking kan in deze context mogelijk relevant zijn waar het gaat om actoren die moedwillig handelingen verrichten die de Nederlandse veiligheid schaden. Drie relevante groepen van actoren zijn criminelen, terroristen en staten. Internationaal opererende criminele organisaties die Nederland schaden, doen dat doorgaans via het economische domein. Drugshandel, mensensmokkel, fraude, witwaspraktijken en internetcriminaliteit hebben een directe relatie met economische processen. Terrorisme is aan de economie gerelateerd waar het gaat om de financiering van terroristische organisaties of om pogingen om door middel van aanslagen economische kernprocessen te raken. Activiteiten vanuit criminele en terroristische organisaties en de relevantie daarvoor voor de nationale veiligheid worden elders in deze studie besproken.

Acties van staten via het economische domein kunnen op meerdere manieren een bedreiging vormen voor de nationale veiligheid. Ten eerste kunnen economische kwetsbaarheden worden benut door andere staten die door direct economisch ingrijpen de concurrentiepositie van de eigen economie versterken ten koste van die van de Nederlandse. Middelen die buitenlandse overheden daarvoor mogelijk kunnen inzetten zijn onder andere het bevoordelen van nationale bedrijven op de eigen markt, het geven van staatssteun aan nationale bedrijven, het uitvoeren of ondersteunen van bedrijfsspionage (al dan niet via het cyberdomein) en het gebruiken van politiek-diplomatieke invloed om de toegang tot markten of grondstoffen in derde landen te beperken. Ook bestaat de mogelijkheid dat buitenlandse overheden gebruik maken van staatsbedrijven of bedrijven waarop ze anderszins een grote invloed hebben om via bedrijfsovernames concurrentievoordelen aan Nederlandse zijde gericht te elimineren en/of afhankelijkheden te creëren. Het is afhankelijk van de schaal van dergelijke maatregelen en hun relevantie voor economische kernprocessen of ze een bedreiging vormen voor de nationale (economische) veiligheid.

Ten tweede kunnen buitenlandse overheden proberen politieke druk uit te oefenen door middel van economische sancties. Het gaat daarbij niet alleen om daadwerkelijke sancties maar ook om het impliciet of expliciet dreigen met sancties. Een afgeleide vorm van sancties zijn *fuzzy sanctions*: consumentenboycots die Nederlandse economische belangen schaden maar die niet door een buitenlandse regering zijn geïnitieerd of geleid worden. Het afgelopen decennium is op internationaal niveau sprake van een betekenisvolle toename van het gebruik van economische strafmaatregelen. Deze trend heeft zich al ingezet in de jaren negentig van de vorige eeuw toen de ineenstorting van het Sovjetimperium een einde maakte aan het conflict tussen de twee supermachten waardoor sancties in de VN minder werden beperkt door geopolitieke overwegingen. Figuur 1 illustreert de toename van het gemiddelde aantal sancties in samenhang met een hogere slaagkans die mogelijk wordt veroorzaakt door een grotere handelsverbondenheid tussen sanctienemer en sanctiedoelwit.



Figuur 1 Veranderende karakteristieken van economische strafmaatregelen (voor en na 1990)

Bron: Berekend uit van Bergeijk 2009, tabel 6.6 p. 134

Het is onduidelijk of de laatstgenoemde waarneming een gevolg is van een betere selectie vooraf van gevallen waarin het sanctie instrument wordt gebruikt, dan wel een meer

algemene trend tot internationalisering van alle economieën reflecteert. Hoe het ook zij: sancties worden vaker ingezet en de desbetreffende stromen zijn omvangrijker dan in het verleden. Het ligt daarom in de lijn der verwachting dat Nederland vaker betrokken zal zijn bij economische strafmaatregelen, ook als sanctiedoelwit. Het kan hierbij ook gaan om sancties tegen andere landen dan Nederland waardoor belangrijke Nederlandse economische belangen indirect worden getroffen. Deze ontwikkeling is niet alleen kwantitatief maar ook kwalitatief opgetreden. Een ander nieuw kwalitatief aspect van sancties zijn de zogenoemde *smart sanctions,* die niet gericht zijn op een bevolking maar op specifieke (aan) beslissers (gelieerde groepen). Deze laatste vorm is nog niet tegen Nederland in praktijk gebracht.

Samengevat betreffen de veiligheidsbelangen die mogelijk geschaad worden via economische beïnvloeding met name de economische veiligheid, de sociale-politieke stabiliteit en de territoriale veiligheid (in dit geval de ongewenste inperking van het autonoom functioneren van de Nederlands staat). Potentieel bedreigende actoren zijn terroristische organisaties, criminele organisaties, maatschappelijke boycotbewegingen, grote mogendheden, en regeringen van landen met een grote mate van invloed over specifieke internationale productketens, grondstoffen, technologieën of met grote financiële reserves.

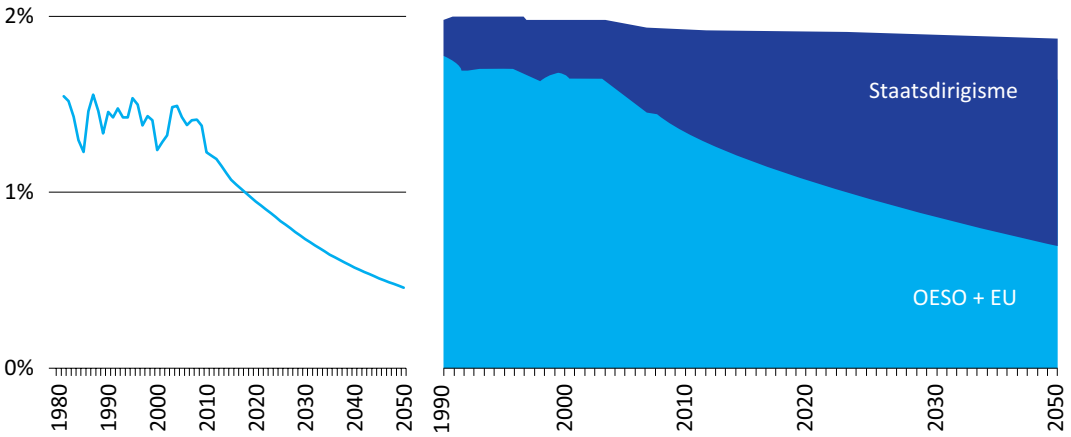
Verwachting voor de komende 5 à 10 jaar

Economische kernprocessen worden steeds gecompliceerder en afhankelijker van techniek en buitenland. Verlenging en vertakking van internationale waardeketens vergroot enerzijds de economische veiligheid (internationale waardeketens hebben de wereldhandelsval van 2008/9 gedempt) maar er ontstaan ook nieuwe risico's. Het creëren van toegevoegde waarde in Nederland wordt steeds afhankelijker van toelevering uit en afzet in het buitenland. Afbreukrisico's ontstaan zowel lager, als hoger in de waardeketen. Nederland is zowel als knooppunt van internationale handelsstromen en als deelnemer in het internationale economische systeem kwetsbaar (van Bergeijk en Mennen 2014); dit blijft ook in de komende jaren het geval. Dit geldt voor potentiële aanvallen vanuit alle relevante groepen van actoren: criminelen, terroristen en staten. Zoals elders in dit rapport wordt besproken mag worden verwacht dat in de toekomst dreigingen vanuit criminele en terroristische actoren relevant blijven en – onder andere via het cyberdomein – verder zullen toenemen. De steeds intensievere integratie van het internet in economie en samenleving geeft ook staten meer mogelijkheden om andere staten via ambigue oorlogsvoering economisch te treffen.

Op grond van gebeurtenissen gedurende de laatste vijf jaar moet Nederland rekening houden met een grotere waarschijnlijk van sancties die tegen haar gericht zijn, of tegen andere landen maar die daarbij ook Nederlandse economische belangen treffen. Wat betreft sancties tegen Nederland kan gedacht worden aan sancties of boycots die zijn ingegeven door religieuze en geopolitieke overwegingen. Het religieuze thema heeft in het verleden al aanleiding gegeven tot *fuzzy sanctions* (rond Fitna), afgelastingen van staatsbezoeken (na afsluiten gedoogakkoord) en dreigementen om Nederlandse bedrijven te boycotten (Saoedi-Arabië). Bij sancties tussen andere partijen waarbij Nederland indirect wordt getroffen kan het gaan om geopolitiek gemotiveerde sancties zoals een verdere verharding van de recente koude handelsoorlog tussen Rusland en het Westen, maar kunnen ook fricties tussen de VS en China tot de mogelijkheden gaan behoren. Het risico op geopolitieke escalatie met betrekking tot handel en investeringen wordt groter naarmate het aandeel van de opkomende markten toeneemt. Enerzijds omdat economische macht vertaald wordt in politieke macht, anderzijds omdat hun afhankelijkheid van de OESO landen afneemt. In het verleden hebben Nederlandse bedrijven al te maken gekregen met Amerikaanse en Europese sancties tegen

landen als Cuba, Iran en Rusland. Eventuele toekomstige sancties door de VS tegen Chinese doelen zouden nog verdergaande gevolgen voor Nederlandse bedrijfsbelangen kunnen hebben.

Een belangrijke verandering in de komende 5 à 10 jaar betreft het afnemende vermogen van Nederland om door middel van zijn internationale invloed mogelijke dreigingen via het economische domein te beperken. Dit volgt uit de zekerheid dat het Nederlandse aandeel in het BPP (Bruto Planetair Product) afkalft, niet omdat Nederland armer wordt, maar omdat de nieuwe economische grootmachten zeer sterk groeien (Figuur 2). De machtsbasis/ invloed van Nederland zal voor 2030 halveren en het is waarschijnlijk dat deze afkalving haar schaduw vooruit zal werpen en in toenemende mate de beleidsruimte van Nederland zal beïnvloeden. Geprivilegieerde informatie en sleutelposities zullen Nederland steeds minder vanzelfsprekend toevallen. Deze beperking van de beleidsruimte is niet goed in geld uit te drukken, maar duidelijk is wel dat dit een belangrijke macro-economische kostenpost kan opleveren. In het verleden heeft Nederland een belangrijke rol kunnen spelen bij het vormgeven van instituties die van wezenlijk belang voor ons welzijn zijn geweest. Het wordt steeds onwaarschijnlijker dat Nederlandse topbeleidmakers die rol toebedeeld zullen krijgen.



Figuur 2 **Afkalvend aandeel van Nederland (links) en verschuiving van aandeel naar beleidsorientatie (prognose tot en met 2050).**
Bron: berekend uit: Fouré, J.,e.a. onderliggende data set

Nederland is nog steeds een belangrijke open economie. Schiphol en Rotterdam zijn mondiale knooppunten; er is betekenisvolle internationale concurrentie maar op middellange termijn mag er vanuit worden gegaan dat Nederland toonaangevend blijft. Anders is dit met de vooraanstaande positie in het financiële speelveld. Hieraan is niet alleen de bankencrisis debet, maar ook beleidskeuzen op het gebied van bijvoorbeeld de ontwikkelingssamenwerking waaronder de reductie van de norm voor ontwikkelingssamenwerking ten opzichte van het BNP. De afkalving is natuurlijk geen uniek Nederlands probleem. Op mondiaal niveau neemt het aandeel af van de markteconomieën die het multilaterale systeem sinds de Tweede Wereldoorlog hebben gedragen en ontwikkeld en die zich committeren aan de spelregels van de OESO. De crisis heeft de geloofwaardigheid van de consensus van Washington ondergraven; het Chinese ontwikkelingsmodel is effectief en biedt een duidelijk alternatief. Onvermijdelijk leiden deze gegevenheden tot wijziging in de normen en regels van het internationale systeem, ook waar het gaat om het verankeren van traditionele waarden van de grote democratische economieën. We zien dat de 'BRIICS' (Brazilië, Rusland,

India, Indonesië, China en Zuid-Afrika) proactief trachten het vacuüm te vullen (vergelijk Morse en Keohane, 2014). Er worden stappen gezet om een alternatief op te zetten voor de Wereldbank. In de bilaterale internationale samenwerking wordt door de BRIICS anders dan door het *Development Assistance Committee* van de OESO geen bijzondere waarde toegekend aan emancipatie, het bereiken van de allerarmsten en mensenrechten. Met het groeien van de economische macht van de BRIICS wordt een geringere terughoudendheid verwacht om economische relaties in het algemeen in een voor hen relevante geopolitieke context te plaatsen.

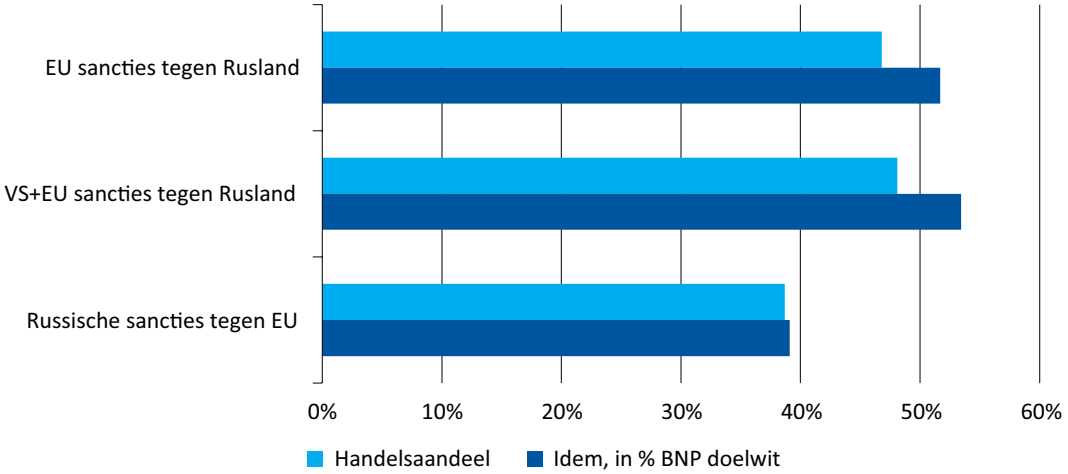
Een complicerende factor bij dit alles is dat essentiële faciliteiten (harde en zachte infrastructuur die noodzakelijk is voor het internationale bedrijfsleven, waaronder communicatiesatellieten, beveiligd berichtenverkeer voor handelskrediet en internationale betalingen, internationale spelregels en mogelijkheden om die af te dwingen, enz.) steeds vaker in andere jurisdicties dan tot nu toe gebruikelijk tot stand worden gebracht; dit laatste wordt zelfs waarschijnlijker naarmate die jurisdicties een groter economisch gewicht/belang hebben. Dit kan grote extraterritoriale werking hebben en zo een bedreiging vormen voor de nationale veiligheid. De SWIFT sancties tegen Iran zijn een voorbeeld van harde infrastructuur (communicatiekanaal voor het internationaal betalingsverkeer) die voor Iran niet langer beschikbaar was. Het is niet te voorzien waar aanbieders van nieuwe mondiale essentiële faciliteiten zich zullen bevinden; wel is voorspelbaar dat dit steeds vaker in de BRIICS-landen zal zijn en dat het moeilijker zal zijn multilateraal beleid vorm te geven of mondiale essentiële faciliteiten op multilaterale wijze te beheren. Het multilaterale systeem is traditioneel de verdedigingslinie voor kleine en middelgrote landen; in de huidige context is regionale samenwerking onontbeerlijker om tegenwicht te kunnen bieden.

Relevantie van afschrikking als veiligheidsconcept

In de economische literatuur speelt het afschrikkingsconcept – een verandering in de (verwachte) kosten-batenverhouding van overwogen gedragingen – een belangrijke rol. De toepassing van dit concept in de vorm van het rationele keuzemodel heeft vooral een eigen plaats gevonden in de economische analyse van crimineel gedrag en de preventie daarvan ('*Law & economics*'). In het verlengde hiervan is er recent veel aandacht voor diverse vormen van terrorisme (Miller, 2013, Schneider e.a. 2014). De analyse van economische sancties (zowel positieve als negatieve interactie) is in een vergelijkbaar kader geplaatst (Dizaji en van Bergeijk 2013). In de kern komen de bevindingen neer op het volgende. Actoren die gedrag overwegen dat de nationale veiligheid bedreigt, kunnen door wijziging in (de afweging van) hun verwachte kosten en baten (tijdelijk) worden geprikkeld om dat gedrag achterwege te laten. Dit effect kan tijdelijk zijn indien substitutie, aanpassing en innovatie optreden. Daarnaast is vaak sprake van verlegging naar andere vormen van wangedrag of andere (gemakkelijkere) doelwitten.

Het afschrikkingsconcept grijpt aan bij het verhogen van de *kosten* die een aanvaller moet maken door te investeren in preventieve beschermingsbarrières en intensievere opsporing. Voor zover de aanvaller en zijn bezittingen zich niet op Nederlands grondgebied bevinden, gaat van het verhogen van straffen geen afschrikwekkende werking uit. Door de mondialisering kunnen economische dreigingen in bepaalde domeinen overal ter wereld ontstaan (cybermisdaad is een voorbeeld). Het identificeren van de bron van de dreiging wordt hierdoor gecompliceerd. Naarmate identificatie moeilijker is, is het afschrikkingsconcept minder toepasbaar. Concrete middelen die ter afschrikking kunnen worden ingezet tegen criminele of terroristische organisaties zijn: het nemen

van (extra) beschermingsmaatregelen, het dreigen met *smart sanctions,* het dreigen met strafmaatregelen gericht op de omgeving van de individuele bedreiger en beleidvorming om de voedingsbodem waaruit de dreiging ontstaat te beïnvloeden. Wat betreft individuele criminelen of terroristen is bovendien het verhogen van de detectiekans een middel dat ter afschrikking kan worden ingezet. Afschrikking tegen statelijke actoren kan mogelijk worden bereikt door het dreigen met tegensancties en door het vergroten van de weerbaarheid tegen sancties.



Figuur 3 Slaagkans voor sancties rond Oekraïne.
Bron: Voxeu, 25 april 2014

De *baten* kunnen voor politiek-gemotiveerde daders worden verlaagd door de (potentiele) impact van de verstoring te verminderen (prioriteitstelling, vervangende productie-mogelijkheden, grotere weerbaarheid, duidelijke communicatie van oplossingen). Afhankelijkheid in toelevering en afzet moet daarbij zoveel mogelijk voorkomen worden; enerzijds om vervangingsmogelijkheden te hebben en anderzijds omdat dan een aanval op meerdere kanalen nodig is om economische kernprocessen of -belangen te treffen. Daarnaast kunnen maatregelen worden genomen om de weerbaarheid van de bevolking en het bedrijfsleven te vergroten (Frey 2009). Verder kan de inschatting die een dader maakt van de kans op mogelijke baten worden beïnvloed door het nemen van beschermingsmaatregelen.

Een complicerende factor is dat zowel aan de kant van de zender (bijv. de determinanten van terrorisme, zie Kis-Katos e.a. 2014) als aan de kant van het doelwit (bijv. de invloed van de regeringsvorm op de effecten van sancties, zie Von Soest en Wahman, 2014) sprake is van grote heterogeniteit. De implicatie is dat bevindingen voor een bepaald domein (bijv. religieus terrorisme) niet noodzakelijkerwijze relevant zijn voor een ander domein. Voor alle afschrikkingsmaatregelen geldt daarnaast dat de effectiviteit ervan aanzienlijk groter is als ze als onderdeel van bilaterale of multilaterale (via de EU of andere samenwerkingsverbanden) samenwerking worden genomen. De mogelijkheden voor Nederland om zonder dergelijke samenwerking afschrikking toe te passen om dreigingen via het economische domein tegen te gaan zijn zeer beperkt.

Literatuur

P.A.G. van Bergeijk, *Economic diplomacy and the geography of international trade*. Edward Elgar, 2009.

P.A.G. van Bergeijk en M.G. Mennen, 'De economische betekenis van nationale veiligheidsrisico's'. In: *Tijdschrift voor Veiligheid*, 13(2014)2, p. 35-51.

S.F. Dizaji en P.A.G. van Bergeijk, Potential early phase success and ultimate failure of economic sanctions: A VAR approach with an application to Iran. In: *Journal of Peace Research*. 50(2013)6, p. 721-736.

J. Fouré, A. Bénassy-Quéré en L. Fontagne, '2012, The Great Shift: Macroeconomic projections for the world economy at the 2050 horizon'. In: *CEPII 2012–03*, CEPII: Parijs.

B.S. Fresy, How can business cope with terrorism. In: *Journal of Policy Modelling*, 31(2009), p. 779-787.

A. Hoeffler, 'Can international interventions secure the peace?'. In: *International Area Studies Review*, 17(2014)1, p. 75-94.

Krisztina Kis-Katos, Helge Liebert en Günther G. Schulze, 'On the heterogeneity of terror'. In: *European Economic Review* 68(2014), p. 116-136.

K. Kholodilin, D. Ulbricht en G. Wagner. 'Are the Economic Sanctions against Russia Effective?'. In: *DIW Roundup: Politik im Fokus* 28. DIW Berlin, German Institute for Economic Research, 2014.

Jeffrey W. Knopf, Steven Metz, en James Andrew Lewis, 'Old Tools, New Century: Deterrence, Containment and Collective Cyberdefense'. In: *World Politics Review*, 2013.

G.D. Miller, 'Terrorist decision making and the deterrence problem'. In: *Studies in Conflict & Terrorism*, 36(2013), p. 132-151.

J. C. Morse en R.O. Keohane, 'Contested multilateralism'. In: *The Review of International Organizations*, 2014, p. 1-28.

Friedrich Schneider, Tilman Brück en Daniel Meierrieks, 'The Economics of Counterterrorism: A Survey'. In: *Journal of Economic Surveys*, 2014.

C. von Soest en M. Wahman, 'Are democratic sanctions really counterproductive?'. In: *Democratization*, p. 1-24.

A.W. de Vries, C. Portela en B.Guijarro-Usobiaga, 'Improving the Effectiveness of Sanctions: A Checklist for the EU'. In: *CEPS special report 95*, 2014.

Bijlage 5
Afschrikking als veiligheidsconcept tegen ambigue oorlogsvoering

Rob Hendriks

Huidige situatie

Anno 2015 lijkt het tijd om te herkennen en erkennen dat er sprake is een significante verandering van het heersende paradigma voor oorlog. Paradigma's hebben grote invloed op de toegepaste typen van oorlogsvoering. Inzicht in die verandering is dus nodig om het dreigingsthema 'ambigue oorlogsvoering' te kunnen beschrijven en doorgronden ten einde aan te kunnen geven of en in hoeverre afschrikking nog van toepassing is. De recente geschiedenis toont grofweg drie opeenvolgende paradigma's voor oorlog.[1]

Van 1648 tot 1945 was het paradigma *'staat vs. staat'* (evt. in wisselend samengestelde verbonden). Het Westfaalse statensysteem, met territoriale integriteit en non-interventie als belangrijkste ingrediënten, leidde tot de '*raison d'état*' en behoud van soevereiniteit als leidende beginselen in het buitenlands beleid van staten. In deze periode was weliswaar vaak sprake van lange oorlogen, maar niet de hele samenleving werd daarin betrokken. Oorlogen kenden ook lange perioden van relatieve rust, impasses zelfs, die gevolgd werden door hevige, maar afgebakende, veldslagen. De natie moest voortbestaan en de legers werden niet totaal gesleten vanwege de noodzaak voortzettingsvermogen te behouden. Dit beperkte karakter van oorlogen veranderde in de loop der tijd en vooral na de industrialisatie kreeg de 'staat vs. staat' oorlog steeds meer een 'totaal' karakter[2], waarbij de hele samenleving in enigerlei vorm bijdroeg aan, maar ook leed onder, de oorlog.

Vervolgens was van 1945 tot 1989 het paradigma *'vast statenpact vs. vast statenpact'* dominant. De NAVO en het Warschau Pact hadden elkaar via MAD[3] in een houdgreep. De Koude Oorlog had desondanks wel degelijk warme momenten; dit naast de oplopende spanningen over Berlijn en Cuba. Mogendheden kregen te maken met dekolonisatie-oorlogen, veelal in de vorm van een '*insurgency*' door de autochtone bevolking en een '*counter-insurgency*' door de koloniale overheerser. De nieuwe onafhankelijke landen waren al snel inzet van het mondiale schaakspel tussen de twee grootste leden van beide pacten (respectievelijk de VS en de USSR), die er voor kozen om invloed in de wereld via derden te doen gelden. Dergelijke '*war by proxy*' (oorlogsvoering via tussenactoren) was weliswaar niet direct gericht op de opponent, maar wel op het politiek-ideologische systeem waar deze voor stond. Dergelijke tussenactoren konden overigens uit het hele spectrum van actoren komen, van statelijke actoren via formele oppositie tot aan informele guerrilla's en zelfs huurlingen.

1 De beschreven paradigma's bestonden overigens niet in isolatie; er waren in de genoemde tijdvakken ook conflicten vanuit andere paradigma's.
2 Bijvoorbeeld: United States vs. Confederate States burgeroorlog, Frans-Duitse oorlog, WO I en WO II.
3 Mutually Assured Destruction – de beschikking over nucleair arsenaal bij beide pacten stond ultimo garant voor wederzijdse totale vernietiging mocht één der actoren de ander aanvallen.

Met de val van de muur in 1989 en vervolgens de desintegratie van het Warschau Pact en de USSR leek de toekomst van de wereld er, vanuit Westers perspectief tenminste, positief uit te zien. Het vigerend paradigma werd *'staat vs. non-statelijke actoren'*. Er waren van 1989 tot 2010 mondiaal ruim dertig conflicten tussen staten en non-statelijke actoren. Betrokkenheid bij oorlog was voor Westerse staten hoofdzakelijk niet langer het gevolg van bedreiging van de eigen soevereiniteit, maar een keuze. Daarbij was internationale crisisbeheersing de belangrijkste reden voor ingrijpen, bij voorkeur op basis van een mandaat van de VN-veiligheidsraad. In deze '*wars of choice*' , veelal, maar niet altijd, te classificeren als '*small wars*', namen westerse landen de rol van de steunverlener aan een '*counter-insurgency*', maar ook die van ondersteuner van een '*insurgency*' op zich. Dit afhankelijk van aard en karakter van de actoren in een dergelijk scenario. Uiteraard mogen de 2e en 3e Golfoorlog (respectievelijk 1990/91 en 2003) hier niet onvermeld blijven. Beide gelden als '*wars of choice*', maar zijn wel duidelijke voorbeelden van het paradigma 'staat vs. staat' en hebben enige tijd gegolden als bewijs van de militaire suprematie van het Westen.[4]
In deze conflicten bleek '*hard power*' onmisbaar te zijn, maar zeker niet afdoende. Zowel het militaire machtsmiddel als de andere machtsmiddelen van staten[5] moesten al hun vermogen, inbegrepen aspecten als psychologische operaties en informatie operaties, aanwenden. Aanvullend bleek een '*comprehensive approach*'[6] nodig om de complexe conflicten zo compleet mogelijk aan te pakken. Op politiek-strategisch niveau ontstond echter onachtzaamheid voor ontwikkelingen in opkomende staten[7] en in plotseling zelfstandige staten. In conceptuele zin: de ideeën van de liberale vrede of democratische vrede voerden in deze periode de boventoon ten opzichte van die van het politiek realisme.

Ook nu nog is het paradigma van het vorige tijdvak, 'staat vs. non-statelijke actor', onverminderd van kracht, getuige bijvoorbeeld de huidige crisis rondom ISIS, de inzet in Mali, maar ook de voortgezette bemoeienis in Afghanistan. Daarbij verschijnt afgelopen periode echter nadrukkelijk een ander paradigma, de 'staat vs. staat 2.0'. Waarbij de staat zich niet per se statelijk gedraagt, althans niet volgens de regels van de internationale gemeenschap. Een actueel voorbeeld hiervan is de Russische benadering van Oekraïne,[8] waarvoor al vingeroefeningen zijn gedaan in 2008 tegen Georgië. Ook landen als bijvoorbeeld India, Pakistan en China hebben zich eerder op deze wijze gemanifesteerd. De reaal-politieke Clausewitziaanse stelling dat 'oorlog de voortzetting is van politiek, met inbegrip van andere middelen',[9] waarbij een staat ook de velden van psychologie/moreel en ethiek/moraal bespeelt, is van toepassing in dit paradigma.

4 Hoewel de concrete doelstellingen op diverse niveaus zijn behaald, is dat conflict echter al snel geëvolueerd naar een staat vs. non-staat conflict; een belangrijk oogmerk, het creëren van een stabiele situatie in de regio, is vooralsnog niet gehaald.

5 Machtsmiddelen van staat: DIME – Diplomacy, Information, Military, Economy.

6 Kortweg een 'whole-of-government approach' met daarbij nog Internationale Organisaties en Non-Gouvernementele Organisaties

7 BRICS: Brazil, Russia, India, China, South Africa

8 Bewapening en inzet van lokale groeperingen, inzet van geanonimiseerde Russische strijdkrachten in Oekraïne en intimiderende positionering van regulier militair vermogen aan de grenzen. Dit in combinatie met cyber operaties en vergezeld van een informatie campagne ter ondersteuning– zie voor details de Oekraïne-casus in dit rapport.

9 De originele Duitstalige tekst stelt herhaaldelijk 'mit Einmischung anderer Mitteln'. Dat betekent zeker niet '(voortzetting) met andere middelen'; die formulering zou impliceren dat de tot aan het uitbreken van een oorlog gebruikte middelen die aan de politiek ter beschikking staan (diplomatie, economie,…) niet meer worden ingezet in oorlog. Juist de combinatie van alle machtsmiddelen is de crux in de stelling.

Welke typen van oorlogsvoering kunnen nu worden onderscheiden in het huidige tijdsgewricht? De vakliteratuur beschrijft de verschillende typen veelal in paren: regulier vs. irregulier, conventioneel vs. onconventioneel, symmetrisch vs. asymmetrisch. De tegengestelden verschillen telkens op één of meer van de volgende karakteristieken: actoren, middelen, methoden en doelstellingen. Contemporaine oorlogsvoering, vooral door en tegen non-statelijke actoren, verloopt echter slechts zelden volgens één van die zuivere varianten, maar is juist veelal hybride. Hybride oorlogsvoering utiliseert alle conceptuele categorieën van oorlogsvoering, en zet feitelijk die elementen daarvan in, die plaatselijk en tijdelijk de gewenste effecten bereiken. Deze mix van in te zetten elementen is daarnaast voortdurend aanpasbaar; deze transformerende aard resulteert in voortdurend wisselende karakteristieken. Dit maakt het zeer ingewikkeld om een adequate respons te vinden op hybride oorlogsvoering.

In het paradigma 'staat vs. staat 2.0' kunnen alle 'zuivere' typen oorlogsvoering in beginsel nog voorkomen. Kenmerkend voor de huidige wijze van oorlogsvoering is echter dat de 'staat 2.0' zich enerzijds openlijk ('*overt*') manifesteert als (evt. zelfs onpartijdige) macht met inzet van alle machtsmiddelen van staat. Anderzijds bedient hij zich van andere actoren ('*by proxy*') en maakt daarnaast ook nog heimelijk ('*covert*') gebruik van zijn machtsmiddelen en van relatief nieuwe methoden als cyber operaties en krachtige informatie operaties ter ondersteuning van de (ontkenbaarheid van) '*covert*' aspecten en rechtvaardiging van de '*overt*' aspecten. Dit is tot op zekere hoogte niet nieuw. Uit de geschiedenis zijn heimelijke acties van strijders, opruiende agenten in den vreemde en dubbele agenda's van staten allemaal al ruimschoots bekend. De nu toegepaste moderne middelen en methoden in combinatie met de verregaande verwevenheid van belangen door mondiale vergroeiing van economieën maken deze benadering echter effectiever en mogelijk destructiever.
Een 'staat 2.0' kan in een dergelijk ambigu optreden, anders dan een non-statelijke actor, het gehele brede palet aan machtsmiddeleninzetten, deels ook *covert*. De nieuwe Russische overkoepelende doctrine voor de krijgsmacht[10] stelt bijvoorbeeld dat oorlog met inzet van alle beschikbare middelen in alle denkbare combinaties en uitvoeringswijzen (inbegrepen '*covert*' acties) de basis is. De '*covert*' aspecten, inclusief de ingebouwde ontkenbaarheid[11] daarvan, in samenhang met de '*overt*' manifestatie als onpartijdig, of zelfs als bovenpartijdige vredesbrenger, maken het optreden ambigu. Zo beschouwd is hybride oorlogsvoering voor de 'staat 2.0' een vigerend uitgangspunt en de combinatie met ambiguïteit een zeer valide mogelijkheid. Gegeven de waarneming dat deze wijze van oorlogsvoering genesteld is in het hernieuwde paradigma 'staat vs. staat 2.0' kunnen we stellen dat ambigue oorlogsvoering een actuele alsmede een blijvende dreiging vormt.

Ambiguiteit in oorlogsvoering is bijna zo oud als oorlog zelf, maar is recent sterk in de aandacht gekomen door de aanwezigheid van Russische militairen op de Krim (in de aanloop naar de annexatie daarvan door Rusland) en in andere delen van Oekraïne, waarbij hun aanwezigheid duidelijk zichtbaar was maar zij hun nationaliteit verborgen hielden (zie box Oekraïne).[12] Onderdeel van de ambigue oorlogsvoering van Rusland is naast de inzet van geanonimiseerde Russische strijdkrachten ook het bewapenen en inzetten van lokale groeperingen in Oekraïne. Opvallend is dat het lijkt dat Rusland – als permanent lid van

10 Hoofd Generale Staf, Valeri Gerasimov, wordt gezien als het brein achter deze doctrine.
11 De noodzakelijke ontkenbaarheid van (delen van) het optreden maken Ambigue Oorlogsvoering overigens ook moeilijk 'perfect' uit te voeren.
12 Zie: Nicu Popescu, Hybrid tactics: neither new nor only Russian (ISS Issue Alert). Parijs: European Union Institute for Security Studies, januari 2015.

de VN Veiligheidsraad een zeer invloedrijke staat - zich enerzijds richtte op de formele ontkenbaarheid van zijn militaire inmenging, maar het anderzijds schijnbaar incalculeerde dat het voor alle betrokkenen duidelijk was dat de betreffende anonieme militaire eenheden zeer waarschijnlijk Russisch waren. Een mogelijk gevolg hiervan is dat ambiguïteit in oorlogsvoering in het vervolg vaker op een dergelijke min of meer openlijke wijze door zowel kleine als grote staten zal worden nagestreefd. De zorg bestaat dat de Russische acties in Oekraïne in combinatie met toenemende geopolitieke spanningen andere staten stimuleert om ambigue oorlogsvoering meer dan voorheen toe te passen.

Een toename in ambigue oorlogsvoering kan op meerdere manieren schadelijk zijn voor de Nederlandse nationale veiligheid. Ten eerste ondermijnt het de internationale rechtsorde: ambiguïteit verlaagt de drempel voor staten om door middel van oorlog of militaire middelen hun belangen na te streven. Ten tweede vergroot het de kans dat Nederland in een gewapend conflict betrokken raakt, met name waar het gaat om de veiligheid van NAVO-bondgenoten. Hoewel Nederlands grondgebied niet direct in een potentiële fysieke frontlinie ligt, geldt dat uiteraard wel voor het grondgebied van andere leden van de bondgenootschappen waaraan Nederland zich in zeer sterke mate heeft gecommitteerd, de NAVO en de EU.[13] Daarnaast kan op langere termijn ook de territoriale veiligheid van Nederland zelf worden aangetast. Hoewel het beschermen van de eigen territoriale veiligheid primair de verantwoordelijkheid is van de Nederlandse overheid, kan zij hier alleen in slagen door samen te werken met buitenlandse partners, en gaat het bij de bescherming van het wederzijdse grondgebied daarmee om zogenaamde 'verlengde belangen'. Ten derde zou een toename van ambigue oorlogsvoering ook tot gevolg kunnen hebben dat, ook als Nederland slechts zijdelings (als diplomatieke actor i.p.v. via een bondgenootschap) bij een conflict is betrokken, Nederlandse veiligheidsbelangen in het geding komen, o.a. als het cyberdomein wordt gebruikt om een aanval op Nederlandse vitale infrastructuur uit te voeren of Nederland getroffen wordt door ambigue (niet-afgekondigde en ontkenbare) economische sancties. Dat laatste kan leiden tot schade aan de economische veiligheid of tot politiek-sociale onrust. Daarnaast is het ook mogelijk dat, zelfs als Nederland op geen enkele wijze een betrokken partij is, vitale infrastructuur op internationaal niveau wordt aangevallen waarvan ook wij afhankelijk zijn.

Verwachting voor de komende 5 à 10 jaar

Ambigue oorlogsvoering blijft ook voor de komende 5 à 10 jaar een relevante dreiging voor de Nederlandse nationale veiligheid. Deze dreiging zal, waar het de directe omgeving van de EU betreft, waarschijnlijk vooral vanuit Rusland komen. Het lijkt waarschijnlijk dat Rusland het middel van ambiguïteit opnieuw zal toepassen als de omstandigheden daar gunstig voor zijn, aangezien tot nu toe het vermogen van andere partijen om effectief te reageren op ambigue Russische inmenging in Oekraïne gering is gebleken. Als meerdere grote staten naar aanleiding hiervan dit middel vaker gaan gebruiken kan dit tot een versterking van internationale spanningen leiden. De in de Clingendael Monitor gesignaleerde toename van spanningen tussen grote mogendheden in de komende jaren, als gevolg van verschuivende machtsverhoudingen, is in dit verband zeer relevant. Ook afgezien van het Russische voorbeeld bestaat de mogelijkheid dat grote staten bij toenemende internationale spanningen er

13 De NAVO als politiek-militair bondgenootschap met traditioneel een focus op de kerntaak van (eigen) territoriale verdediging en daarnaast met een aangenomen rol als 'crisis-response' actor. De EU een politiek-economische unie met oorspronkelijk het zwaartepunt gericht op economie (en zo economische veiligheid), maar ook een groeiende rol op fysiek veiligheidsgebied, primair als 'crisis-response' actor.

voor kiezen de kans op militaire escalatie te beperken door ambiguïteit toe te passen in hun militaire optreden of bij hun betrokkenheid bij kleinere conflicten.

Voor ambigue oorlogsvoering geldt dus de verwachting dat dit verschijnsel de komende jaren niet zal afnemen en eerder zal toenemen. Dit temeer omdat de veiligheidsbelangen sterk met elkaar verbonden zijn en sterk afhankelijk van twee voorwaarden die door ambigu optreden worden aangetast: geloofwaardige bondgenootschappen en een goed functionerende internationale rechtsorde. Daarenboven geldt een sterke verwevenheid tussen externe en interne veiligheid, wat een open samenleving als de Nederlandse extra kwetsbaar maakt voor ambigue oorlogsvoering. Zo kunnen aanvallen die niet gericht zijn op Nederland of op zijn bondgenoten, ook al significante gevolgen hebben voor de Nederlandse veiligheidsbelangen. Bij een direct ambigu optreden tegen Nederland of haar bondgenoten zijn de gevolgen nog ernstiger.

De kans op een daadwerkelijke bedreiging van Nederland, zeker indirect (dus via een bondgenoot), is in het nieuwe paradigma van de staat 2.0 die ambigu kan en durft op te treden al duidelijk groter dan voorheen. Of deze kans de komende 5 tot 10 jaar nog verder zal toenemen is voor een belangrijk deel afhankelijk van hoe Nederland, ingebed in de internationale gemeenschap en met name in de NAVO en de EU, zal reageren op de Oekraïne-crisis.

Relevantie van afschrikking als veiligheidsconcept

Meer nog dan bij conventionele bedreigingen dient afschrikking tegen ambigue oorlogsvoering volledig geloofwaardig te zijn. Die geloofwaardigheid zal moeten voortkomen uit drie factoren: bewustzijn, beschikbaarheid en bereidheid. Het *bewustzijn* van de realiteit van ambigue oorlogsvoering is onontbeerlijk op politiek-strategisch niveau; de gedachte dat moderne staten in de 21e eeuw dergelijk optreden niet zullen toepassen is onjuist. Het herkennen en erkennen van het feit dat het paradigma van oorlog is gewijzigd – en dat dít ambigue oorlogsvoering tot een bestaande en blijvende dreiging maakt – is namelijk de basis voor alle denken en handelen in relatie tot die dreiging. Dergelijk bewustzijn uit zich in een krachtige politieke uitstraling van een solidaire en eensgezinde NAVO en EU, een uitstraling die de andere twee factoren ondersteunt.

Beschikbaarheid betreft de aanwezigheid van de capaciteiten die nodig zijn om afschrikking te creëren en waar te maken. Ambigue oorlogsvoering, wanneer daadwerkelijk toegepast, is het best te counteren met ambigue oorlogsvoering. Dit zou echter een bewuste keuze inhouden voor het verlagen van de mate waarin Nederland zich houdt aan internationale normen, waarden en mogelijk zelfs wetten en verdragen. En het belang van die zaken was nu juist (mede) een reden om een ambigu optredende opponent aan te grijpen. Als alternatief mag dan hybride oorlogsvoering gelden. Afschrikking ten opzichte van ambigue oorlogsvoering vereist dus openlijke aanwezigheid van de concepten, methoden, middelen en vaardigheden die benodigd zijn om hybride op te treden. Enerzijds dient het conventionele vermogen op orde te zijn. Aan eigen kant geldt immers eveneens dat het potentiële samenspel tussen elementen uit alle typen oorlogsvoering de kern is van het vermogen tot hybride optreden. Het NATO Readiness Action Plan dat onder andere voorziet in ophoging van het aantal reactietroepen, als ook verkleining van de reactietijden van die troepen is een voorbeeld van een (grootschalig) initiatief dat leidt tot *beschikbaarheid.*

Daarnaast is het van belang om te realiseren dat in het paradigma staat vs. non-statelijke actor al veel kennis en kunde is opgedaan op vele facetten die nuttig en noodzakelijk zijn voor hybride oorlogsvoering (tegen een staat 2.0). De NAVO heeft bijvoorbeeld (ook) functionele doctrine over psychologische operaties en informatie operaties en thematische doctrine over 'counter-insurgency' (COIN). Diverse bondgenoten zetten, net als Nederland, in op ontwikkeling van (counter-)cyber operaties. Dergelijke thematische doctrine kan worden gebruikt bij 'non-Artikel 5' inzet én bij Artikel 5 inzet. Ten slotte zijn ook de overige machtsmiddelen van de staat aanwezig en inzetbaar in het geval van Nederland en zijn bondgenoten. Er is daarnaast, wederom in diverse COIN crisissituaties, ook daadwerkelijk ervaring opgedaan in het gebruik van economische middelen[14] in parallel met diplomatieke, informatieve en militaire machtsmiddelen. Het is essentieel te realiseren dat een '*comprehensive approach*', die als standaard geldt bij het ondersteunen van een partner in een COIN of ander crisisscenario, ook (en wellicht zelfs nog intensiever) zal moeten worden toegepast in een optreden tegen een ambigue opponent.

Bereidheid tot inzet van het beschikbare vermogen is de laatste noodzakelijke component van geloofwaardige afschrikking. Dergelijke bereidheid blijkt al tot op zekere hoogte uit de bovenbeschreven beschikbaarheid van concepten, methoden en middelen. Uiteindelijk is echter slechts daadwerkelijke inzet het ultieme bewijs van bereidheid. Maar hybride optreden om aan te tonen dat het kan, is uiteraard geen verstandige modus operandi. De dichtstbijzijnde variant van inzet is dan openlijke oefening als middel tot afschrikking. In reactie op ambigue oorlogsvoering tegen niet-NAVO (en/of niet-EU) landen –en ter geruststelling van de ongeruste bondgenoten aan de oostzijde van het NAVO territorium- is inmiddels een uitgebreid oefenprogramma ontworpen en deels uitgevoerd. Dit om de boodschap te versterken dat de NAVO echt gewapenderhand zal optreden bij een aanval op haar bondgenootschappelijk grondgebied. De Verenigde Staten hebben publiekelijk verklaard eventueel met conventionele strijdmiddelen te reageren op een cyberaanval die levens kost of serieuze materiële schade berokkent. Maar het is niet (altijd) makkelijk om de schuldige achter een cyberaanval te vinden. Een nog openstaande optie is om geregeld een oefening in hybride oorlogsvoering uit te voeren, waarbij inbegrepen dan ook cyberoperaties en informatie operaties met relatief onschuldige, maar niet eenvoudig realiseerbare resultaten die achteraf openbaar worden gemaakt. Een parallel denken als bij oefeningen met conventionele inzetmiddelen is hier nodig. Zo kan er binnen de eigen normen en waarden worden gebleven, maar wordt wel een beeldtaal gebruikt die vanuit het culturele en machtspolitiek filter van de staat 2.0 luid en duidelijk valt te begrijpen. Bij voorkeur zijn dergelijke activiteiten gepositioneerd in de partnerlanden aan de buitengrenzen van de EU en/of NAVO, hetgeen de signaalwerking nog versterkt. Voor bovenbeschreven oefeningen geldt al wat zeker voor echte inzet geldt: politieke (morele) moed is geboden, een overkoepelende strategie die ruimte biedt aan inzet van alle machtsmiddelen van de staat en aan alle benodigde elementen -en de doctrines daarover- uit alle typen van oorlogsvoering is onontbeerlijk, ethische en juridische afwegingen dienen duidelijk te zijn voordat inzet daadwerkelijk nodig is.

De kosten/baten-afweging bij staten die ambigue oorlogsvoering overwegen kan op meerdere manieren worden beïnvloed. Aan de kostenkant kan dit op directe wijze worden gedaan door de dreiging van vergelding krachtiger en geloofwaardiger te maken. Afschrikking door vergelding is echter lastig vanwege het attributieprobleem. Het is immers

14 Zowel financiële steun aan partners als het financieel blokkeren van opponenten.

inherent aan ambigue oorlogsvoering dat acties die hieronder vallen mogelijk niet direct herleid kunnen worden tot een bepaalde dader. In het geval dat er ernstige verdenkingen bestaan, of eigenlijk al vaststaat om welke dader het gaat, zonder dat dit direct is aan te tonen, kan er worden overgegaan op impliciete (niet als zodanig aangekondigde) economische of diplomatieke vergeldingsmaatregelen. Bij het toepassen van dergelijke tegenmaatregelen is het probleem dat daardoor wordt bijgedragen aan het ondermijnen van de internationale rechtsorde. Wanneer voldoende duidelijk kan worden aangetoond wie verantwoordelijk is voor bepaalde ambigue acties wordt de mogelijkheid van vergelding door juridische of politiek-militaire tegenacties aanzienlijk groter.

Concluderend kan gesteld worden dat het indirect verhogen van de kosten-inschatting door mogelijke daders mogelijk is door het investeren in internationale normen die het risico op reputatieschade bij ambigu oorlogvoeren vergroten. Als deze vorm van oorlogsvoering internationaal niet alleen als illegaal maar ook als moreel zeer verwerpelijk wordt gezien kan zelfs de verdenking dat een staat van dit middel gebruik maakt al tot grote imagoschade leiden. Dit zou – afhankelijk van de actuele situatie – de drempel om in een gewapend conflict tot ambigu handelen over te gaan kunnen verhogen. Daarnaast kunnen de kosten van ambigue oorlogsvoering mogelijk ook worden verhoogd door investeringen in een betere informatie- of inlichtingenpositie en een krachtige communicatiestrategie via internationale media en diplomatieke kanalen. Hoe groter de kans op ontmaskering van de dader, hoe meer deze wellicht zal moeten doen om het vermogen tot ontkenbaarheid bij ambigu optreden te kunnen handhaven. Specifiek voor de dreiging van ambigue oorlogsvoering door Rusland tegen NAVO-lidstaten geldt dat investeringen door NAVO-landen in militaire middelen en samenwerking relevant is, mits in combinatie met een geloofwaardige kans op ontmaskering en vergelding, omdat dit leidt tot een vergroting van noodzakelijke voorinvesteringen aan Russische zijde.

Ook aan de batenzijde zijn investeringen die de kans op ontmaskering vergroten relevant. Dit betekent immers dat er voor de ambigu optredende staat een groter risico is dat de poging faalt en het ontkennen van de betrokkenheid geen zin meer heeft. Het is echter bijna onmogelijk om de gelegenheid van een ambigue aanval volledig weg te nemen, hiervoor zal de kans op ontmaskering 100% moeten zijn. In aanvulling hierop kunnen maatregelen worden genomen om het achterliggende doel bij de aanvaller van het creëren van verwarring en onzekerheid weg te nemen, bijvoorbeeld door goed voorbereid te zijn op mogelijke ambigue oorlogshandelingen op internationaal niveau die voor Nederland relevant zijn. Voor maatregelen aan zowel de kosten- als de batenzijde geldt dat Nederland hierin aanzienlijk effectiever kan optreden door hierin samen te werken met andere landen en met internationale organisaties.