Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Χίμαιρα

Een duiding van het fenomeen ‘hybride dreiging’

Leeswijzer

Deze fenomeenstudie is geschreven in het najaar van 2016 en werd in de eerste helft van 2017 als 'departementaal vertrouwelijk' gerubriceerd uitgebracht voor gebruik binnen de Rijksoverheid. Gezien de aanhoudende actualiteit van de thematiek en de behoefte van partijen buiten de Rijksoverheid aan duiding van het fenomeen, is besloten dit rapport volledig te derubriceren zodat exploitatie buiten de Rijksoverheid mogelijk is, echter zonder uitgebreide herziening of update. De gebruikte voorbeelden stammen daarom hoofdzakelijk uit het tijdvak van eerdere gerubriceerde publicatie.

Bij het opstellen van deze analyse is gebruik gemaakt van producten van onder meer wetenschappelijke instellingen, denktanks, buitenlandse overheden, EU, NAVO, AIVD, MIVD en het Analistennetwerk Nationale Veiligheid. De in deze publicatie gehanteerde definitie en begrippenkader worden onderschreven door AIVD en MIVD.

"Te vechten en te overwinnen in al onze oorlogen is niet opperste uitmuntendheid; opperste uitmuntendheid is juist het breken van de weerstand van de vijand zonder te vechten."

Sun Tsu

Inhoudsopgave

Management samenvatting

Hoewel de term 'hybride dreiging' relatief nieuw is, is wat ermee wordt bedoeld niet nieuw. Het concept op zich maakt sinds jaar en dag deel uit van interstatelijke verhoudingen. Het gaat in wezen om dreigingen, die in verschillende gedaantes verschijnen en op meerdere nationale veiligheidsbelangen tegelijkertijd impact (kunnen) hebben, en daarmee 'een dreiging voor de nationale veiligheid' vormen. Het woord 'hybride' verwijst naar de gebruikte mix van middelen, het asymmetrische karakter van een dreiging, de veelvormige manifestatie en de meervoudige impact van de dreiging. Aangezien de integraliteit en complexiteit van dreigingen aan de basis ligt van het nationale veiligheidsdenken voegt de term 'hybride' in dit opzicht niets toe. Om recht te doen aan de aard en origine van de dreiging is het beter om te spreken van "een dreiging voor de nationale veiligheid door …" bijvoorbeeld "hybride conflictvoering" of "terrorisme" dan van "hybride dreigingen" zonder verdere nadere duiding.

In dit document wordt uitgegaan van de dreiging voor de nationale veiligheid door hybride conflictvoering, met de bijbehorende definitie dat het gaat om: *een conflictvoering tussen staten, grotendeels onder het juridisch niveau van openlijk gewapend conflict, met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken*.
Deze vorm van conflictvoering wordt gekenmerkt door:

1. De geïntegreerde inzet van meerdere militaire en niet-militaire middelen, zoals diplomatieke, economische en digitale middelen, desinformatie, beïnvloeding, militaire intimidatie et cetera, die behoren tot het instrumentarium van staten.
2. Georkestreerd als onderdeel van een strategie/campagne.
3. Met als oogmerk het bereiken van bepaalde strategische doelstellingen.
4. Een belangrijk kenmerk is de misleiding, ambiguïteit en ontkenning waarmee de acties gepaard (kunnen) gaan waardoor attributie en effectieve respons worden bemoeilijkt.

De aard van conflictvoering is geëvolueerd. Deze evolutie zit hem vooral in de nieuwe technologische mogelijkheden waardoor nieuwe dimensies als strijdvelden zijn toegevoegd. Bovendien is de activiteit van actoren merkbaar toegenomen en zien we toegenomen behendigheid van actoren om in hun instrumentarium te switchen. Ook is de schaal waarop deze geïntegreerde strategie wordt ingezet nieuw, en het succes dat daarmee geboekt is aan de randen van Europa.

De definitie ziet op statelijke actoren, omdat het hoogst onwaarschijnlijk is dat niet-statelijke actoren aan de vereiste elementen van hybride conflictvoering voldoen (zoals het hebben van strategische doelstellingen of het ter beschikking hebben van voldoende statelijke instrumenten om een geïntegreerde inzet mogelijk te maken). Zij komen dus niet in aanmerking om te worden gedefinieerd als initiator van hybride conflict, maar vallen als instrument (proxy) wel binnen de scope van de definitie van hybride conflictvoering.

Aan de hand van voorbeelden van de activiteiten zijn manifestaties van de verschillende middelen van hybride conflictvoering geschetst en is inzichtelijk gemaakt of en hoe ze de nationale veiligheidsbelangen kunnen raken. De manifestaties die zijn behandeld zijn: militair; diplomatiek en internationaal-politiek; economisch; digitaal; buitenlandse inmenging (incl. politieke beïnvloeding); en propaganda en desinformatie. Vooral de manifestaties in het cyber- en informatiedomein hebben een vlucht genomen doordat de moderne samenleving sterk gedigitaliseerd en genetwerkt is. Alle manifestaties hebben de potentie om meerdere nationale veiligheidsbelangen te raken.

De verdediging tegen hybride conflictvoering kent een specifieke en generieke benadering. Specifiek is het kennen van de tegenstander: zijn strategische doelstellingen en ambities; zijn sterke en zwakke punten; en "connecting the dots". Generiek is: het kennen van de eigen kwetsbaarheden; het handelen gericht op het inperken van *mogelijkheden* van vreemde mogendheden; het handelen gericht op het reduceren van de impact; en het handelen gericht op het wegnemen van de ontvankelijkheid voor informatieoperaties.

Χίμαιρα (Chimaera) ofwel hybride[1]

Aanleiding

De actualiteit in internationale ontwikkelingen, waarbij bepaalde statelijke actoren steeds agressiever worden in de geïntegreerde inzet van hun instrumentarium, heeft aanleiding gegeven tot nadere bestudering van het fenomeen 'hybride dreigingen' ten behoeve van standpuntbepaling van de Nederlandse overheid hierin. Het doel was om te komen tot een analyse over het fenomeen, waarbij wordt ingegaan op:

- de definitiekwestie;
- incl. mogelijke actoren (statelijke/niet-statelijke);
- hoe dit fenomeen de nationale veiligheid kan raken;
- voorbeelden worden gegeven, waar mogelijk, van actuele manifestaties.

1 De Chimaera is een figuur uit de Griekse mythologie. Het is een monsterlijk wezen, samengesteld uit delen van meerdere beesten. Het woord wordt tegenwoordig ook wel gebruikt om het 'concept' van een chimaera aan te duiden. Dat wil zeggen, het idee van één wezen dat opgemaakt is uit verschillende andere (ons bekende) wezens. Een andere term voor zulke wezens is een "hybride".

De definitie

Het *buzz word* van het moment is "hybride". Hybride betekent: nauwe vermenging/ combinatie of kruising van ongelijksoortige zaken. En deze vermenging of kruising vindt in veel domeinen plaats: in de biologie (zowel in diersoorten als bij gewassen), in de technologie, in sport et cetera.

Niet een hybride dreiging, maar een dreiging voor de nationale veiligheid.

Ook in het veiligheidsdomein steekt de term 'hybride' steeds vaker de kop op. Zo wordt er gesproken over 'hybride dreigingen' waaronder dan een veelheid aan gebeurtenissen of fenomenen met veiligheidsimplicaties wordt geschaard. Al naar gelang de gebruiker zijn dat migratie, piraterij, terrorisme, etnische conflicten, Brexit etc. De term "hybride dreiging" is daarmee een moeilijk hanteerbaar containerbegrip geworden en vervuilt en verwart een zinvolle inhoudelijke discussie. Wat voegt de term "hybride dreiging" nu toe?

Het gaat in wezen om dreigingen, die in verschillende gedaantes verschijnen en op meerdere nationale veiligheidsbelangen impact (kunnen) hebben, en daarmee 'een dreiging voor de nationale veiligheid' kunnen worden genoemd. Het woord 'hybride' verwijst naar de gebruikte mix van middelen, het asymmetrische karakter van een dreiging, de veelvormige manifestatie en de meervoudige impact (dus op meerdere NV-belangen) van de dreiging. In plaats van te spreken van een hybride dreiging, is het beter te spreken van een dreiging voor de nationale veiligheid. In het nationale veiligheidsdenken staat integraliteit en complexiteit van dreigingen al centraal. De term "*hybride* dreiging" voegt dus eigenlijk niet iets nieuws toe, houdt echter wel een risico op verwarring in. Gebruikt als containerbegrip is de ene 'hybride dreiging' namelijk totaal anders dan de andere 'hybride dreiging'. Om helder te krijgen en houden waar het over gaat is het beter terug te redeneren naar de generator van de dreiging en de dreiging dienovereenkomstig te benoemen. In het ene geval zal het gaan om een systeemdreiging (in casu Brexit), in het andere geval gaat het om een terroristische dreiging.

Is hybride oorlogvoering dan een betere term?

Iets concreter dan de term 'hybride dreiging' is de term 'hybride oorlogvoering'. Conventionele oorlogvoering is een openlijk inter- of intrastatelijk conflict, primair maar niet uitsluitend gevoerd met militaire middelen. Bij hybride oorlogvoering is er sprake van de vervaging van de grens tussen oorlog en vrede; het slagveld is geen duidelijk afgebakend gebied meer. Het betreft veelal een geïntegreerd gebruik van conventionele en non-conventionele middelen, openlijke en heimelijke activiteiten en de inzet van militaire, paramilitaire en civiele actoren en middelen om ambiguïteit te creëren en kwetsbaarheden van de tegenstander te raken om geopolitieke en strategische doelstellingen te bereiken. Er wordt op een geïntegreerde wijze gebruik gemaakt van een spectrum aan middelen: op politiek, economisch, militair, informatiegebied. Beïnvloeding en misleiding door gemanipuleerde informatievoorziening maken een belangrijk deel uit van hybride tactieken. Hybride oorlogvoering zal zich (voor een groot deel) afspelen onder de juridische drempel[2] van gewapend conflict. Hoewel deze benadering door een militaire bril naar het gebruik van civiele middelen kijkt, betekent dit niet dat een benadering vanuit het civiele domein een ander inzicht oplevert. Beide perspectieven bieden uitzicht op conflictvoering of agressie met het hele spectrum dat binnen het statelijk instrumentarium beschikbaar is. Dezelfde semantische discussie speelt internationaal, waar de term 'hybrid warfare' is ingeruild voor de term 'hybrid threats' om de dreiging associatief uit het puur-militaire domein te halen.[3]

Er zijn enkele interessante juridische noties m.b.t. tegenstanders die zich bedienen van de methode van hybride oorlogvoering, die niet terug te vinden zijn in de diverse definities maar die duidelijk illustreren wat de juridische drijfveren en mogelijkheden zijn voor deze actoren.[4] Het gaat er bijvoorbeeld om dat ze gebruik maken van de complexiteit van internationale wet- en regelgeving omtrent conflicten; dat de juridische interpretatieruimte die bij internationale regels bestaat wordt uitgebuit; dat juist expres wordt geopereerd in onder-gereguleerde gebieden, zoals het digitale domein of juist onder de juridische drempels van conflict. Dat wil zeggen dat bewust wordt geopereerd op een wijze die onder de drempel valt van wat in het algemeen onder internationaal recht als 'gewapend conflict' wordt gekwalificeerd.

2 Dat wil zeggen: onder de drempel van wat in het algemeen onder internationaal recht als 'gewapend conflict' wordt gekwalificeerd.

3 In deze internationale discussie wordt ook het gevaar onderkend dat een te brede definitie een containerbegrip zonder betekenis is en een te enge definitie slechts een synoniem is voor de Russische interventie in Oekraïne.

4 Aurel Sari, "Hybrid Warfare, Law and the Fulda Gap", in *Complex Battlespaces. The Law of Armed Conflict and the Dynamics of Modern Warfare*, maart 2017 en "Blurred Lines: Hybrid Threats and the Politics of International Law", *Strategic Analysis January 2018*, The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Er is geen unieke definitie, maar de meeste[5] komen erg met elkaar overeen en bevatten de volgende elementen:

1. De geïntegreerde inzet van meerdere militaire (conventioneel en onconventioneel ingezet) en niet-militaire middelen, zoals:
   - Militair conventioneel: bijv. samentrekken van troepen aan de grens bijv. onder mom van alarmeringsoefeningen, militaire intimidatie
   - Militair onconventioneel: bijv. niet-identificeerbare troepen (w.o. special forces), private militaire bedrijven, 'vrijwilligers' en proxies
   - Diplomatiek: bijv. beïnvloeden van internationale structuren door verdragen te sluiten/eruit terug trekken of besluitvorming in internationale gremia te traineren/blokkeren.
   - Economisch: bijvoorbeeld het genereren van economische druk, incl. het afsluiten van toegang tot markten/energievoorziening of het lastigvallen van commerciële activiteit (incl. met militaire middelen)
   - Cyber (spionage, beïnvloeding, aanvallen, sabotage)
   - Propaganda/desinformatie
   - Beïnvloeding/manipulatie/ondermijning (in inlichtingenmatige zin)

Deze voorbeelden zijn uiteraard niet uitputtend. Een dergelijke volledige gereedschapskist staat eigenlijk alleen in zijn geheel aan statelijke actoren ter beschikking.[6] Niet-statelijke actoren kunnen wel een of enkele middelen inzetten, maar nooit allemaal, waarmee de diversiteit van hun aanvalsmiddelen dus beperkt is. De *diversiteit* van in te zetten middelen is een vereiste om te kunnen spreken van *hybride* conflictvoering, vanwege de gevarieerde mix die wordt verondersteld.

2. Oogmerk is het bereiken van bepaalde (specifieke) strategische doelstellingen.[7] Bijvoorbeeld het voorkomen dat Oekraïne zich aansluit bij NAVO en EU.
3. Georkestreerde inzet als onderdeel van strategie/campagne.
4. Een belangrijk kenmerk van hybride oorlogvoering is misleiding, de ambiguïteit en ontkenning waarmee de acties gepaard gaan waardoor attributie en een effectieve respons wordt bemoeilijkt.

5 Zoals naar voren komen in bijvoorbeeld: Understanding hybrid threats, EPRS At a Glance, juni 2015; https://www.hybridcoe.fi/hybrid-threats/; https://www.nato.int/cps/en/natohq/topics_156338.htm; Munich Security Report 2015; US Joint Irregular Warfare Center, Irregular Adversaries and Hybrid threats: an assessment 2011; Army Doctrine Publication (ADP) 3-0: Unified Land Operations (HQ, Department of the Army, Oct. 2011); Frank Hoffman, Conflict in the 21st century: the rise of hybrid wars, Potomac Institute for Policy Studies, december 2007. De laatst twee zien vooral op de mengvormen van actoren (statelijk/niet-statelijk) en militaire capaciteiten en op de aard van het conflict/mix van tactics. Het Munich Security Report en de studie van het US Joint Irregular Warfare Center zijn juist meer gericht op de mix van gebruikte instrumenten (power instruments) en komen daarmee overeen met de NAVO-definitie. Deze definities komen uit het militaire domein en kijken vanuit dit domein naar het gebruik van civiele middelen, maar het perspectief is ook andersom te bekijken en gebruiken: vanuit het civiele domein.

6 Zie ook de definitie in MIVD Jaarverslag 2016 p.24, waar dit onderscheid ook wordt gemaakt.

7 De MIVD onderscheid het gebruik van hybride oorlogvoering als *doel* en als *middel*. Is er sprake van inzet als *doel* dan zal deze vooral gericht zijn op het beïnvloeden van democratische besluitvormingsprocessen. Is er sprake van inzet als *middel* dan gaat het om een strategische *shaping* operatie om een zo gunstig mogelijke politieke, economische, militaire etc uitgangspositie te verwerven in de aanloop naar een conflict.

Hier zijn enkele kanttekeningen bij te plaatsen. Allereerst is het geïntegreerd gebruik van verschillende middelen bij conflicten geen nieuwe trend, maar zo oud als oorlogvoering zelf. Een belangrijke notie is dat het begrip hybride oorlogvoering, zoals dat sinds 2014 wordt gebruikt[8], vooral een Westers construct is, als gevolg van het succes van het Russisch optreden in Oekraïne. Binnen het Westers denken over conflictoplossing wordt ook gebruik gemaakt van een hybride benadering: de Comprehensive Approach, 3D-benadering. Je zou kunnen zeggen dat hybride oorlogvoering de 'comprehensive approach gone bad' is: een kwaadaardige integrale strategie.[9] Wat 'nieuw' is, is dat de dreiging zich sinds 2014 aan onze grenzen heeft gemanifesteerd en dat de frequentie, schaal, agressie en het succes van de manifestaties ons verrast heeft. Een belangrijk 'inhoudelijk' verschil tussen vroeger en nu is gelegen in het feit dat het digitale domein, inclusief de mogelijkheden voor beïnvloedingsoperaties in een genetwerkte wereld, als 'slagveld' is toegevoegd.[10] Informatieoperaties zijn door internet en sociale media veel indringender dan vroeger: sneller, directer de doelgroep bereikend, real-time aan te passen, kortom effectiever. Maar rechtvaardigt deze nieuwe dimensie, die zich overigens overal manifesteert, een nieuwe naam?

Ten tweede wekt de term "oorlogvoering" (onterecht) de indruk dat het slechts een dreiging betreft wanneer sprake is van een oorlogssituatie. Alsof de agressieve, vijandige handelingen van anderen om hun eigen agenda te realiseren ons pas schaden als er een -op oorlog afstevenend- conflict tussen hen en ons speelt. Het zou dan beter zijn te spreken van, bijvoorbeeld, assertief (of agressief) statelijk handelen. Dan is het duidelijk dat de assertiviteit/agressie die schade toebrengt zich afspeelt *onder* de drempel van oorlogvoering. En dat ook staten die tot onze bondgenoten behoren, assertief kunnen handelen, ten koste van onze belangen. De term 'assertief statelijk handelen' werd, in overeenstemming met internationale denktanks/onderzoek, al gebruikt. Onder 'assertief statelijk handelen' vallen alle hierboven genoemde middelen. Bij assertief statelijk handelen hoeft overigens geen sprake te zijn van een conflict: het gaat vooral om een assertieve, soms aan agressie grenzende, manier van belangenbehartiging, waarbij schade aan anderen "*collateral damage*" is. Van een bewuste strategie om schade toe te brengen is niet sprake. Daarmee onderscheidt het zich fundamenteel met wat wordt bedoeld met hybride oorlogvoering/hybride dreiging, waarbij het toebrengen van schade aan anderen wel opzettelijk is.

De term 'assertief statelijk handelen' sluit niet-statelijke actoren uit: Is dat erg?

Voor de dreiging die uitgaat van het handelen van niet-statelijke actoren zijn andere benamingen mogelijk. Bij een meer toegesneden benaming blijft de origine van de dreiging duidelijker, zonder dat dit afbreuk doet aan erkenning van de intenties en capaciteiten en mogelijke impact. Zolang we oog houden voor ontwikkelende intenties en capaciteiten: out of the box denken en gedegen analyses zijn daarbij natuurlijk onontbeerlijk. De afgelopen tijd toont een groeiende dreiging die uitgaat van staten die op geïntegreerde wijze hun gereedschapskist inzetten om strategische doelstellingen te bereiken. Internationaal is er behoefte om allereerst te focussen op statelijke actoren. Daarmee sluit de afbakening 'assertief statelijk handelen' aan op deze behoefte.

8 De term hybride oorlogvoering kwam al eerder in zwang en werd vooral populair door het werk van Frank Hoffman in 2007. In deze context werd vooral het gebruik van conventionele en onconventionele militaire middelen bedoeld.

9 Wanneer de integrale strategie wordt gebruikt om illegale doeleinden te bereiken of om doeleinden te bereiken via illegale middelen.

10 De globalisering en digitalisering van de moderne samenleving die maakt dat de impact van economische en digitale middelen groter is dan vroeger (nieuwe arena's van belang). Daardoor worden deze middelen meer ingezet dan voorheen.

Dergelijke afbakening wordt ook in het Nationaal VeiligheidsProfiel (NVP) gebruikt. In het NVP wordt hybride dreiging specifiek benoemd als fenomeen binnen geopolitieke ontwikkelingen: "Hybride dreiging gaat uit van een conflictvoering *tussen staten*, meestal onder het niveau van gewapend conflict, waarbij op een geïntegreerde wijze gebruik gemaakt wordt van een spectrum aan middelen: op politiek, economisch, sociaal-cultureel, maatschappelijk, militair, informatiegebied. Het oogmerk is het bereiken van bepaalde (specifieke) strategische doelstellingen door, onder andere, het beïnvloeden van besluitvormingsprocessen. Om die te bereiken worden kwetsbaarheden van de tegenstander gebruikt en geraakt. En dit gebeurt door het gebruik van conventionele en non-conventionele middelen, openlijke en heimelijke activiteiten en de inzet van militaire, paramilitaire en civiele actoren en middelen. Beïnvloeding en misleiding door gemanipuleerde informatievoorziening maken een belangrijk deel uit van hybride tactieken Een belangrijk kenmerk van dergelijke conflictvoering is vaak misleiding, de ambiguïteit en ontkenning waarmee de acties gepaard gaan waardoor attributie en respons worden bemoeilijkt. Een toename van deze vorm van conflictvoering is geconstateerd." Ook het HCSS verkiest de term 'hybride *conflict*voering' boven 'hybride *oorlogvoering*'.[11]

Vervolgens rijst de vraag, is dit een nieuw fenomeen?

Het antwoord daarop is: nee, althans niet helemaal. Het gebruik van andere dan conventionele oorlogsmiddelen is zo oud als oorlogvoering zelf. Waar het om gaat is dat de vijand moet worden geraakt, ook als daarvoor het gebruik van met pokken besmette kleding[12], de inzet van proxies[13] of het Paard van Troje nodig is. Het geïntegreerd gebruik van de instrumenten van nationale macht (national power) is niet nieuw. Zelfs het incorporeren van dergelijke ambitie in een strategie is niet nieuw of voorbehouden aan één actor (de Russische Federatie). De Verenigde Staten hebben in hun Army Doctrine 'strategie' gedefiniëerd als "a prudent idea or set of ideas for employing the *instruments of national power* in a synchronized and integrated fashion to achieve theater, national and/or multinational objectives".[14]

Wat vooral anders is, zijn de nieuwe technologische mogelijkheden, de toegenomen behendigheid van actoren om in hun instrumentarium te switchen en de schaal waarop deze geïntegreerde strategie wordt ingezet, en het succes daarmee geboekt aan de randen van Europa. Daarmee is de aard van de conflictvoering geëvolueerd, want de technologische ontwikkelingen voegen nieuwe dimensies toe, en is de activiteit van actoren toegenomen.

De digitalisering en globalisering hebben nieuwe arena's van belang geopend: het maakt dat de impact van bijvoorbeeld economische en digitale middelen groter is dan vroeger. Hierdoor is het gebruik van andere dan militaire middelen toegenomen. Vooral het gebruik van informatie- en beïnvloedingsoperaties heeft een vlucht genomen. Een belangrijk nieuw aspect is de digitalisering en de rol die internet en social media in de moderne samenleving spelen. Dit betekent een katalysator voor heel veel 'traditionele' tactieken: deze kunnen makkelijker, goedkoper, sneller worden ingezet met grotere impact als gevolg en ook nog eens met meer ambiguïteit. Of het nu gaat om spionage, sabotage of propaganda. Al langer wordt onderkend dat

11 *Coming to Grips with Hybrid Warfare*, The Hague Centre for Strategic Studies, 2015, p. 12
12 In de achttiende eeuw als wapen gebruikt door de Britten tegen Indianen in Noord-Amerika en tegen de Amerikaanse revolutionairen. BBC-History-World Wars: Silent Weapon: Smallpox and biological Warfare, 17 februari 2011, www.bbc.co.uk
13 Staten hebben al vaker afscheidingsbewegingen of terroristische groeperingen gesponsord omdat dat hun eigen strategische doelstellingen ten goede kwam.
14 *Army Doctrine Publication (ADP) 3-0: Unified Land Operations*, U.S. Department of Army, October 2011

cyberspionage een toenemend probleem is. Meer recent heeft men oog gekregen voor het gevaar van de inzet van desinformatie via digitale kanalen. Het feit dat internet en social media het mogelijk maken om snel, via verschillende wegen en in verschillende vormen/met verschillende stemmen de gewenste boodschap *direct* bij een doelgroep te krijgen, maakt dat propaganda/desinformatie als conflictmiddel in waarde is toegenomen. Deze waarde wordt versterkt door het feit dat mensen in toenemende mate hun mening vormen op basis van informatie op internet en sociale media, en daarmee vooral hun eigen wereldbeeld bevestigd zien. In het digitale domein geldt dat attributie heel moeilijk is, dat maakt dit domein uitermate geschikt voor heimelijke conflictvoering.

Conclusie: *Met het huidige gebruik van de term 'hybride' lijkt vooral de veelvormigheid die de manifestatie van de dreiging kan aannemen (incl. cyber) te worden bedoeld.*[15] *Het hele idee van nationale veiligheid gaat uit van het integraal benaderen van de dreiging, juist om te voorkomen dat complexe dreigingen worden onderschat en om ook bij eenvoudiger dreigingen de mogelijke meervoudige impact te voorzien. Om recht te doen aan de aard en origine van de dreiging is het beter om te spreken van "een dreiging voor de nationale veiligheid door hybride conflictvoering", "een dreiging voor de nationale veiligheid door assertief statelijk handelen" of "een dreiging voor de nationale veiligheid door terrorisme" dan van "hybride dreigingen" zonder verdere nadere duiding. In dit document zal daarom verder worden uitgegaan van de dreiging voor de nationale veiligheid door hybride conflictvoering, met de bijbehorende definitie dat het gaat om: een conflictvoering tussen staten, grotendeels onder het niveau van openlijk gewapend conflict, met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken. De behoefte aan nadere duiding van het fenomeen 'hybride dreigingen' lijkt bovendien primair ingegeven door de actualiteit in internationale context, waarbij bepaalde statelijke actoren steeds agressiever worden in de geïntegreerde inzet van hun instrumentarium. De definitie zoals boven omschreven sluit daarmee aan op deze behoefte.*

15 Terwijl de militaire specialist zal zeggen dat het bij hybride niet zozeer gaat om de manifestatie (de output) als wel om het geïntegreerd gebruik van middelen (de input).

Mogelijke actoren

Welke statelijke actoren bedienen zich van deze geïntegreerde inzet van middelen en actoren om hun strategische doelstellingen te bereiken?

Er zijn natuurlijk veel staten die hun instrumentarium strategisch inzetten.[16] Niet alle staten doen dat op dezelfde geïntegreerde wijze, maar er zijn er in ieder geval een aantal die opvallen door hun hoge graad van integratie en activiteit, bijvoorbeeld China en de Russische Federatie. De activiteiten van de Russische Federatie springen de afgelopen jaren bijzonder in het oog door hun veelzijdigheid, agressie en hoge frequentie. Over het feit dat Moskou zich bedient van hybride conflictvoering bestaat internationaal weinig discussie, in combinatie met de veelzijdigheid, het duidelijke gebruik van het militaire instrument en de frequentie maakt dat de Russische activiteiten zeer geschikt zijn om als illustratie van manifestaties van hybride conflictvoering te gebruiken. Daar komt bij dat hybride conflictvoering[17] door Moskou tot officiële strategie is verheven.[18] Dikwijls wordt dan verwezen naar de Russische Chef van de Generale Staf generaal Gerasimov en zijn "Gerasimov-doctrine".[19] Het gaat hierbij eigenlijk niet om een doctrine, maar om een bespiegeling op 'de nieuwe generatie van oorlog voeren'. Om deze redenen is ervoor gekozen Russische voorbeelden ter illustratie van mogelijke manifestaties te gebruiken, hoewel er ook andere staten zijn waarvan manifestaties zijn waargenomen. Waar opportuun zijn dergelijke manifestaties danwel staten, die in de behandelde domeinen actief zijn, toegevoegd in hoofdtekst danwel voetnoten.

16 In het laatste AIVD jaarverslag worden in ieder geval China, Rusland, Turkije, Iran en Noord-Korea genoemd als landen die met kwade intenties danwel schadelijke gevolgen voor Nederlandse belangen hun instrumentarium inzetten. *AIVD Jaarverslag 2018*, 2 april 2019

17 In het Russisch worden overigens andere termen gebruikt bijv. non-lineaire oorlogvoering. De term hybride oorlogvoering is door het Westen opgeplakt.

18 Vanwege het feit dat dit voor Moskou een officiële strategie is in combinatie met de Russische activiteiten in alle arena's, is er voor gekozen om Russische voorbeelden te gebruiken ter illustratie: zo wordt goed duidelijk dat er actoren zijn die daadwerkelijk de volle breedte van hun instrumentarium inzetten om hun doelstellingen te behartigen.

19 In de zomer van 2014 muntte Mark Galeotti de term 'Gerasimov-doctrine', die inmiddels een heel eigen leven is gaan leiden en is opgeblazen tot mythische proporties. Zo heeft Galeotti het nooit bedoeld, hij zocht gewoon naar een pakkende titel voor z'n blog. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/

De Russische generaal Gerasimov heeft în februari 2013 zijn ideeën en ambities over conflictvoering geformuleerd, in een Russisch vakblad "Militair-Industriële Koerier". In essentie wees Gerasimov in zijn toespraak en dit artikel op de Westerse manier van oorlog voeren - zoals de Russen dat percipiëren! - en hoe de Russische Federatie zich daartegen zou moeten wapenen. Deze worden aangeduid met de "Gerasimov-doctrine" en de hoofdpunten daaruit zijn:[20]

- Vervaging van de grens tussen vrede en conflict, zeer snelle overgang van de ene naar de andere toestand.
- 21ste eeuwse oorlogvoering/lessen uit de Arabische Lente: een goed functionerende staat kan in zeer korte tijd (maanden/dagen) veranderen in een arena van fel gewapend conflict, slachtoffer worden van buitenlandse interventie en wegzinken in een web van chaos, humanitaire rampen en burgeroorlog. Dit is typisch voor oorlogvoering in de 21ste eeuw. *[Gerasimov framet hiermee de Arabische Lente als gevolg van heimelijke Westerse operaties. Tekenend is de gelijkenis van de omschrijving met de gebeurtenissen in Oekraïne.]*
- De rol van niet-militaire middelen om politieke en strategische doelen te bereiken is toegenomen, vaak zijn ze effectiever dan wapens.
- De focus van gebruikte conflictmethoden is verschoven naar brede inzet van politieke, economische, informationele, humanitaire en andere niet-militaire maatregelen. Deze worden toegepast in combinatie *[of met het oog op het mobiliseren van]* het 'protest potentieel' van de bevolking. *[Interessant juridisch aspect is dat aan een staat zelfbescherming volgens internationaal recht alleen toegestaan is tegen een dreiging van buitenaf, niet tegen een home-grown dreiging.[21]]*
- Het openlijk gebruik van militaire middelen –onder het mom van 'peacekeeping' of crisismanagement- wordt pas in een bepaalde fase ingezet, vooral voor het behalen van het uiteindelijke succes in het conflict *[openlijk gewapend conflict is dus een 'last resort']*
- Nieuwe technologieën bieden nieuwe militaire mogelijkheden op strategisch, tactisch en operationeel niveau. De verschillen tussen deze niveaus en ook tussen offensieve en defensieve operaties verdwijnen. De overwinning op de doelstellingen van de vijand wordt over de hele diepte van diens territorium uitgevoerd. *[niets nieuws onder de militaire zon]*
- Asymmetrische acties zijn gemeengoed geworden, deze maken het mogelijk de voordelen van de vijand in gewapend conflict [zoals een beter/groter leger] teniet te doen. Onder asymmetrische acties worden verstaan: het gebruik van special-operations troepen en het gebruik van interne oppositie om een permanent operatie front door het hele territorium van de vijandige staat te creëren, maar ook informationele acties.[22] *[let op het expliciet gebruik van interne oppositie als middel in conflictvoering. Volgens Gerasimov zijn deze veranderingen terug te vinden in de militaire doctrines van grootmachten en worden ze ook zo ingezet, bijv. door de VS in Irak (in 1991 en 2003)]*
- De 'informatie ruimte' biedt grote asymmetrische mogelijkheden om het strijd-potentieel van de vijand te verkleinen. Noord Afrika is een voorbeeld van het gebruik van technologieën voor het beïnvloeden van staatsstructuren en bevolking met behulp van informatienetwerken. Het is noodzakelijk om activiteiten in de 'informatieruimte' te perfectioneren. *[Het lijkt er op dat Gerasimov hier doelt op de rol van social media bij de opstanden in Noord Afrika. Het informatiedomein wordt echt als strijddomein gezien, net als land, lucht, zee en cyber.]*

20 Mark Galeotti, *The 'Gerasimov Doctrine' and Russian non-Linear War*, https://inmoscowsshadows.wordpress.com/2014/07/06

21 Zoals Dr. Aurel Sari,(University of Exeter Senior Lecturer, Director of Exeter Centre for International Law) nog eens benadrukte in zijn lezing, "legal aspects of hybrid threats" tijdens de ESDC-cursus *EU facing 'hybrid threats' challenges*, 6-8 december 2016

22 Maar ook het gebruik van huurlingen/private militaire bedrijven, bijv. de 'Wagner Group' in Syrie en Afrika. Met informationele acties worden desinformatie en psy-ops bedoeld, waarover verderop meer.

- Het is belangrijk een systeem van gewapende verdediging van staatsbelangen buiten de eigen landsgrenzen te ontwikkelen. Manieren om militairen buiten de eigen landsgrenzen in te zetten zijn 'peacekeeping' en humanitaire hulp.
- Militaire wetenschap en leiding moeten niet negatief tegenover nieuwe ideeën en non-standaard benaderingen staan: hoe sterk de vijand ook is, er zijn altijd manieren om hem te verslaan. Hij zal altijd kwetsbaarheden hebben en dat betekent dat er adequate manieren om hem te bevechten zijn. *[hieruit spreekt pragmatisme en opportunisme en Realpolitik: gebruik wat nodig is om je doel te bereiken]*

Hierbij moeten twee zaken benadrukt worden: allereerst dat, hoewel activiteiten van de Russische Federatie hier als voorbeeld worden gebruikt, dit geenszins de enige actor is die van dergelijke instrumenten gebruikt maakt.[23] En ten tweede, dat de Russische activiteiten in grote mate worden ingegeven vanuit opportunisme en pragmatisme: geschikte gelegenheden worden herkend en gebruikt maar niet zozeer gecreëerd.[24]

Doen ook niet-statelijke actoren aan hybride conflictvoering?

Nee, als initiator (of dader) van hybride conflictvoering komen niet-statelijke actoren in de hier gehanteerde definitie niet in aanmerking. Dat komt doordat zij niet in staat worden geacht om aan *daadwerkelijke* hybride conflictvoering te doen, conform de vereiste elementen uit de definitie. Zo is het hoogst onwaarschijnlijk dat een niet-statelijke actor specifieke strategische buitenlands- en veiligheidsdoelstellingen heeft of dat hij de beschikking heeft over voldoende verschillende statelijke instrumenten om deze doelstellingen via een geïntegreerde inzet te behartigen.[25] Hoewel het optreden van niet-statelijke actoren in media vaak wordt gekenmerkt als hybride oorlogvoering, moet dit optreden worden beschouwd als terrorisme, insurgency, etc.[26] Niet-statelijke actoren worden wel vaak als *instrument* (proxies) gebruikt in hybride conflictvoering.

23 Zo worden de afgelopen jaren in toenemende mate vraagtekens gezet bij Chinese economische activiteiten: werden die vroeger nog veelal als goedaardig beschouwd, nu worden ze gezien als instrumenteel aan bredere Chinese belangen en (in potentie) schadelijk voor nationale veiligheidsbelangen van het Westen. Ook worden China's ambities en handelen steeds vaker geïnterpreteerd als aanval op Westerse waarden of ondermijning van de Westerse eenheid. Zie bijvoorbeeld: "Rethinking security. China and the age of strategic rivalry", *China and the Age of strategic Rivalry. Highlights from an Academic Outreach Workshop*, Canadian Security Intelligence Service (CSIS), mei 2018; en *Authoritarian Advance. Responding to China's Growing Political Influence in Europe*, GPPI en MERICS, februari 2018

24 Het idee dat "de Russen overal achter zitten" is een ernstige overschatting, tegelijkertijd is het goed in ogenschouw te nemen dat het in 'conflict zijn met het Westen' de bril is waardoor de Russische autoriteiten naar de wereld en gebeurtenissen en ontwikkelingen kijken.

25 Om een strategie als 'hybride' te kwalificeren is een mate van diversiteit aan inzetbare middelen vereist waarover niet-statelijke-actoren nauwelijks beschikking hebben. Het is altijd mogelijk dat toekomstige ontwikkelingen niet-statelijke actoren wel binnen bereik van de definitie brengen. We zagen bijvoorbeeld dat de terroristische organisatie ISIS over een breder spectrum aan middelen beschikte dan terroristische organisaties tot dan toe, en ook statelijke aspiraties had.

26 Diverse deskundigen vragen zich af of sommige terroristische organisaties aan hybride oorlogvoering doen dan wel een 'hybride dreiging' vormen. De meningen zijn daarover echter verdeeld. Sommige auteurs die voorstander zijn om ook voor sommige terroristische organisaties de term 'hybride dreiging' te hanteren, zien de karakteristieken van hybride dreiging als volgt: 1) de combinatie van 'conventionele' militaire inzet met guerrilla tactieken; 2) aanpassingsvermogen: aanpassen aan veranderende strijdcondities; 3) het gebruik van terrorisme; 4) propaganda & informatie oorlogvoeringoorlogvoering; 5) criminele activiteiten (als financieringsmiddel); 6) negeren van internationaal recht. Sommige wetenschappelijke onderzoekers en analisten leggen bijvoorbeeld ISIS of Hezbollah, die gedeeltelijk beschikken over een statelijk instrumentarium, langs deze meetlat en komen tot de conclusie dat ook bij dergelijke organisaties van hybride conflictvoering sprake is. Zie bijvoorbeeld Scott Jasper en Scott Moreland in "The Islamic State is a Hybrid Threat: Why does That Matter?" in *Small Wars Journal*, december 2014. De vraag is echter of deze kwalificering juist is: de termen 'hybride dreiging' en hybride oorlogvoering' worden hier teveel opgerekt.

Manifestaties en mogelijke consequenties

In dit deel zal worden ingezoomd op de manifestaties van hybride conflictvoering en hoe die de nationale veiligheid kunnen bedreigen of schaden.

Wat zijn de nationale veiligheidsbelangen (NV-belangen) die kunnen worden geraakt?

In 2007 startte de Nederlandse overheid met een nieuwe aanpak om de nationale veiligheid beter te kunnen beschermen: het kabinet nam de rijksbrede Strategie Nationale Veiligheid aan.[27] Daarin werd vastgesteld dat "de nationale veiligheid is in het geding als de nationale veiligheidsbelangen van onze samenleving en/of staat zodanig worden bedreigd dat sprake is van (potentiële) maatschappelijke ontwrichting".
De Nederlandse overheid heeft zich gecommitteerd aan het beschermen van deze belangen:
Territoriale veiligheid kan op verschillende manieren worden geschaad: wanneer een deel van ons grondgebied lange tijd onbruikbaar of ontoegankelijk is (bijv. door een overstroming); als de internationale positie van ons land wordt aangetast op politiek-bestuurlijk niveau hetzij op economisch gebied (bijv. een internationaal conflict en inmenging van ongewenste partijen in het bedrijfsleven); maar ook door de aantasting van de integriteit van de digitale ruimte[28] en aantasting van integriteit van bondgenotschappelijk grondgebied kunnen dit belang schaden.

27 De Strategie Nationale Veiligheid is het instrument voor risicomanagement van de Rijksoverheid, teneinde de nationale veiligheidsbelangen van de Nederlandse samenleving beter te kunnen beschermen en zodoende te voorkomen dat de Nederlandse maatschappij ontwricht raakt als gevolg van een crisis. Met de Strategie Nationale Veiligheid legt het Rijk verschillende typen rampen en crises langs eenzelfde meetlat om ze met elkaar te kunnen vergelijken en daardoor beter onderbouwde beleidskeuzes mogelijk te maken. Meer informatie: https://www.nctv.nl/organisatie/nationale_veiligheid/strategie_nationale_veiligheid/documenten.aspx

28 Deze integriteit wordt aangetast wanneer de beschikbaarheid, vertrouwelijkheid en integriteit van essentiële informatiesystemen is aangetast, bijvoorbeeld als de basisregistratie personen (BRP) is gecompromitteerd. Maar ook de procesbesturing van vitale infrastructuur geldt als essentiële informatiedienst.

Fysieke veiligheid is in het geding als er sprake is van slachtoffers[29] (boven een bepaald drempelaantal) en gebrek aan primaire levensbehoeften.
Economische veiligheid wordt geschaad wanneer sprake is van aantasting van de vitaliteit van de Nederlandse economie (werkeloosheid, uitvallende sectoren, afnemend vertrouwen) en van financiële/economische schade.
Ecologische veiligheid wordt geschaad wanneer het zelfherstellend vermogen van onze leefomgeving ernstig wordt aangetast.
Sociale en politieke stabiliteit Schade aan dit belang wordt veroorzaakt door verstoringen van het dagelijks leven van de bevolking, de aantasting van democratische instituties[30] en normen en waarden en destabilisatie van het sociaal-maatschappelijk klimaat in onze samenleving. Rampen waarbij bijv. vitale infrastructuur wordt verstoord leiden al snel tot een ernstige verstoring van het dagelijks leven. Voor grote groepen mensen geldt dat zij gedurende een tijd niet normaal kunnen participeren in de samenleving (werk, school, maatschappelijke activiteiten). Maar ook incidenten of ontwikkelingen die leiden tot brede angst en woede in de maatschappij (sociaalpsychologische impact) kunnen schade toebrengen aan de sociale en politieke stabiliteit.
Internationale rechtsorde komt in het geding wanneer de uitgangspunten van de naoorlogse internationale rechtsorde worden aangetast. Denk hierbij aan de normen van staatssoevereiniteit, vreedzame co-existentie en geschillenbeslechting, maar ook de effectiviteit en legitimiteit van multilaterale instituties zoals IMF, VN, NAVO, EU.[31] Voorbeelden van zulke aantasting zijn: het manipuleren van verkiezingen; het ondermijnen van de basisbeginselen van multilaterale instituties en het verlammen van besluitvorming van zulke instituties.

Welke middelen worden dan ingezet? Welke manifestaties zien we? Schade aan welke NV-belangen?

Zoals eerder beschreven gaat het hier om de geïntegreerde inzet van het statelijke instrumentarium, waarbij onder meer de volgende middelen kunnen worden onderscheiden.

1. Militaire manifestaties

Militaire manifestaties zijn te onderscheiden in verschillende categorieën:

A De demonstratieve inzet van conventionele (nucleaire) militaire middelen, zoals het samentrekken van troepen aan de grens bijvoorbeeld onder mom van alarmeringsoefeningen (messaging, intimidatie). De Russische Federatie heeft afgelopen jaren aangetoond dat het op korte termijn voldoende gevechtskracht aan één van zijn grenzen kan ontplooien voor het voeren van een regionaal conflict. Dit zien we zowel langs de Oekraïens-Russische grens als ook langs de grens tussen EU/NAVO en de Russische Federatie.[32]

29 doden, zwaargewonden en chronisch zieken waaronder ook psychische aandoeningen
30 externe beïnvloeding van politieke processen schaadt het functioneren van democratische instituties en daarmee de sociale en politieke stabiliteit.
31 Het belang van internationale rechtsorde ziet ook op het internationaal financieel-economisch bestel en de werking, legitimiteit en naleving van internationale verdragen voor rechten van de mens.
32 zoals de overplaatsing van een raketsysteem naar de Russische exclave Kaliningrad. De overgeplaatste raketten kunnen worden uitgerust met atoomkoppen en hebben een bereik van meer dan vijfhonderd kilometer. Ze kunnen daardoor de hoofdsteden bereiken van Polen, Litouwen en Letland. Dit zorgt in deze landen voor ongerustheid, "Rusland plaatst raketten aan Poolse grens", *Het Parool, Nederlands dagblad*, 11 oktober 2016. Een Estse defensiedeskundige beweert zelfs dat er in het Westers wapenarsenaal geen vergelijkbaar wapen aanwezig is. Overigens houdt de NAVO ook oefeningen langs de grens met de Russische Federatie, "NAVO tart Rusland met grootste oefening ooit in Oost-Europa", NOS.nl, 6 juni 2016

Dergelijk militair machtsvertoon wordt ook wel *strategic messaging* genoemd.[33] Een goed voorbeeld hiervan is de inzet van (strategische) bommenwerpers en jachtvliegtuigen langs de grenzen van en in de verantwoordelijkheidsgebieden van NAVO-bondgenoten, waarbij vaak zonder transponders wordt gevlogen.[34] Het doel van deze activiteiten is het afgeven van een strategische boodschap: het tentoonspreiden van militaire vermogens zodat dit afschrikwekkend en intimiderend werkt (regional deterrence).

B Ook militaire interventies onder het mom van peacekeeping of humanitaire hulp worden gebruikt. De militaire interventie in Syrië, op verzoek van Assad en zodoende conform internationaal recht, heeft met succes de Westerse inspanningen gedwarsboomd. De situatie in Syrië is volatieler geworden, de vluchtelingenstroom richting de EU (en daarmee de druk op Europese solidariteit) heviger. De onconventionele inzet van militaire middelen, zoals onidentificeerbare troepen, special forces, private militaire bedrijven, 'vrijwilligers'. Dit hebben we natuurlijk gezien in Oekraïne met desastreuze gevolgen voor dat land: een (bevroren) burgeroorlog.

Dat ook andere statelijke actoren via dergelijke militaire manifestaties, onder drempel van gewapend conflict, gebruiken om boodschappen af te geven blijkt uit de militaire activiteiten van China in de Zuid-Chinese Zee. [35] Hier ligt een omstreden gebied: diverse landen maken aanspraak op wateren en eilanden.[36]

Mogelijke consequenties

Dit soort militaire manifestaties kunnen druk zetten op het belang van de internationale rechtsorde, omdat ze bijvoorbeeld de basisbeginselen van het internationale regime ondermijnen, danwel leiden tot verlamming van de besluitvorming binnen multilaterale instituties.

De huidige activiteit van *strategic messaging* is risicovol:

- Allereerst hebben de activiteiten verslechterende internationale verhoudingen tot gevolg, met het risico op escalatie en misverstanden/misinterpretatie van de activiteiten die kunnen leiden tot een gewapende respons. Bijvoorbeeld wanneer art. 5 van de NAVO wordt ingeroepen en dit leidt een open militair conflict.
- Het risico voor de burgerluchtvaart door het niet-voeren van transponders door militaire vliegtuigen bij *strategic messaging*-acties.[37] Het voeren van transponders voor militaire vliegtuigen is weliswaar geen verplichting maar kan leiden tot risico's voor de burgerluchtvaart, zeker in relatief 'kleine' luchtruimen als in de Baltische Zee regio. Het Nederlandse luchtruim is ook klein, maar hier is veel minder militair luchtverkeer dan in de Baltische zee-regio.

33 Strategic Messaging is het uiten van extreme onvrede over veiligheidsontwikkelingen door het opzichtig optreden met conventionele en nucleaire militaire middel, *MIVD Jaarverslag 2016*, 24 april 2017. Voorbeelden zijn: het rondvaren met vloten door Noordzee, Sub's in het Kattegat en Noordzee, militaire vliegtuigen die zonder vluchtplan & transponder luchtruim EU/NAVO invliegen (daarbij gevaar voor burgerluchtvaart veroorzaken) en oefeningen gericht tegen NAVO. Zweden is een ideaal target: want wel EU-lid, maar geen NAVO-lid, dus geen risico op art. 5.

34 Bijvoorbeeld schending van het Finse luchtruim op 7 oktober 2016.

35 Zie bijvoorbeeld "Militaire oefening China zet conflict Zuid-Chinese Zee op scherp", *Trouw*, 5 juli 2016 en "Filipijnen roepen op tot 'zelfbeheersing en nuchterheid in de Zuid-Chinese Zee", *Het Financieele Dagblad*, 13 juli 2016. Een week voordat het internationaal arbitragehof in Den Haag uitspraak deed over de Chinese acties in het gebied hield China daar militaire oefeningen. Daarmee werd het signaal afgegeven dat ze zich niets aantrekken van een eventuele nadelige uitspraak.

36 Naast China maken ook Vietnam, Taiwan, Filippijnen, Brunei en Maleisië zowel territoriale aanspraak (op de Paracel- en Spratly-eilanden) maar ook maritieme aanspraak (op de zee en de zeebodem) . Dit heeft alles te maken met economische belangen van handelsroutes, visserij en olie- en gasreserves. Maar ook met geopolitieke verhoudingen, militaire expansie en het internationale recht op vrije doorvaart.

37 In november 2014 werd hiervoor gewaarschuwd door de NAVO en door minister van Buitenlandse Zaken Koenders, omdat het aantal luchtruimschendingen dat jaar verdrievoudigd was ten opzichte van 2013. De piloten hielden daarbij geen contact met de Europese luchtverkeersleiding, dienden geen vluchtplan in en zetten hun transponders uit waardoor passagiersvliegtuigen hen niet zien aankomen. "Koenders waarschuwt voor Russische luchtmacht", *Trouw*, 24 november 2014. In 2014 meldden diverse media uitwijkacties van burgerluchtvaartvliegtuigen voor Russische toestellen.

- De *strategic messaging* activiteiten met nucleair materieel verhogen het risico op een nucleair incident met langduriger gevolgen voor de fysieke en ecologische veiligheid ter plaatse.

De militaire interventie in Syrië zet druk op Westerse bondgenootschappen (NAVO en EU) omdat deze secundaire gevolgen heeft (vluchtelingenstroom) die op die bondgenootschappen neerslaan. Incidenten als gevolg van drukte in het Syrisch strijdtheater kunnen leiden tot escalatie. Zoals bij het neerhalen van een Russisch toestel door de Turkse luchtmacht wegens luchtruimschending in november 2015. Turkije is lid van de NAVO en de actie zorgde voor grote nervositeit binnen de NAVO over mogelijke escalatie met Moskou. Onwillekeurig dringt zich de vraag op: welke schending en welke NAVO-bondgenoot is het inroepen van art. 5 waard? Discussie en twijfel hierover ondermijnt de solidariteit van het bondgenootschap en dat is precies een van de strategische doelstellingen van het Kremlin. Daarnaast werden door de interventie de Westerse inspanningen in het vredesproces onderuit gehaald.

Met de onconventionele inzet van militaire middelen in Oekraïne heeft Moskou een strategisch doel behaald: Oekraïne is zwak en verdeeld en zal niet toetreden tot de EU en NAVO zolang dit conflict daar heerst.[38] Daarmee zou deze inzet impact hebben op de onafhankelijkheid en het beleid van een voor Nederland belangrijk bondgenootschap. Een verzwakking van bondgenootschappen waarvan Nederland deel uit maakt is slecht voor de Nederlands internationale positie en de Nederlandse belangenbehartiging in de internationale arena.

2. Diplomatieke en internationaal-politieke manifestaties

Hierbij moet worden gedacht aan het opzeggen/opschorten van verdragen.[39] Maar ook het spelen van hindermacht in internationale gremia (bijv. de VN Veiligheidsraad) met pogingen om besluitvorming te blokkeren of traineren, liefst in samenwerking met andere gelijkgestemden in anti-Westerse sentimenten.[40] Met het vormen van alternatieve/concurrerende allianties op bestaande Westers gedomineerde structuren kan worden geprobeerd om een nieuwe arena met andere spelregels te creëren, waarin Moskou wel de dominantie heeft. Er zijn meer statelijke actoren die graag zien dat de Westers gedomineerde spelregels wat worden gemarginaliseerd, bijvoorbeeld China.

Mogelijke consequenties

Dit heeft mogelijk gevolgen voor de geopolitieke verhoudingen. Bij aanhoudende polarisatie, is het mogelijk dat Putin verder gaat met het zoeken naar bondgenoten 'tegen het westen/de VS/NAVO/EU'. Nederland zal, als onderdeel van verschillende internationale organisaties (bijv. VN, Raad van Europa), daar eventuele gevolgen van voelen. Zoals bijv. het blokkeren of dwarszitten van besluitvorming in gremia waar ook de Russische Federatie lid is. Maar ook consequenties voor Westerse bondgenootschappen die doorwerken naar Nederland, bijv. het stationeren van extra troepen in oostelijk gebied van NAVO/EU waaraan Nederland als bondgenoot moet bijdragen.
Gevolgen voor de verhouding Nederland – Rusland zullen merkbaar zijn in het langer opschorten van samenwerking op tal van terreinen, waaronder een aantal overeenkomsten dat voor Nederland van belang is.

38 Indien toetreding van Oekraïne een doelstelling van het Westen/de NAVO was, is deze daarmee gefrustreerd. Het is niet gezegd dat toetreding inderdaad een doelstelling was!
39 zoals de opschorting van de Plutonium Management and Disposition Agreement op 3 oktober 2016
40 Uit gebrek aan geopolitiek overwicht kan Rusland niet veel meer dan Westerse politieke inspanningen saboteren.

3. Economische manifestaties

Rusland beschikt over een breed palet aan economische instrumenten[41], waarvan het mogelijk effect overigens per land verschilt. Het doel is het genereren van economische druk op het slachtoffer. In Westerse democratieën hebben economische gevolgen voor burgers eerder effect op het beleid van overheden dan in de Russische Federatie het geval is. Onder economische instrumenten wordt onder meer verstaan:

- Het beperken van toegang tot markten/handelsroutes/grondstoffen/energievoorziening;
- Het lastigvallen van commerciële activiteit (incl. met militaire middelen)
- Het doen van buitenlandse overnames/investeringen, met het oog op het beïnvloeden/manipuleren van de continuïteit van vitale sectoren; de integriteit en exclusiviteit van informatie; het functioneren van de democratische rechtsorde.
- Het creëren van strategische afhankelijkheden, door monopolisering van essentiële grondstoffen (olie/gas/rare earth metals) en doorvoerroutes.
- Het instellen van economische sancties/boycots

De Chinese economische manifestaties vloeien voort uithaar economische beleidsplannen, zoals 'Made in China 2025' en de 'Nieuwe Zijderoutes', waarmee het de eigen economische en geopolitieke invloed wil vergroten.[42] China zet hierbij een breed scala aan (heimelijke) middelen in, waaronder (digitale) economische spionage.

Mogelijke consequenties

Deze instrumenten worden ingezet om druk te genereren op individuele landen om zo hun beleid en standpunt ten opzichte van Moskou te beïnvloeden, èn om allianties zoals de EU maar ook de NAVO uit elkaar te spelen. Vooral daar waar een instrument een aantal lidstaten aanzienlijk harder treft dan andere, zal er discussie ontstaan en kan dit instrument als wig functioneren om de Europese solidariteit open te breken. Het doel van deze wigfunctie is drieledig: 1) het doen afbrokkelen van steun voor de Europese sancties tegen de Russische Federatie; 2) het zaaien van tweespalt binnen de EU en 3) het zaaien van tweespalt tussen de EU en de VS.

Effecten voor de energievoorzieningszekerheid. Het Kremlin kan besluiten om het energiewapen in te zetten als reprimande tegen internationale sancties, hoewel dit een dubbelsnijdend zwaard is, dat ook de Russische belangen zwaar treft. De Russische afhankelijkheid van olie- en gasinkomsten is zo groot en de EU zo'n belangrijke afnemer van het gas, dat het onwaarschijnlijk is dat afsnijden van gaslevering aan EU een reële optie is. Desalniettemin is EU bezig met het ontwikkelen van een Europese energievoorzieningszekerheid strategie, om de afhankelijkheid van Russische gas te verkleinen. Dit leeft ook in het publieke debat, getuige de discussie over Nordstream-2. Afhankelijk van de uitwerking van de ambities uit dit document, kan dit gevolgen hebben voor de Nederlandse gaswinning.

Er zijn economische effecten voor Nederland als onderdeel van een internationaal/mondiaal systeem, wanneer bijvoorbeeld de wederzijdse economische sancties, gasperikelen en kapitaalvlucht uit Rusland gevolgen hebben voor de wereldeconomie. Maar er zijn ook economische effecten voor Nederland doordat de bilaterale handelsbetrekkingen met de Russische Federatie negatieve gevolgen ondervinden.

41 Waarbij het kanttekening verdient dat China veel diepere zakken heeft dan Rusland en zijn economische macht over de hele wereld aanwendt. Bij de motieven daarachter en de lokale impact ervan zijn vraagtekens te plaatsen, zie bijv. "Belt and Road projects direct Chinese investments to all corners of the globe. What are the local impacts?", *Washington Post*, 11 september 2018

42 *AIVD Jaarverslag 2018*, 2 april 2019

Gevolgen van de manier waarop China middels economische middelen de eigen belangen behartigt zijn bijvoorbeeld dat het verdienvermogen van Nederlandse bedrijven wordt ondermijnd.[43] Op termijn kunnen de activiteiten zelfs resulteren in economische en politieke afhankelijkheden.

4. Digitale manifestaties

Het betreft hier niet zozeer een specifiek instrument, als wel een domein waarbinnen verschillende instrumenten kunnen worden ingezet. De AIVD neemt van onder meer Iran, Noord-Korea en Rusland waar dat zij zich schuldig maken aan sabotage en/of misbruik van de ICT-infrastructuur.[44] Van China, Iran en Rusland is gebleken dat zij offensieve cyberprogramma's hebben, gericht tegen Nederland.[45] Moskou, maar ook de NAVO, benadert het digitale domein ook nadrukkelijk als een nieuwe strijdarena[46] die is toegevoegd aan de reeds bestaande arena's (militair, internationaal-politiek en economisch) en gebruikt dit domein ook in combinatie met militaire middelen.[47] Moskou heeft het belang van dit domein tijdig onderkend, heeft fors geïnvesteerd in offensieve cybercapaciteiten en is in het digitale domein een zeer geduchte tegenstander. Moskou zet de cybercapaciteiten voor een diversiteit aan doelstellingen in: om informatie te verwerpen of vervormen; om landen te desoriënteren; ter afleiding of ondersteuning van eigen militaire activiteiten en als middel voor verstoring van civiele infrastructuur.[48] Russische hackers hebben aanvallen gepleegd op o.a. overheden, internationale organisaties, industriële installaties, financiële instellingen en media.
De afgelopen jaren waren er diverse incidenten die het gebruik van cybermiddelen ten behoeve van manipulatie, sabotage en desinformatie illustreren:

- **De hack op de Democratic National Committee (DNC)** De Amerikanen hebben publiekelijk Moskou beschuldigd. Volgens sommige analisten zou deze campagne tot doel hebben de presidentiele verkiezingen te beïnvloeden en de kandidatuur van Trump te bevoordelen, terwijl anderen geloven dat de bedoeling van het lek was om het Amerikaanse politieke proces in zijn algemeenheid in diskrediet te brengen en te verstoren.
- **Cyberaanval op de Bondsdag** Het Bondsdag-netwerk werd zeer breed geïnfiltreerd. Het grootste gedeelte van het netwerk moest hierdoor compleet vervangen worden. In totaal zou het gaan om meerdere duizenden computers. Het duurde zeker 15 weken voordat het netwerk weer was opgebouwd, geïnfecteerde systemen opnieuw geïnstalleerd en functionaliteiten hersteld. De hack op de Bondsdag wordt meestal toegeschreven aan een Russische statelijke actor.
- **Digitale sabotage bij TV5Monde** De aanval slaagde er in de uitzendingen te verstoren en de systemen van de zender te saboteren. Verder plaatsten de aanvallers onder meer een afbeelding met de tekst 'Je suis IS' op de pagina en maakten zij cv's van Franse militairen openbaar. De aanval werd uitgevoerd onder naam van het 'Cybercaliphate'.[49] Beveiligingsbedrijven relateerden de aanval echter (op basis van technische indicatoren) aan een spionagecampagne die door diverse onderzoekers aan een Russische statelijke

43 China heeft interesse in Nederlandse bedrijven uit de sectoren: hightech, energie, maritiem en 'life sciences & health'. Ibidem
44 Ibidem
45 Ibidem. Van een offensief cyberprogramma wordt gesproken als staten digitale middelen inzetten voor spionage en sabotage om zo hun eigen politieke, militaire, economische en/of ideologische doelen te bereiken ten koste van Nederlandse belangen.
46 De NAVO heeft onlangs cyber als domein van militair optreden benoemd, naast land, lucht, zee en ruimte.
47 Zoals tijdens de annexatie van de Krim, toen de belangrijkste Oekraïense overheidswebsite als gevolg van een cyber aanval 72 uur offline was. Maar ook Georgië heeft dit in 2008 ondervonden. *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, Policy Paper no. 9 (2016) van het Russia Studies Centre, mei 2016
48 *MIVD Jaarverslag 2016*, 24 april 2017
49 Deze naam werd ook gebruikt bij de digitale aanval op de site van CentCom, het Amerikaanse strategische hoofdkwartier dat de militaire operaties in het Midden-Oosten en Centraal-Azië aanstuurt.

actor wordt toegeschreven. Dezelfde campagne wordt meestal in verband gebracht met aanvallen op o.a. militaire doelen, veiligheidsdiensten en ambassades van de Verenigde Staten en bondgenoten in (Oost-)Europa. Mogelijke motivaties voor de aanval zijn: dat Russische actoren ontevreden waren met de berichtgeving van TV5 Monde over het Oekraïne conflict; dat Russische actoren de aandacht van de operaties van het Kremlin in de Oekraïne wilden afleiden door het Westen zich te laten richten op ISIS; dat Russische actoren wilden laten zien waartoe ze in staat zijn, namelijk het saboteren van media.

- **De close access hackpoging op de OPCW**[50] Tijdens en live uitgezonden persconferentie maakte de MIVD bekend dat het op 13 april 2018 een hackaanval van de Russische geheime dienst verhinderd op de OPCW in Den Haag. De Russen zouden geprobeerd hebben om het wifi-netwerk van de OPCW te hacken. De hackaanval vond plaats in dezelfde periode als het onderzoek van de OPCW naar de vergiftiging van de Russische oud-dubbelspion Sergej Skripal en zijn dochter. In die tijd deed de OPCW ook onderzoek naar de gifgasaanval in Douma, in Syrië. Rusland is een belangrijke bondgenoot van het Syrische regime. De OPCW was dus met twee voor Moskou gevoelige onderzoeken bezig.
- **Trollen/Social Cyber Attacks** Gebruikt voor het online verspreiden van desinformatie/ het voeren van online informatieoperaties. Zie verder bij manifestatie zes: propaganda en desinformatie.

Mogelijke consequenties

De mogelijke consequenties van de inzet van cybercapaciteiten zijn legio: van spionage tot beïnvloeding en verstoring, afhankelijk van wat het beoogde doel van de inzet van deze capaciteiten is. De effecten kunnen dan ook over de hele linie van nationale veiligheidsbelangen voelbaar zijn. Een saboterende cyberaanval op vitale infrastructuur kan leiden tot fysieke en ecologische schade, slachtoffers en maatschappelijke onrust. Spionage schaadt de integriteit en exclusiviteit van informatie. Trollenfabrieken en social cyberattacks (als onderdeel van een bredere al lopende beïnvloedingscampagne) schaden de politieke en sociale stabiliteit, kunnen de sociale cohesie ondermijnen en uiteindelijk het functioneren van de democratische rechtsorde. Ze hebben allemaal gemeen dat ze economische en reputatieschade toebrengen aan het slachtoffer (bedrijf of overheid). Het lastige bij cyberaanvallen is de attributie: het is heel moeilijk onomstotelijk vast te stellen wie er achter een aanval of campagne zit. Hierdoor is een adequate politiek-diplomatieke respons nauwelijks mogelijk. Bovendien laat de lastige attributie ruimte voor twijfel, waar de agressor handig van gebruik kan maken. Cybercapaciteiten zijn daarmee ideale instrumenten voor hybride conflictvoering: ze bieden veelzijdigheid, heimelijkheid en ontkenbaarheid ineen. En kunnen zowel digitale, economische als fysieke schade toebrengen.

5. Buitenlandse inmenging (inclusief politieke beïnvloeding)[51]

Sinds jaar en dag maken heimelijke activiteiten onderdeel uit van de middelen die staten inzetten om hun belangen (in het buitenland) te behartigen. Het gaat bij deze activiteiten ook om de inmenging in het buitenland. Voor het bereiken van bepaalde strategische doelstellingen zetten staten soms middelen in die niet direct naar het doel leiden, maar door een combinatie van de middelen de doelstelling bereikbaar maken. Bij buitenlandse inmenging gaat het vaak om specifieke beïnvloeding van in het buitenland

50 Organisation for the Prohibition of Chemical Weapons. "MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen", NOS.nl 4 oktober 2018 en Kamerbrief van de minister van Defensie d.d. 4 oktober 2018, kst-33694-21, vergaderjaar 2018-2019

51 Inmiddels is door de Nederlandse overheid een aanpak van buitenlandse inmenging geformuleerd. In de brief van ministers van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer van 16 maart 2018 wordt uiteengezet wat het kabinet onder ongewenste buitenlandse inmenging verstaat. De brief gaat ook in op de inzet van het kabinet om de weerbaarheid tegen ongewenste buitenlandse inmenging te vergroten. Kamerstuk 30821 nr. 42, vergaderjaar 2017-2018.

woonachtige diaspora. Dit wordt ook wel diasporabeleid of de 'lange arm' genoemd[52] en is een subversief[53] middel dat onderdeel kan zijn van een bredere campagne, waarbij diaspora wordt ingezet als instrument. "Dergelijke ongewenste en heimelijke activiteiten van buitenlandse mogendheden in Nederland zijn een inbreuk op de Nederlandse soevereiniteit en kunnen ernstige schade toebrengen aan de nationale veiligheid. Dergelijke inmenging kan leiden tot ernstige aantastingen van de politieke en bestuurlijke integriteit, ondermijning van de internationale rechtsorde en stabiliteit, radicalisering onder bevolkingsgroepen en aantasting van grondrechten, ondermijning van voor Nederland vitale sectoren en aantasting van de internationale concurrentiepositie van Nederland."[54] Buitenlandse inmenging gaat echter veel verder dan alleen het beïnvloeden, manipuleren of intimideren van diaspora.[55]

In het Nationaal VeiligheidsProfiel (NVP) is het subthema "Ondermijning democratische rechtsstaat en open samenleving" opgenomen.[56] Dit illustreert het actuele en duurzame karakter van de dreiging die van buitenlandse inmenging uitgaat. Het gaat in het NVP om ondermijning van het politieke en maatschappelijke systeem van Nederland[57] dat omschreven kan worden als 'democratische rechtsstaat' en 'open samenleving', die op korte of langere termijn wordt teweeg gebracht .[58] "Het gaat om stelselmatige, doelbewuste en in vele gevallen heimelijke activiteiten van statelijke of niet-statelijke actoren die door de nagestreefde doelen, de gebruikte middelen of ressorterende effecten de democratische rechtsstaat en de overheid die deze draagt kunnen compromitteren, verzwakken, destabiliseren, ondergraven of saboteren. Of om activiteiten die door de nagestreefde doelen, de gebruikte middelen of ressorterende effecten ernstig schade toebrengen aan de noodzakelijke samenhang van de samenleving doordat ze het onderling vertrouwen en de solidariteit tussen burgers doen afkalven. De ondermijning leidt in vele gevallen niet tot directe, acute ontwrichting maar de aantastende werking kan op langere termijn leiden tot ernstige disruptie en disfunctioneren van de democratische rechtsorde en open samenleving."

52 Meestal wordt de beïnvloeding van diaspora primair gedreven vanuit (politiek en financiëel) lijfsbehoud van de beïnvloedende overheid: Het streven naar behoud van de statelijke status quo in het herkomstland (incl. de bestaande statelijke structuur, rol en positie staatshoofd, rol en positie onderdanen (zowel in binnen- als buitenland). Daartoe dienen 'dissidente' geluiden, ook binnen de diaspora, worden onderdrukt. Daarnaast heeft een herkomstland financiële belangen bij de diaspora

53 Qua effect, maar soms ook qua intentie.

54 *Openbaar jaarverslag 2003*, AIVD

55 De Nederlandse overheid onderkent het gevaar van ongewenste buitenlandse inmenging en heeft daarover haar standpunt kenbaar gemaakt in een brief aan de Tweede Kamer d.d. 16 maart 2018, kst-30821-42,vergaderjaar 2017-2018. Hierin wordt de volgende definitie gegeven: "Ongewenste buitenlandse inmenging betreft namelijk doelbewuste, vaak stelselmatige en in vele gevallen heimelijke activiteiten van statelijke actoren (of actoren die aan statelijke actoren zijn te relateren) in Nederland of gericht op Nederlandse belangen, die door de nagestreefde doelen, de gebruikte middelen of ressorterende effecten het politieke en maatschappelijke systeem van Nederland kunnen ondergraven." De Kamerbrief geeft voorbeelden van verschillende staten die dergelijke buitenlandse inmenging aanwenden. Het AIVD Jaarverslag 2018 noemt met naam China, Iran, Rusland en Turkije.

56 Het NVP volgt de Nationale Risicobeoordeling (NRB) op en wordt gemaakt door het Analistennetwerk Nationale Veiligheid in opdracht van de Stuurgroep Nationale Veiligheid.

57 Het totaal aan mogelijke implicaties van beïnvloeding zijn breder dan deze insteek van het NVP.

58 Of; 'democratische rechtsorde' in zijn verticale dimensie (de verhoudingen tussen overheid en burgers, te betitelen als 'democratische rechtsstaat') en zijn horizontale dimensie (de verhoudingen tussen burgers onderling, te betitelen als 'open samenleving').

Als statelijke actoren die zich hiervan bedienen worden ook buitenlandse mogendheden onderkend waarmee Nederland in conflict is of op gespannen voet staat. Bij buitenlandse inmenging wordt gebruik gemaakt van verschillende beïnvloedingsmethodes: bijvoorbeeld door invloed te verwerven onder studenten, in de media, bij sommige politici, in de publieke opinie, zonder dat betrokkenen het vaak meteen beseffen. Soms kan er sprake zijn van heimelijke financiering. Ook desinformatie, het verspreiden van valse geruchten en complottheorieën via (schimmige) nieuwssites en sociale media behoort tot de gebruikte tactieken. Het geheel van deze heimelijke inmengings- en beïnvloedingsactiviteiten wordt omschreven met de term '*active measures*'.[59] Het gaat hierbij naar de inschatting van de, bij het tot stand komen van het NVP, betrokken experts om zeer reële risico's voor de belangen van de nationale veiligheid. Dergelijke beïnvloedingsmethodes vinden vaak in combinatie met/aanvulling op elkaar plaats, zodat er op verschillende plekken in de maatschappij invloed wordt uitgeoefend.
De Russische Federatie is zeer bedreven in het gebruik van *active measures*, een methodiek die ook wel "het hart en de ziel" van de Sovjet inlichtingenmachine werd genoemd.[60] Het doel was niet zozeer inlichtingen te vergaren, als wel de subversieve werking van de *active measures*: het verzwakken van het Westen; het drijven van wiggen in de Westerse allianties, met name de NAVO; verdeeldheid zaaien tussen bondgenoten; afbreuk doen aan het aanzien van de VS/het Westen bij het algemeen publiek in de rest van de wereld. Allemaal ter voorbereiding op het eventuele geval dat er daadwerkelijk oorlog uit zou breken.

Op dit moment worden verschillende Russische *active measures* waargenomen of erkend. Meest duidelijk natuurlijk in Oekraïne, waar beïnvloeding van de publieke opinie en besluitvormers aan de orde van de dag is en waar ook is geressorteerd in het stimuleren van de lokale bevolking tot gewapend verzet tegen de eigen overheid. Maar ook in het Westen wordt inmenging waargenomen, onder meer het financieel steunen van anti-EU partijen (zoals het Front National van Marine LePen).

Nederland is, als lidstaat van de EU en de NAVO, maar zeker ook als *lead nation* bij het onderzoek naar de toedracht van de crash van MH17, een relevant doelwit voor beïnvloeding. Dat betekent dat het voorstelbaar is dat Nederland te maken krijgt met ongewenste inmenging vanuit Moskou. Een uitgelezen moment voor inmenging is rond belangrijke staatsmomenten, zoals verkiezingen. We zagen dat ook in de VS gebeuren en zagen de zorgen bij andere EU-lidstaten die in 2017 verkiezingen hadden.[61] Verkiezingen zijn een uitgelezen moment om politieke besluitvorming en de publieke opinie te beïnvloeden. Verschillende (statelijke) actoren hebben daar baat bij en kunnen middelen inzetten voor dergelijke beïnvloeding. Hierbij kan het gaan om het verstoren van het democratisch proces door middel van digitale sabotage (bijv. manipulatie stemcomputers, accounts/computers van politieke partijen)[62], het beïnvloeden van de stem zelf (door middel van propaganda, desinformatie,) of het aantasten van de (gepercipieerde!) betrouwbaarheid van de uitslag. Deze beïnvloeding kan in verschillende fasen van de verkiezingen plaatsvinden: in de aanloop/campagneperiode, op de verkiezingsdag zelf, en tot slot daarna in de verslaglegging van de uitslagen.
Het was daarom voorstelbaar dat Nederland tijdens de totale verkiezingsperiode (voor-tijdens-na)

59 *Active measures* is de Sovjet term voor buitenlandse inmenging en deze maatregelen omvatten het hele scala van beïnvloedingsmethodes: van media manipulaties tot geweld.
60 Door oud-KGB majoor-generaal Oleg Kaloegin.
61 "Maaßen warnt vor Einfluss Moskaus auf Bundestagswahlkampf", *Hamburger Abendblatt Online*, 16 november 2016. En nog steeds bestaan de zorgen: „Cyber attacks rob future elections of their legitimacy, Jeremy Hunt warns", *The Telegraph*, 7 maart 2019. Waarin minister van Buitenlandse Zaken Hunt specifiek doelt op autoritaire regimes die democratische processen in het Westen op de korrel nemen. Hij noemt Rusland, China, Iran en Noord-Korea als actoren die achter diverse hacks en online campagnes zaten.
62 "Microsoft spots Russian hacking campaign ahead of EU elections", *Sky News*, 20 februari 2019

geconfronteerd zou worden met pogingen tot beïnvloeding van de verkiezingen. Het feit dat in hetzelfde jaar twee andere belangrijke lidstaten van EU en NAVO en deelnemers aan de *Coalition of the Willing* tegen ISIS–Frankrijk- en Duitsland- ook verkiezingen hebben, maakte de pogingen tot beïnvloeding eigenlijk alleen maar aannemelijker. De Nederlandse verkiezingen vonden het eerst plaats, gevolgd door de Franse in april/mei en de Duitse in september. Frankrijk en Duitsland zijn grotere vissen, dit maakte Nederland mogelijk een geschikt proefkonijn. Vanuit dit bewustzijn zijn de Nederlandse verkiezingen nauwlettend gevolgd, zowel nationaal als internationaal.

Het NVP besteedde aandacht aan ongewenste inmenging met een scenario waarin concrete voorbeelden van (heimelijke) inmenging en beïnvloedingsactiviteiten van buitenlandse overheden, zijn uitgewerkt. Zie onderstaande figuur voor het scenario en de gebruikte bouwstenen. Het scenario was een *worst case scenario* met een waarschijnlijkheidsbeoordeling van 'waarschijnlijk': het scenario is zeer voorstelbaar en er zijn aanwijzingen dat het scenario zich kan voordoen. Er was bij deze beoordeling sprake van slechts kleine onzekerheid. De impact op de nationale veiligheidsbelangen was als volgt. Op territoriale veiligheid was sprake van ernstige impact op de internationale positie. Er werd geen impact geïdentificeerd op de fysieke veiligheid. Er was sprake van aanzienlijke impact op economische veiligheid als gevolg van kosten. Op ecologische veiligheid werd geen impact geïdentificeerd. Maar op de sociaal-politieke stabiliteit werd een zeer ernstige aantasting van de democratische rechtsstaat geïdentificeerd en een ernstige sociaal-maatschappelijke impact. De gebruikte bouwstenen zijn echter slechts een greep uit de mogelijke middelen uit *active measures*. Een andere impact is dus zeker mogelijk, zowel wat betreft de getroffen belangen als wat betreft de ernst van de impact.

NVP Scenario worst case statelijke actoren – 'Ondermijning vanuit buitenland' – Verhaallijn

De Nederlandse jeugd, media en elite (zakelijk, politiek, academisch) worden via een scala aan (heimelijke) activiteiten beïnvloed door een niet-westers land dat de EU wil ondermijnen en de tegen dit land opgelegde sancties opgeheven wil zien. Er worden bijvoorbeeld geruchten verspreid over vermeende, grote fraude- en corruptieschandalen binnen de EU (zie o.a. 'middelen' in het bouwstenenschema voor andere gebruikte activiteiten). Een aantal Nederlandse bestuurders en politici ziet zich genoodzaakt om af te treden (ondanks gebrek aan duidelijk bewijs). Er worden complottheorieën over het Nederlandse en Europese migratiebeleid verspreid. Tevens wordt gesuggereerd dat migranten vrouwen hebben lastig gevallen en de overheid niet optreedt. Na verloop van tijd begint de Nederlandse bevolking het vertrouwen in de overheid te verliezen en heerst er twijfel over de EU en andere samenwerkingsverbanden. Een ultrarechtse partij met een anti-EU en anti-migratie agenda, wiens activiteiten door het betreffende land heimelijk worden gesponsord (iets wat ook in andere EU landen gebeurt), ziet zijn aanhang sterk toenemen. De tegenstellingen tussen voor – en tegenstanders van de EU en het vluchtelingenbeleid worden steeds groter. De Nederlandse anti-EU en anti-migratiepartij organiseert regelmatig demonstraties die uitmonden in ernstige onlusten. Nederlandse politici en bestuurders krijgen via de sociale media rond de thema's EU en migratie voortdurend en op grootschalige wijze te maken met een stroom van uitingen van haat, intimidatie en bedreigingen, waardoor ze in hun functioneren ernstig worden gehinderd.

NVP Scenario worst case statelijke actoren – 'Ondermijning vanuit buitenland'- Bouwstenen

De volgende bouwstenen zijn bij dit scenario gebruikt:

Actor =	overheden uit landen waarmee Europa/Nederland op gespannen voet staat/een conflict heeft.
Doelen =	vertrouwen in de overheid aantasten; legitimiteit van overheid ondergraven; politieke invloed verkrijgen; imago van Nederland/het Westen aantasten; wig drijven binnen EU.
Middelen =	legitimiteit van de overheid ter discussie stellen en in de praktijk ondergraven; Intimidatie; (heimelijke) beïnvloeding; Propaganda via klassieke en sociale media; Desinformatie via klassieke en sociale media; Rekruteren van personen; Intredepolitiek/met verborgen agenda lidmaatschap verkrijgen van politieke partijen, gemeenteraden, overlegorganen van overheid e.d. ; Het cultiveren/'tasken' van personen met invloed in het bedrijfsleven; Invloed in de media verkrijgen om een bepaald beeld naar buiten te brengen; Invloed in de wetenschap krijgen.
Targets =	Overheden (landelijk of lokaal); Media; Wetenschap; Westerse wereld/EU; Nederlandse burgers/publieke opinie.

Mogelijke consequenties

Ook bij buitenlandse inmenging zijn de mogelijke consequenties legio, afhankelijk van wat het beoogde doel, het target en de gebruikte middelen (routes) zijn. De effecten kunnen dan ook over de hele linie van nationale veiligheidsbelangen voelbaar zijn.

6. Propaganda en desinformatie

Het informatiedomein en informatieconfrontatie heeft een centrale plaats in het Russische militaire denken. Informatieconfrontatie kan niet als een zelfstandige, losstaande dreiging worden beschouwd: het is onderdeel van een groter plan, van een coherente en complementaire campagne. Het is de rode draad door de wijze waarop in Moskou conflictvoering wordt bedreven. Het doel is om in de besluitvormingscyclus van de tegenstander te komen en deze dan te vertragen, te verwarren.[63] Het doel van desinformatie is (o.a.) om besluiteloosheid te creëren, waardoor je kwetsbaarder wordt voor een besluitvaardige tegenstander. Een ander doel van desinformatie is om Westerse waarden in diskrediet te brengen.[64] Zo worden Westerse vrijheden en verworvenheden (zoals de acceptatie van homoseksualiteit) afgeschilderd

63 *MIVD Jaarverslag 2016*, 24 april 2017

64 Desinformatie richt zich bijv. op het vergroten van sociale spanningen en het polariseren van het politieke spectrum, zodat het vormen van een regering met draagvlak in de maatschappij moeilijker wordt. Via het ondermijnen van vertrouwen in de Nederlandse overheid, (inter)nationale autoriteiten en gevestigde media worden Westerse verworvenheden als democratie aangetast.

als tekenen van morele neergang. Deze visie op informatieconfrontatie kleurt ook de Russische perceptie.[65] Zo wordt dus ook informatie van buitenaf (uit het Westen) ontvangen: als onderdeel van informatieoperaties.

Dit verklaart waarom het voor Moskou zo belangrijk is om controle over de media te hebben. Voor Moskou is het essentieel om '*information superiority*' te verkrijgen vis-à-vis het Westen, omdat dit welhaast het belangrijkste middel is om de Westerse superioriteit op het gebied van militaire middelen te compenseren. De informatieconfrontatie is een essentieel onderdeel van de Russische hybrideconflictvoering. Een oogmerk hierbij is het creëren van onzekerheid door de besluitvormingsprocessen van de NAVO en de EU te frustreren. Het effect hiervan is dat deze organisaties als gefragmenteerd , besluiteloos en zwak kunnen worden afgeschilderd.

Voor Moskou is propaganda/desinformatie altijd een belangrijk en veelgebruikt instrument geweest, maar de rol van dit instrument is toegenomen met de komst van internet en sociale media. Allerlei actoren gebruiken sociale media in hun strijd, net zoals de telegraaf in de negentiende eeuw een nieuwe oorlogsinstrument werd.[66]
Voorbeeld MH17: De ontkennende, tegenstrijdige en verwarrende berichtgeving die vanuit de Russische Federatie over de toedracht van de crash van MH17 en het onderzoek daarnaar wordt verspreid. Deze desinformatie-campagne kwam al direct na de crash op gang. Moskou wil met deze desinformatie bereiken dat in ieder geval de Russische nieuwsconsument niet meer weet wat te geloven. En dat het internationale onderzoek naar de crash in diskrediet wordt gebracht zodat dit een eventuele rechtsgang verder bemoeilijkt.

De grondslag voor desinformatie: het strategisch narratief

Het is belangrijk om te beseffen dat Moskou zich bedient van een strategisch narratief dat als basis dient voor de informatieconfrontatie: Geschiedenis als een oneindige dialoog tussen verleden en heden. Hierbij worden verwijzingen naar en echo's van het verleden gebruikt om gebeurtenissen in het heden te duiden, zin te geven. Het narratief legitimeert de actie en wordt aangepast aan het publiek, ook op landenniveau.[67] Ten aanzien van Oekraïne wordt het narratief van de gedeelde culturele geschiedenis gebruikt (Kiev als moeder aller Russische steden etc), daarom moeten de Russische Federatie en Oekraïne bij elkaar blijven. Moskou bedient zich ook vaak van het nazi/fascisten-narratief, vanwege de heldenrol van de Sovjet-Unie in de overwinning op nazi-Duitsland. Dit narratief heeft als doel te appelleren aan die heldenrol en de tegenstander af te schilderen als nazi/fascist (de meest ongewenste rol in de moderne geschiedenis) waarover in het verleden al werd gezegevierd. De Russische inlichtingendiensten spelen bij de vorming van dit narratief een belangrijke rol: zij hebben een steeds grotere greep op de samenleving gekregen en ook op de geschiedschrijving of de interpretatie van de geschiedenis.

65 Mark Laity, oud-BBC correspondent en huidig Chief Strategic Communications SHAPE/NAVO, tijdens "Disinformation as a weapon in hybrid warfare", 12 oktober 2016, Lezing Atlantische Commissie
66 *War goes viral. How social media is being weaponized across the world*, www.theatlantic.com/magazine/archive/2016/11
67 Zo zou er ook een speciaal narratief voor Nederland zijn. Daarnaar gevraagd kon Laity niet goed antwoord geven "dan werd het te politiek", 12 oktober 2016. Het doel is iig dat wij onzekerheid hebben over MH17. Verder krijgen we hetzelfde narratief voorgeschoteld van het (moreel) verval van de EU, dat ze alle lidstaten voeren.

Verschijningsvormen desinformatie

Het gaat om oude ideeën (delay, deceive, confuse) met moderne middelen (sociale media). Tijdens de Koude Oorlog was propaganda en desinformatie (van beide zijden) in sterke mate op ideologische leest geschoeid. Hoewel het ideologisch fundament tegenwoordig minder uitgesproken is (dit geldt ook weer voor beide zijden), wordt de propaganda en desinformatie in toenemende mate in ideologische termen gegoten. Er is sprake van een toenemende waarden- en normentegenstelling.
Nieuw, i.v.m. de opkomst van internet en sociale media, is het fenomeen trollen/Social Cyber Attacks. Trollen is het cyber-werkwoord voor het creëren van verwarring en het zaaien van paniek/haat door middel van desinformatie verspreid door zogenaamd echte gebruikers op sociale media. Sommige (statelijke) actoren hebben dit middel geprofessionaliseerd door de inzet van 'trollenfabrieken': hele organisaties medewerkers die de hele dag door posts op sociale media zetten.[68] De Russische Federatie gebruikt het creëren van verwarring en zaaien van paniek al langer om de juiste condities te creëren die de Russische belangen dienen. Met de komst van het internet tijdperk heeft de Russische Federatie deze nieuwe technieken opgenomen in haar arsenaal met online desinformatie campagnes, propaganda verspreiding en het breed inzetten van internet trolling. Volgens Margarita Levin Jaitner (Swedish Defense University) maakt de Russische Federatie naast 'trolls' gebruik van zogenaamde 'opinion agents'[69] die worden ingezet om het wantrouwen dat Russen in de massale media hebben te omzeilen door ze via sociale netwerken en blogs te bestoken met 'truthful information'. Sociale media zijn ook voor het Nederlandse publiek een belangrijke nieuwsbron. Dit geldt met name voor mensen die via de reguliere media niet (voldoende) worden bediend met berichtgeving die aansluit op het eigen wereldbeeld. Het risico van sociale media is de filterbubbel, die ervoor zorgt dat de ontvanger met name berichtgeving krijgt die hem steunt of versterkt in zijn overtuigingen. Als correcties van onwaarheden al plaatsvinden, dan worden ze nauwelijks gelezen of gedeeld door het publiek dat met verzonnen berichten is bereikt. Bij het NATO Strategic Communications Centre of Excellence worden de strategische communicatie aspecten van social media in het Rusland-Oekraïne conflict geduid. Ze gaan in op het gebruik van PSYOPS (Psychological Operations) en sociale media en introduceren hierbij de term Social Cyber Attacks.[70] Het gaat hierbij om het handelen onder een valse identiteit of anoniem waarbij gemanipuleerde signalen worden verspreid of bestaande signalen worden gemanipuleerd om de volgende effecten te bereiken: chaos, paniek en grootschalige publieke ongehoorzaamheid. Deze puur psychologische effecten zijn effectief ingezet in het Rusland-Oekraïne conflict om militaire operaties te ondersteunen.

Daarnaast maakt Moskou gebruik van ouderwetse middelen zoals het vervalsen van officiële documenten en officiële communicatie van andere overheden, om deze zo in diskrediet te brengen en te dwingen tot allerlei uitleg en verklaringen.
Enkele voorbeelden van (flagrante) desinformatie en gevolgen zijn:

- De dreigvideo met betrekking tot het Oekraïne-referendum, waarin bij een "Nee" werd gedreigd met geweld en een Nederlandse vlag werd verbrand. Deze video werd gelukkig binnen 2 uur gedebunked.
- De Lisa-casus: verkrachting van 12-jarig meisje in Duitsland door asielzoekers. Dit bericht werd pas na 2 dagen gedebunked en bracht in de tussentijd honderden demonstranten tegen Merkel op de been.

68 Deze trollenfabrieken hoeven niet perse te opereren vanuit Rusland. Een recent voorbeeld is de Internet Research Agency, die in de VS is gevestigd en vanaf daar opereert, maar de Russische agenda pusht.
69 In Nederland kennen we dit fenomeen ook. Of deze opinion agents een link met Rusland hebben is de vraag. Wat in ieder geval wel zeker is, dat de Russische staatsmediabureaus op de hoogte zijn welke groepen/initiatieven/influencers op sociale media in het Nederlands taalgebied actief zijn, deze volgen en regelmatig citeren in de eigen berichtgeving.
70 zoals gedefinieerd door Dr Rebecca Goolsby

Russische desinformatie-capaciteiten

Het Kremlin geeft financiële steun aan honderden mediakanalen en veel NGO's. Dat betekent dat er duizenden professionals aan het werk zijn tegen de EU/NAVO/Westen/VS. Ze zijn in staat maatwerk te leveren: desinformatie per doelgroep/land. Zo zal bijvoorbeeld in de Baltische staten de Russischtalige minderheid een cruciale tool zijn. Ook is de lokale bevolking betrokken (bewust/onbewust) bij desinformatie: bijv. de lokale reporters van de internationale Russische media kanalen, zoals de newsoutlets van het Russische RT. Hiermee wordt aan de desinformatie een schijn van onpartijdigheid verleent.
Voor Moskou[71] is de informatieconfrontatie een 24/7 business, waarin sprake zou zijn van korte en directe commandolijnen.[72]

Mogelijke consequenties

Er is op dit moment in Nederland (en het Westen) sprake van een grotere kwetsbaarheid/bevattelijkheid voor desinformatie dan voorheen. De dreiging is significant, omdat het publiek rijp is voor desinformatie campagnes.[73] Daar staat tegenover dat de dreiging de afgelopen jaren op zowel nationaal als internationaal niveau is onderkend, dat er door zowel particuliere[74] als publieke[75] initiatieven wordt ingezet op onderzoek naar en bestrijding van desinformatie. Ook de grote aandacht die alle media besteedden aan het fenomeen hebben het bewustzijn over het bestaan ervan vergroot. Op termijn kan dit alles de weerbaarheid verhogen. Dat het publiek rijp is voor desinformatiecampagnes komt door het toegenomen wantrouwen van burgers in overheid, gevestigde media en autoriteiten. En juist dat wantrouwen wordt uitgebuit in desinformatie-campagnes. De polarisatie binnen de samenleving wordt uitgebuit voor destabilisering van de EU. Het feit dat we in het Westen geen sterk eigen narratief hebben dat we tegenover het Russische narratief kunnen zetten maakt ons kwetsbaarder. Het feit dat gebruikers van sociale media geen passieve consumenten zijn, zoals bijv. TV-kijkers, maar actief betrokken zijn bij de discussie en de informatie die wordt gedeeld, maakt dat zij deze informatie ook meer zullen internaliseren. De impact van desinformatie is dus veel directer en de berichtgeving kan *realtime* worden aangepast naar gebleken (in)effectiviteit.[76] Desinformatie is dus zeer flexibel en verder vrij goedkoop. Een geslaagde informatieconfrontatie zou burgers kunnen mobiliseren zich af te wenden van de eigen overheden en instituties, kan leiden tot ernstige polarisatie, en zo voorts. Als we een blik vooruit in de toekomst werpen, dan zullen de technologische ontwikkelingen ons nog voor grote uitdagingen stellen in het domein van desinformatie: de komst van 'deep fakes' ofwel bewerkte video's.[77] De term 'deep fake' staat voor audio en videobeelden die door middel van kunstmatige intelligentie zijn gecreëerd. Met deze technologie is het mogelijk om geluid- en beeldopnames te creëren, waarin echte mensen dingen zeggen of doen die ze in werkelijkheid nooit gezegd of gedaan hebben. Terwijl deze techniek ooit alleen maar werd toegepast n de special effect studio's van Hollywood, is de technologie nu toegankelijker geworden voor de massa. Bovendien ontwikkelt de technologie steeds verder waardoor video en audio materiaal steeds sneller en makkelijker kunnen worden geproduceerd met ook nog eens een realistischer resultaat. En terwijl wetenschappers proberen met algoritmes 'deep fake' video's te ontmaskeren en onschadelijk te maken, zorgen de zelflerende algoritmen ervoor dat deze video's steeds realistischer worden en

71 En andere grote spelers.
72 Lezing "Disinformation as a weapon in hybrid warfare", 12 oktober 2016
73 ibidem
74 Zoals Bellingcat en de Alliance for Securing Democracy.
75 Zoals EU vs Disinformation van de EU European External Action Service East Stratcom Task Force
76 Lijkt een bepaalde verhaallijn niet aan te slaan, dan wordt deze losgelaten en een andere geprobeerd.
77 "You thought fake news was bad? Deep fakes are where truth goes to die", *The Guardian*,12 november 2018 en *VPRO Tegenlicht* op 18 november 2018

moeilijker te detecteren zijn. Niet voor niets heeft het Amerikaanse Ministerie van Defensie de 'deep fake' technologie aangemerkt als een bedreiging voor de nationale veiligheid.

Concluderend kan worden opgemerkt dat de hier beschreven manifestaties meestal op alle nationale veiligheidsbelangen, behalve ecologische veiligheid, impact kunnen hebben. De potentiële dreiging die van hybride conflictvoering uitgaat is dus aanzienlijk te noemen.

Wat kunnen we doen om ons te verdedigen?

De vraag die direct rijst is natuurlijk: wat kunnen we doen om de effecten van hybride conflictvoering tegen te gaan? Daarvoor is een specifieke en een generieke benadering mogelijk.

De specifieke benadering richt zich op de actor. Het draait er daarbij om dat we de tegenstander goed kennen:

- Het kennen van zijn strategische doelstellingen en ambities zorgt ervoor dat wij weten waar hij heen wil. Vanaf dat punt kunnen we de routes die naar deze bestemming leiden identificeren. Deze routes kunnen vervolgens worden versterkt, gemonitord op misbruik of van bypasses worden voorzien.[78]
- Het kennen van zijn sterke en zwakke punten. De tegenstander zal bij voorkeur middelen inzetten en in domeinen opereren waarin hij superioriteit heeft ter compensatie van die domeinen waarin wij superieur zijn. Het kennen van deze sterke en zwakke punten helpt bij het inschatten, voorspellen zo je wilt, van de te gebruiken middelen of het te bespelen domein.
- Het herkennen van hybride conflictvoering is *"connecting the dots"*: het met elkaar in verband brengen van verschillende manifestaties om zo het patroon of de strategie te ontdekken/onderkennen.

De generieke benadering richt zich op onszelf:

- Het kennen van de eigen kwetsbaarheden, want dat zijn de plaatsen waar de tegenstander in eerste instantie zal proberen toe te slaan. Deze kwetsbaarheden kunnen zowel van fysieke/materiele aard zijn; als van immateriële aard.
- Het handelen gericht op het inperken van de mogelijkheden van vreemde mogendheden om misbruik te maken van onze kwetsbaarheden, bijvoorbeeld door het diversifiëren van afhankelijkheden in grondstoffen.
- Het handelen gericht op het reduceren van impact, bijvoorbeeld door zorg te dragen voor analoge redundantie van digitale oplossingen in de vitale processen.
- Het handelen gericht op het wegnemen van de ontvankelijkheid voor informatieoperaties. Bij desinformatie is ontmaskering de eerste stap, omdat het de activiteiten van de tegenstander blootlegt. Maar het hebben van een goed eigen narratief dat structureel en geloofwaardig wordt uitgedragen is belangrijk

78 Een bypass maakt het mogelijk de hoofdroute af te sluiten als de tegenstander zich daarop bevindt, zonder dat wijzelf de toegang tot de 'bestemming' verliezen.

voor het verhogen van de eigen weerbaarheid. De EU/Europese integratie is eigenlijk een geweldige prestatie en toont de kracht van het Westen om via vreedzame middelen tot welvarende en egalitaire samenleving te komen. Dat zou een heel sterk narratief zijn, ware het niet dat dit in het collectieve geheugen is weggezakt. Een internationale inventarisatie kan inzicht geven in welke instrumenten andere landen inzetten om de weerbaarheid te vergroten, denk daarbij aan *public diplomacy*.

Hybride conflictvoering heeft veel weg van schaken: het bereiken van het strategische doel gaat meestal niet via de meest directe weg, maar juist via de weg van de minste weerstand of de minste zichtbaarheid. Net als bij schaken is het van belang het gehele speelbord integraal in het oog te houden en je niet blind te staren op de bewegingen van de individuele stukken.

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

april 2019