Geloofwaardige afschrikking in het cyberdomein?

Nederland moet doorpakken met strategie tegen cyber én hybride conflictvoering

Luitenant-kolonel J.C. Klinkenberg MSc EMSD en tweede-luitenant J.B. Dieker MA*

De Nederlandse *Defensie Cyber Strategie* van 2018 (DCS2018) schenkt opvallende aandacht aan offensieve cybercapaciteiten. De strategie werkt echter niet uit op welke manier die capaciteiten bijdragen aan geloofwaardige afschrikking in het cyberdomein. Door deze onduidelijkheid voor vriend en vijand is het risico op escalatie juist hoger. Dit artikel analyseert de lacunes in de Nederlandse cyberstrategie en betoogt daarnaast dat het probleem breder moet worden aangepakt: veel landen gebruiken cyberoperaties als onderdeel van hybride oorlogvoering, dus een effectieve cyberstrategie moet onderdeel uitmaken van een overkoepelende afschrikkingsstrategie daartegen.

Eind 2018 publiceerde het ministerie van Defensie de nieuwe *Defensie Cyber Strategie*. De strategie viel op vanwege de prominente aandacht voor het thema 'afschrikking [met] geloofwaardige offensieve cybercapaciteiten'.[1] Een gedurfde keuze, die zich onderscheidde van de tot voorheen overwegend *defensieve* toon van het Nederlandse veiligheidsbeleid.[2] Helaas heeft het enthousiasme waarmee deze nieuwe koers werd ingezet nog niet geleid tot een nadere uitwerking van het concept van afschrikking met offensieve cybercapaciteiten, waardoor er voor vriend en vijand veel te raden overblijft wie of wat er precies afgeschrikt moet worden met deze strategie. Bovendien is dit idee van afschrikking — waarbij een tegenstander afziet van een aanval omdat de geanticipeerde vergeldingsaanval die daarop volgt meer kost dan dat de initiële aanval zou opleveren (*deterrence by punishment*)[3] — vooral gericht op het afschrikken van statelijke cyberoperaties met een hoge impact op de nationale veiligheid.[4] Hierdoor blijft het gros van de cyberdreigingen in Nederland buiten schot, terwijl de ernst en omvang van cyberincidenten toenemen.[5] Het probleem is dat Nederland met deze strategie het risico loopt dat vijandelijke voorbereidingen (onder de grens van een gewapend conflict) op mogelijke aanvallen op vitale infrastructuur zich te makkelijk kunnen uitbreiden, omdat er te veel onduidelijkheid is over de grenzen van het

* LtKol J.C. Klinkenberg MSc EMSD werkt bij het Directoraat-generaal Beleid, Directie Operationeel Beleid en Plannen, Afdeling Operationeel Beleid. Daarvoor was hij werkzaam bij het Defensie Cyber Commando. TLt J.B. Dieker MA werkt bij de Bestuursstaf van het Commando Luchtstrijdkrachten en is tewerkgesteld bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dit artikel is geschreven op persoonlijke titel.

1 *Defensie Cyber Strategie 2018* (Den Haag, Ministerie van Defensie, 2018) 8. Zie: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018.

2 Zie bijvoorbeeld de *Nationale Veiligheid Strategie 2019* en de *Notitie Geïntegreerde Buitenland- en Veiligheidsstrategie* (GBVS), die vooral de nadruk leggen op preventie, multilateralisme en de ontwikkeling van een internationaal normatief kader.

3 Glenn H. Snyder, *Deterrence and Defense* (Princeton, Princeton Legacy Library, 1961) 10-12.

4 Met cyberoperaties wordt in dit artikel bedoeld: hoogwaardige cyberaanvallen door statelijke actoren. Met cyberincidenten wordt in dit artikel bedoeld: cyberaanvallen die uiteenlopen in complexiteit en impact, maar die altijd onder de grens van een cyberoperatie liggen.

5 NCTV, *Cybersecuritybeeld Nederland 2019* (Den Haag, Ministerie van Justitie en Veiligheid, 2019). Zie: https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019.

toelaatbare en de mogelijke sancties op het overschrijden daarvan. Daarmee is het fundament van de cyberstrategie — afschrikking op basis van een solide verdediging en digitale weerbaarheid (*deterrence by denial*) — nog steeds het belangrijkste uitgangspunt voor de bescherming van nationale veiligheidsbelangen. Echter, ook op dit punt loopt de uitwerking van de strategie niet in de pas met de snelle ontwikkeling van de dreiging, ondanks positieve ontwikkelingen zoals de onlangs aangekondigde oprichting van de Cyber Intel/Info Cel (CIIC).[6] Met name het uitwerken van rollen en verantwoordelijkheden, het delen van informatie en de beschikbare capaciteit zijn belangrijke aandachtspunten voor de defensieve kant van de cyberstrategie. Defensie moet dus doorpakken met de operationalisering van de huidige strategie, omdat deze tot op heden hooguit in de grondlak staat.

Dit artikel begint met een toelichting op de in de inleiding geschetste lacunes in de *Defensie Cyber Strategie* van 2018. Daarna volgt een korte beschrijving van de toenemende ernst van cyberdreigingen in Nederland, gevolgd door een aantal concrete suggesties die de operationalisering van de afschrikkingsstrategie kunnen verbeteren. Tot slot legt het artikel uit waarom het noodzakelijk is om de strategie van afschrikking niet te beperken tot het cyberdomein. Vijandelijke cyberactiviteiten zijn in toenemende mate onderdeel van strategische, grensoverschrijdende campagnes met een hybride karakter.[7] Om die reden worden de aanbevelingen in dit artikel voorgesteld als onderdeel van een bredere afschrikkingsstrategie tegen hybride conflictvoering.

Een gat tussen beleid en uitvoering

Een bekende uitdaging bij het opstellen van een strategie is dat de inspirerende woorden die op papier staan zich soms niet (snel genoeg) vertalen naar een verdere operationalisering en implementatie van de nieuwe koers. De *Defensie Cyber Strategie* van 2018 (DCS2018) vormt hierop geen uitzondering, zeker als het gaat om het concept van afschrikking. Dit artikel concentreert zich op de 'offensieve' kant van de strategie (deterrence by punishment), maar zoals gesteld in de inleiding kan hetzelfde betoog worden gehouden voor de 'defensieve' kant van de strategie (deterrence by denial). Terwijl uitvoerende eenheden zoals het Defensie Cyber Commando, het Defensie Cyber Security Centrum en de inlichtingen- en veiligheidsdiensten hard werken aan het gereedstellen en inzetten van cybercapaciteiten die invulling geven aan afschrikking met offensieve cybercapaciteiten, blijft de nadere uitwerking van het strategische concept zélf vooralsnog achterwege. Dat is zorgwekkend, omdat Nederland zodoende wel internationaal uitdraagt dat het 'met de grote jongens meedoet', maar niet specificeert

Logo van het Cyber Warfare Team van het Commando Luchtstrijdkrachten FOTO MCD, PHIL NIJHUIS

6 'Diensten krijgen gedeeld kantoor voor aanpak internetdreiging', in: *NRC Handelsblad*, 15 juni 2020. Zie: https://www.nrc.nl/nieuws/2020/06/15/diensten-krijgen-gedeeld-kantoor-voor-aanpak-internetdreiging-a4002910.

7 MIVD, *Jaarverslag 2019* (Den Haag, Ministerie van Defensie, april 2020). Zie: https://www.defensie.nl/downloads/jaarverslagen/2020/04/30/jaarverslag-mivd.

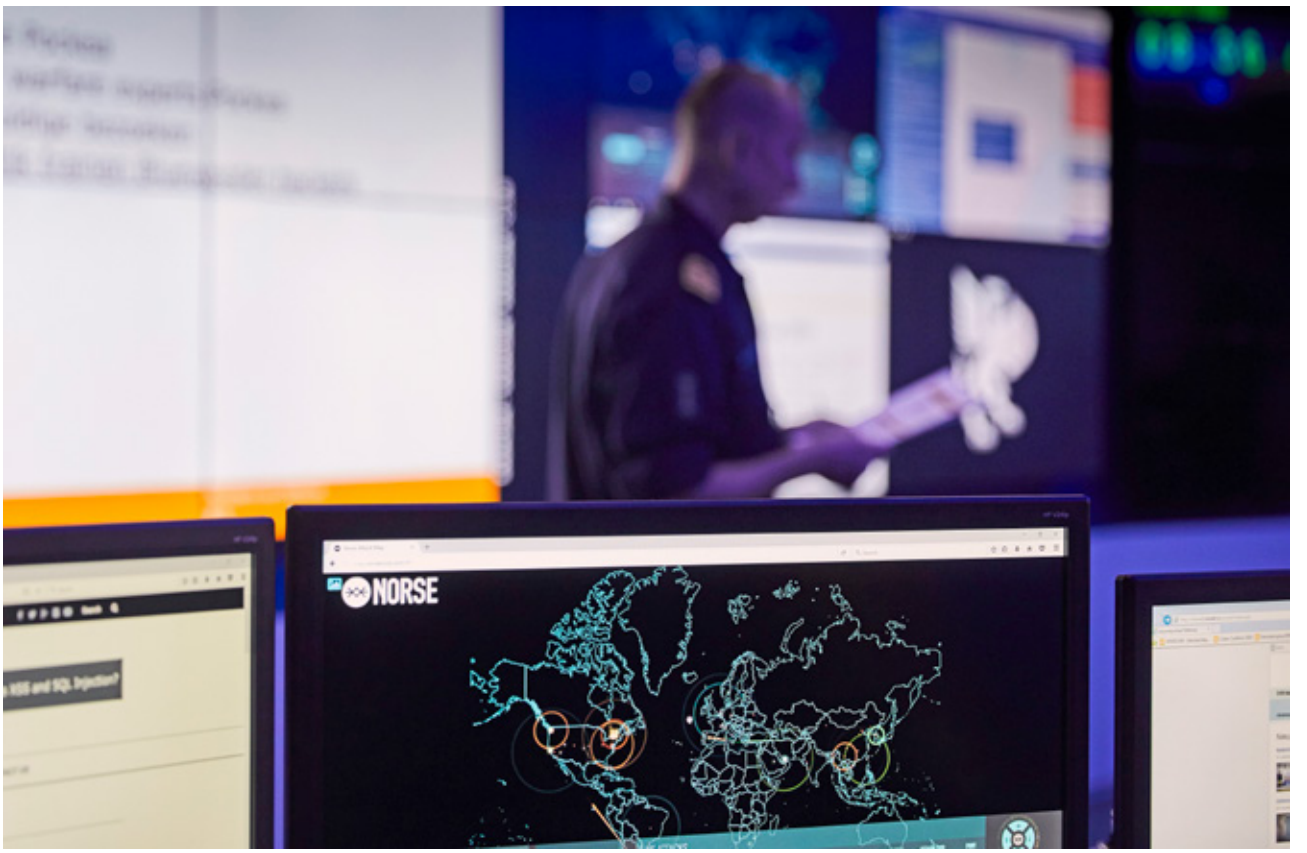

FOTO MCD, PHIL NIJHUIS

NAVO-oefening bij het Defensie Cyber Commando. Door de lacunes in de Nederlandse cyberstrategie weten vriend en vijand niet op welke manier Nederland kan reageren op vijandelijke cyberoperaties

welke tegenstanders en welke activiteiten daarbij in het vizier liggen. Bovendien is nog veel onduidelijk over de wijze waarop offensieve cybercapaciteiten kunnen worden ingezet. Weliswaar wordt ook hieraan gewerkt vanuit verschillende hoeken, maar het ontbreekt aan de geïntegreerde, strategische aanpak die juist zo noodzakelijk is bij het uitwerken van deze complexe materie. Wanneer je deze strategie verder gaat uitwerken moet je uitspraken doen over essentiële vragen, zoals; wie of wat wil ik afschrikken, waarmee, hoe en tegen welke risico's?

Zolang deze vragen niet beantwoord zijn, weten vriend en vijand niet op welke wijze Nederland (al dan niet in bondgenootschappelijk verband) kan reageren op significante vijandelijke cyberoperaties. Deze onduidelijkheid vergroot de kans op *onbedoelde* escalatie, omdat een eventuele Nederlandse vergelding mogelijk wordt opgevat als een buitenproportionele reactie op andermans handelen.

Het grootste probleem is echter dat het uitblijven van de verdere operationalisering afbreuk doet aan de geloofwaardigheid van de strategie, omdat er geen concrete doelen worden gesteld waaraan vervolgens specifieke middelen worden gekoppeld. Potentiële tegenstanders krijgen zodoende weinig tot geen informatie over de Nederlandse offensieve cybercapaciteit, en van de bereidheid om deze in te zetten.[8] Van

8 Michael J. Mazarr et al, *What Deters and Why: Exploring Requirements for Effective Deterrence of Interstate Aggression* (Santa Monica, CA, RAND Corporation, 2018). Zie: https://www.rand.org/pubs/research_reports/RR2451.html.

een afschrikkende werking kan dan nauwelijks sprake zijn, waarmee de DCS2018 mogelijk nooit verder komt dan een ambitieuze intentieverklaring.

Ernst van cyberdreigingen neemt toe

De laatste uitgave van Cybersecuritybeeld Nederland (CSBN2019) beschrijft dat de ernst van cyberdreigingen tegen Nederland niet is afgenomen, integendeel zelfs. Het aantal cyberincidenten neemt jaar op jaar toe, waarbij landen als China, Iran en Rusland omvangrijke cyberprogramma's hebben die (mede) gericht zijn tegen Nederland.[9] Daarbij schuift de grens steeds verder op richting vitale infrastructuur en systemen die de veiligheid en het functioneren van de rechtsstaat waarborgen. Deze toename komt mogelijk mede doordat deze (voorbereidingen op) aanvallen zich allemaal afspelen onder de grens van een gewapend conflict (de zogeheten *grey zone*), waardoor een militaire reactie niet voor de hand ligt. Offensieve cybercapaciteit heeft op die toenemende cyberdreiging in de grey zone mogelijk wel een dempende werking. Dat wil zeggen dat cyberincidenten in de grey zone zich in de toekomst blijven manifesteren, maar dat deze niet zullen escaleren tot cyberoperaties met een hoge impact, omdat potentiële tegenstanders beseffen dat er grenzen zijn die niet overschreden moeten worden.

Een kritische voorwaarde voor deze afschrikkende werking is echter dat die grenzen en de consequenties van het overschrijden daarvan voldoende duidelijk gemaakt zijn, maar dat werk is tot nu toe blijven liggen. Overigens beperkt deze afschrikking zich niet tot militaire middelen, want onder de grens van een gewapend conflict zijn er juist andere machtsinstrumenten die de Nederlandse overheid kan inzetten (deze komen later in het artikel aan de orde). Dit vereist echter wel een interdepartementaal mechanisme om de inzet van deze machtsmiddelen effectief te orkestreren, waaraan het op dit moment nog ontbreekt. Het gevolg is dat Nederland nu meer risico loopt op het gebied van nationale en economische veiligheid, sociale stabiliteit en in zijn onafhankelijkheid van nationale besluitvorming.[10] Deze risico's kunnen en moeten gereduceerd worden, maar dit vraagt wel om een verdere ontwikkeling van de huidige strategie.

Doorpakken met afschrikking

Zoals eerder gesteld: de huidige cyberafschrikkingsstrategie is nog verre van compleet en heeft eerst en vooral behoefte aan een verdere operationalisering. Teneinde het offensieve deel van afschrikking (deterrence by punishment) daarin voldoende terug te laten komen, moet op zijn minst aandacht worden besteed aan de volgende elementen:

1. Vaststellen en bekend maken op welke actoren de afschrikkingsstrategie gericht is;
2. Per actor bekend stellen welke activiteiten/gedrag niet getolereerd zullen worden, zonder in detail te treden over de gestelde grenzen (*thresholds*);
3. Per actor vaststellen welke kwetsbaarheden, waarden en vitale belangen zij hebben en hoe Nederland deze belangen kan aangrijpen of 'onder schot' houden met eigen machtsinstrumenten (DIMEFIL);[11]
4. Vaststellen welke machtsinstrumenten ter beschikking staan en deze ordenen in een nationaal responskader;
5. Vaststellen hoe en onder welke omstandigheden verschillende machtsinstrumenten nationaal en internationaal ingezet kunnen worden, en wie verantwoordelijk is voor de besluitvorming daarover;
6. Onderzoeken in hoeverre Nederland bereid is om de risico's en mogelijke nadelige consequenties van het offensieve deel van de afschrikkingsstrategie te accepteren.

9 *Cybersecurity Beeld Nederland 2019.*

10 *WRR-rapport 101: Voorbereiden op digitale ontwrichting* (Den Haag, Wetenschappelijke Raad voor het Regeringsbeleid, 2019). Zie: https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting.

11 Machtsinstrumenten worden vaak als volgt opgesomd: *diplomatic, information, military, economic, finance, intel, legal/law enforcement* (DIMEFIL).

I. Non-respons, alleen versterken van de eigen verdediging
II. Proactieve cyberoperaties die vijandelijke activiteiten vroegtijdig signaleren en indien nodig aangrijpen (zonder de tegenstander fysieke schade toe te brengen
III. Voorbereiding van toekomstige handelingsopties die erop gericht zijn om vijandelijke kwetsbaarheden, waarden of vitale belangen aan te kunnen grijpen (strategisch plannen)
IV. Diplomatieke protesten
  - Niet-publiek protest richting verantwoordelijke actor
  - Publiek statement, individueel of via internationale organisatie
  - Publieke attributie
  - Blokkeren toegang tot Nederlandse digitale infrastructuur, waarop geen internationale verplichting rust deze beschikbaar te stellen
  - Uitzetting van diplomaten
V. Internationaalrechtelijke toegestane tegenmaatregelen
  - Via een heimelijke of openlijke cyberoperatie uitschakelen van netwerken of systemen die door een ander land worden gebruikt bij een cyberaanval
VI. Juridische maatregelen
  - Aanklagen individuen of organisaties
VII. Politieke en/of economische maatregelen
  - Opleggen reisbeperkingen aan individuen
  - Opleggen economische beperkingen aan individuen, organisatie of staten
  - Publieke informatiecampagne die de offensieve cyberactiviteiten van een tegenstander (internationaal) aan de kaak stelt
VIII. Heimelijke vergelding in het cyberdomein
  - Cyberoperatie die niet publiekelijk bekend wordt gemaakt. Bijvoorbeeld door sabotage van netwerken of systemen die door een ander land worden gebruikt bij een cyberaanval
IX. Openlijke vergelding in het cyberdomein
  - Cyberoperatie die publiekelijk bekend wordt gemaakt
X. Gebruik van militair geweld
  - Gebruik van kinetische en/of niet-kinetische middelen die de tegenstander (fysieke) schade toebrengen. Bijvoorbeeld door het bombarderen van een militaire cybercapaciteit, of het saboteren van militaire systemen en netwerken.

Figuur 1 Nationaal Responskader Cyber (concept)

12 NCTV, *Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig* (Den Haag, Ministerie van Justitie en Veiligheid, 2018) 23. Zie: https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.

13 Zo heeft het Ministerie van Buitenlandse Zaken reeds een diplomatiek responskader ontwikkeld en dit toegepast na de verijdelde aanval op de OPCW in Den Haag, en bestaat er sinds 2017 een *EU Cyber Diplomacy Toolbox*.

14 Sico van der Meer, *State-level responses to massive cyber-attacks: a policy toolbox* (Den Haag, Instituut Clingendael, 2018. Zie: https://www.clingendael.org/sites/default/files/2018-12/PB_cyber_responses.pdf.

Uitwerking van de eerste drie punten komt in de eerste plaats voor rekening van Defensie, maar wel in goed overleg met nationale en internationale partners. Voor een effectieve afschrikkingsstrategie is het immers noodzakelijk om duidelijk en consistent te communiceren op wie deze zich richt, afstemming met partners is daarin cruciaal. Die afstemming kan op nationaal niveau structureel worden ingericht tussen de meest betrokken partijen, een nationaal responskader kan helpen bij de verdere uitwerking daarvan.

Nationaal responskader

Het hierboven genoemde idee om een breed nationaal responskader op digitale aanvallen te ontwikkelen (punt 4) werd eerder al beschreven in de *Nederlandse Cybersecurity Agenda* (NCSA) van 2018: 'Nederland ontwikkelt een breed strategisch kader ten behoeve van respons op digitale aanvallen. Daarin zijn alle beschikbare instrumenten opgenomen, waaronder (publieke) attributie, afschrikking, inzet van offensieve capaciteiten en bredere respons in het cyberdomein. Daartoe versterkt Nederland onder andere de diplomatieke en politieke reactie op verstorende of destructieve cyberoperaties van statelijke actoren.'[12]

Tot nu toe is dit nationale responskader er nog niet gekomen, ondanks inspanningen binnen verschillende departementen om hun aandeel hierin te realiseren.[13] Het vaststellen van een nationaal responskader is niet alleen nuttig om het eigen handelen goed te kunnen orkestreren (punt 5), het is ook bruikbaar als handvat in interdepartementale verkenningen over de offensieve ambities en risicobereidheid binnen de (nationale) cyberstrategie (punt 6). Bovendien kan een responskader dienen als escalatieladder en als hulpmiddel bij het vaststellen van de proportionaliteit van een respons.

Figuur 1 geeft een voorbeeld van hoe een nationaal responskader eruit zou kunnen zien. Dit concept is gebaseerd op een eerder gepubliceerd voorstel van Clingendael-onderzoeker Sico van der Meer, maar aangevuld met elementen die noodzakelijk zijn voor de operationalisering van de afschrikkingsstrategie.[14]

De noodzaak voor een bredere afschrikkingsstrategie

De behoefte aan een uitgewerkte afschrikkingsstrategie geldt niet alleen voor de nationale veiligheidsbelangen in het cyberdomein. Offensieve cyberactiviteiten die gericht zijn tegen Nederland staan namelijk zelden op zichzelf en zijn in toenemende mate onderdeel van bredere strategische campagnes die meerdere landen op de korrel nemen.[15] Bovendien beperken deze cybercampagnes zich niet tot (de toeleveranciers van) Defensie of andere ministeries, maar richten zich ook op vitale sectoren en het verkrijgen van persoonsgegevens en gegevens van andere organisaties, zoals telecomproviders, universiteiten, onderzoeksinstituten, biotechnologiebedrijven, hightechindustrie, handel en startups.[16]

Daarnaast beperken buitenlandse operaties onder de grens van een militair conflict zich niet tot het cyberdomein. Nederland wordt immers regelmatig blootgesteld aan heimelijke politieke beïnvloedingsoperaties, bijvoorbeeld vanuit Rusland.[17] Het voortdurend verspreiden van desinformatie op sociale media is een voorbeeld hiervan, waarbij Rusland de beeldvorming ten aanzien van (bijvoorbeeld) de toedracht van de ramp met vlucht MH17 tracht te beïnvloeden. Een mondiale trend is dat Rusland met doelgerichte informatieoperaties onderwerpen aangrijpt die bij de verschillende doellanden of bondgenootschappelijke organisaties voor verdeeldheid zorgen. Maatschappelijke polarisatie en de versplintering van het politieke landschap in een groot aantal landen spelen Rusland hierbij in de kaart.[18] Naast Rusland maken ook andere landen gebruik van deze tactieken, die zich het beste laten samenvatten als hybride conflictvoering.[19]

Vanwege de sterke samenhang tussen cyber en hybride conflictvoering is het weinig zinvol om separate afschrikkingsstrategieën voor beide onderwerpen na te streven. Temeer omdat landen als Rusland en China in toenemende mate cyberoperaties plannen *als onderdeel* van hun hybride strategie. Gezien de huidige stand van zaken voor zowel de nationale cyberstrategie als de nationale beleidsontwikkeling op het gebied van *counter-hybrid*, is ons advies om hier de krachten te bundelen bij het verder ontwikkelen en operationaliseren van een brede afschrikkingsstrategie. Een eerste aanzet hiertoe is reeds verwoord in de Kamerbrief 'Tegengaan statelijke dreigingen', waarin de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) spreekt over een 'integrale aanpak'.[20] In de kern beschrijft deze aanpak dat *connecting the dots* van essentieel belang is, zowel bij het kijken naar statelijke dreigingen als bij het formuleren van tegenmaatregelen.

De voorgestelde brede afschrikkingsstrategie moet zich vervolgens niet beperken tot een zuiver nationale focus, omdat internationale samenwerking vaak de enige manier is om succesvol op te treden tegen steeds beter georganiseerde hybride operaties.[21] Samenwerking en solidariteit tussen landen en binnen bondgenootschappelijke organisaties zoals de NAVO en de EU versterken het afschrikkende effect, niet in de laatste plaats omdat het doel van de tegenstander veelal is om deze solidariteit te ondermijnen.

Andere overwegingen zijn om de huidige rolverdeling en informatie-uitwisseling tussen overheid, inlichtingendiensten en private actoren tegen het licht te houden en op zoek te gaan naar meer effectieve vormen van samenwerking. Daarbij is het de moeite waard om te kijken naar strategische partnerlanden als het Verenigd Koninkrijk, Denemarken of Frankrijk, die

15 Richard J. Harknett en Max Smeets, 'Cyber campaigns and strategic outcomes', in: *Journal of Strategic Studies* 43 (2020) (4 maart 2020). Zie: https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354.

16 AIVD, *Jaarverslag 2019* (Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, april 2020).

17 AIVD, *Jaarverslag* 2019.

18 Ibidem.

19 Hieronder wordt in dit artikel verstaan: 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.

20 NCTV, Kamerbrief 'Tegengaan statelijke dreigingen' (Den Haag, Ministerie van Justitie en Veiligheid, 18 april 2019) 2.

21 Vytautas Keršanskas, *Deterrence: Proposing a more strategic approach to countering hybrid threats* (Helsinki, Hybrid Centre of Excellence, 9 maart 2020). Zie: https://www.hybridcoe.fi/wp-content/uploads/2020/06/Deterrence_public.pdf.

mogelijk beter zijn georganiseerd in hun brede aanpak van cyber en hybride conflictvoering.

Tot slot heeft het weinig zin om te spreken over een strategie van afschrikking, zolang er niet voldoende is nagedacht over de implicaties en mogelijke consequenties daarvan. Geloofwaardige afschrikking betekent immers dat je als land bereid bent om de tegenstander pijn te doen, om te escaleren, en om zelf te incasseren. Daarnaast loopt het concept van afschrikking wellicht tegen zijn grenzen aan wanneer het gaat om vijandige activiteiten die zich afspelen onder de grens van een gewapend conflict. Hier ligt, naast een betere verdediging, mogelijk een meer prominente rol voor het vroegtijdig verstoren van tegenstanders. De Verenigde Staten proberen dit sinds 2018 met *Defend Forward*,[22] waarmee potentiële dreigingen tegen Amerikaanse militaire (industriële) belangen en digitaal geweldgebruik proactief worden aangegrepen. In de verdere uitwerking van deze strategie stellen de Amerikanen dat zij voortaan niet wachten tot een cyberaanval plaatsvindt, maar dat zij actief gaan jagen op hun tegenstanders.[23] Door vroegtijdig te signaleren en te verstoren probeert het U.S. Cyber Command (USCyberCom) een aanval in de kiem te smoren, waarbij zelfs niet geschuwd wordt om in te breken op systemen die op het grondgebied van bondgenoten staan, als deze door een tegenstander gebruikt worden.[24] Deze strategie neemt overigens geen afscheid van het concept van afschrikking, maar vult dit juist aan met vroegtijdige verstoring in de grey zone omdat afschrikking daar niet effectief blijkt te zijn.

FOTO NAVO

Secretaris-generaal van de NAVO Jens Stoltenberg spreekt tijdens de Conference on the Cyber Defence Pledge in Frankrijk. Een brede afschrikkingsstrategie moet zich niet beperken tot een nationale focus, omdat internationale samenwerking de kans op succes tegen hybride operaties vergroot

De vrijheid die de Amerikanen nemen om in andermans systemen op zoek te gaan naar de *bad guys* schuurt met de soevereiniteit van staten. De VS gaat zelfs nog een stap verder, door zich ook te nestelen in de vitale infrastructuur van potentiële tegenstanders. Een prominent voorbeeld hiervan is de berichtgeving over de Amerikaanse aanwezigheid in het Russische elektriciteitsnetwerk.[25] De boodschap is helder: 'wat jullie kunnen, kunnen wij ook'. Bovendien stelt USCyberCom glashelder dat het streeft naar *cyberspace superiority*.[26] Dit betekent dat er in cyberspace altijd een dusdanig overwicht is dat de eigen troepen hun operaties adequaat kunnen uitvoeren. Volgens onderzoekers Michael Fischerkeller en Richard Harknett is het uiteindelijke doel van USCyberCom om zijn tegenstanders te laten inzien welk gedrag acceptabel is, en wanneer die grens overschreden wordt.[27] Het idee, aldus de onderzoekers, is dat op deze wijze in de grey zone op langere termijn duidelijke internationale normen

22 U.S. Department of Defense, *Department of Defense Cyber Strategy 2018* (Washington, D.C., U.S. DoD, 2018). Zie: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

23 U.S. Cyber Command, *Command Vision for US Cyber Command, Achieve and Maintain Cyberspace Superiority* (Fort Meade, U.S. Cyber Command, 2018). Zie: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

24 Ellen Nakashima, 'U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies', in: *The Washington Post*, 9 mei 2017. Zie: https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.

25 David A. Sanger en Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', in: *The New York Times*, 15 juni 2019. Zie: https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

26 *Command Vision for US Cyber Command, Achieve and Maintain Cyberspace Superiority.*

27 Michael P. Fischerkeller en Richard J. Harknett, 'Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace', *Lawfare* (9 november 2018). Zie: https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

FOTO U.S. ARMY CYBER COMMAND, STEVEN STOVER

Amerikaanse militairen van een Expeditionary Cyberspace Electromagnetic Activities-team oefenen in Indiana. De VS streeft naar cyberspace superiority, zodat de eigen troepen hun operaties adequaat kunnen uitvoeren

ontstaan voor het gebruik van cyberspace,[28] al dan niet afgedwongen door de Amerikaanse overmacht daarin. De nieuwe Amerikaanse koers is in Nederland niet onopgemerkt gebleven en biedt stof tot nadenken.[29]

Dit zijn allemaal zaken die vooraf goed onderzocht moeten worden, en die je bijvoorbeeld kunt uitwerken met behulp van scenario's en *war games*. Alleen dan kom je tot het inzicht wat de gekozen strategie betekent en wat er allemaal 'geregeld' moet zijn om daadwerkelijk effect te kunnen sorteren. Dit geoperationaliseerde strategische denken – of strategische cultuur – is de grote afwezige in debatten en beleidsontwikkeling ten aanzien van onze nationale veiligheid.

Samenvattend kunnen de zes eerder beschreven elementen breder worden getrokken naar een afschrikkingsstrategie die zowel nationaal als internationaal inzet op samenwerking tussen overheden, organisaties en private actoren. Deze beweging dient echter hand in hand te gaan met een strategische dialoog die recht doet aan het machtspolitieke speelveld waarin Nederland zich daarmee in toenemende mate begeeft, en de mogelijke consequenties die daaruit volgen.

Ter afsluiting

Dit artikel doet een concrete aanzet om de huidige cyberstrategie, en met name de operationalisering daarvan, op een hoger plan te tillen. Idealiter wordt deze 'strategie-upgrade' meteen naar een bredere scope getrokken, met prominente aandacht voor het afschrikken van hybride conflictvoering. Sterker nog, cyberafschrikking moet eigenlijk gezien worden als een junior partner van hybride afschrikking, parallel aan hoe onze niet-westerse rivalen het positioneren. Het meest belangrijke is echter dat er een interdepartementale dialoog op gang komt waarin meer aandacht komt voor de implicaties van de snel veranderende veiligheidsomgeving, en hoe Nederland daar adequaat mee omgaat. ■

28 Fischerkeller en Harknett, 'Persistent Engagement and Tacit Bargaining'.

29 Robert Chesney, Max Smeets, en Monica Kaminska, 'A Transatlantic Dialogue on Military Cyber Operations', *Workshop Report*, University of Texas at Austin, (Amsterdam, 13 augustus 2019). Zie: https://www.lawfareblog.com/workshop-report-transatlantic-dialogue-military-cyber-operations-amsterdam.