Persistent Engagement

De nieuwe cyberstrategie voor Nederland?

Majoor M.C.P.J. Smits EMSD en kolonel dr. B.M.J. Pijpers *

'Cyber warriors are not just loitering in their barracks, and their capabilities are not sitting in the arsenals awaiting some future war. They are constantly engaged in offensive, defensive and espionage operations'.[1]

Nederland is dagelijks slachtoffer van cyberaanvallen door entiteiten al dan niet behorend bij een buitenlandse staat. Maar ondanks de kwaadwillende intenties zijn deze 'aanvallen' veelal niet gewelddadig; van een gewapend conflict is zeker geen sprake. De vraag vanuit de krijgsmacht is hoe hiertegen op te treden. Andere landen, zoals de Verenigde Staten, hebben al een antwoord door op proactieve wijze, buiten het eigen grondgebied de potentiële gevaren in de kiem te smoren. Is dit ook voor Nederland een optie? Het recent gepubliceerde coalitieakkoord lijkt hier reeds een opening voor te geven. Buiten de vaak juridische of ethische appreciatie van dit controversiële vraagstuk gaat dit artikel in op de Amerikaanse doctrine van Persistent Engagement en de vraag of dit concept past in de Nederlandse strategische cultuur.

In navolging van de Verenigde Staten heeft ook het Verenigd Koninkrijk recentelijk zijn eigen cybereenheid opgericht, de National Cyber Force.[2] Ook Nederland heeft al sinds enige tijd het Defensie Cyber Commando (DCC). De vraag is echter niet of er een cybereenheid is, maar vooral hoe deze eenheden hun taken invullen.[3]

De door de VS gehanteerde doctrine van 'Persistent Engagement' (PE)[4] of 'defend forward' is erop gericht om cyberaanvallen niet pas aan te grijpen op het moment van impact, maar proactief de inzet of zelfs de ontwikkeling van cybercapaciteiten te neutraliseren, om te voorkomen dat de opponent de aanval uitvoert.[5] Op vergelijkbare wijze zijn ook andere landen actief: vermoedelijk zijn dat landen als China, Rusland, Iran, maar ook Israël en het eerdergenoemde VK lijken deze proactieve kant op te gaan.[6] De PE-doctrine suggereert dat tussen deze landen een stilzwijgende overeenstemming bestaat om elkaar op assertieve wijze de loef af te steken en daarmee gedragsnormen in cyberspace te creëren;[7] deze wijze van optreden heet daarom ook wel 'agreed competition'.[8]

* Majoor (KL) Michael Smits EMSD is geplaatst bij de Defensiestaf, Directie Internationale Militaire Samenwerking van het ministerie van Defensie. Kolonel (KL) dr. Peter Pijpers is universitair hoofddocent Cyber Operations bij de Faculteit Militaire Wetenschappen aan de NLDA. Dit artikel is gebaseerd op de HDV-thesis van majoor Smits. De auteurs danken luitenant-kolonel (KLu) Ferry Oorsprong voor zijn reflecties.

1 Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', in: *Journal of Cybersecurity* 5 (2019) (1) 5.

2 Joe Devanny en Tim Stevens, 'What Will Britain's New Cyber Force Actually Do?', *War On The Rocks* (2021). De Britse National Cyber Force is, anders dan de Amerikaanse tegenhanger, geen zogeheten *unified command*, maar ressorteert onder zowel het ministerie van Defensie als het ministerie van Buitenlandse Zaken.

3 Max Smeets, 'NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis', in: T. Minárik et al (ed.), *Silent Battle*, (Tallinn, NATO CCD COE, 2019) 168-173; Julia Voo et al., 'National Cyber Power Index 2020' (2020) 26-49.

4 United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority' (2018).

5 Een aanval in de context van dit artikel is geen 'gewapende aanval', maar slaat op een aanval in cyberspace, zoals onder andere verwoord in de Amerikaanse doctrine: 'Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves', U.S. Department of Defense, 'Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (As Amended Through 15 January 2016)' (2007) 111.

6 Robert Chesney, 'Adapting to the Cyber Domain: Comparing U.S. and U.K. Institutional, Legal and Policy Innovations', *Aegis Series Paper*, nr. 2103 (mei 2021).

7 Michael P. Fischerkeller en Richard J. Harknett, 'Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace', *Lawfare*, 2018.; Louk L.C. Faessen en Deborah Lassche, 'Persistent Engagement in Het Cyberdomein: Stabilisatie of Escalatie?', in: *Militaire Spectator* 189 (2020) (12) 636–47.

8 Michael P. Fischerkeller en Richard J. Harkanett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', *Institute for Defense Analysis* (2018).

Is Persistent Engagement, proactief cybergevaren in de kiem smoren, geschikt als strategie voor Nederland? FOTO DARPA

Ook Nederland realiseert zich dat een afwachtende houding bij cyberaanvallen niet per se de beste strategie is. Zo is de *Geïntegreerde Buitenland- en Veiligheidsstrategie* (GBVS),[9] maar ook de *Defensie Cyberstrategie* (DCS)[10] geënt op het voorkomen van cyberdreigingen door capaciteiten te versterken en de verdediging op orde te hebben. Nederland geeft in de GBVS aan te investeren in de internationale rechtsorde, 'mede omdat dit een vorm van *forward defense* is.'[11] Ook de DCS van 2013 houdt de mogelijkheid open dat 'offensieve middelen worden ingezet om een cyberaanval te voorkomen of af te slaan en de vrijheid van het eigen militair optreden in het digitale domein te waarborgen («actieve verdediging»)';[12] al met al een respons die niets te wensen overlaat.

De bewoordingen uit de GBVS of DCS bijten dus op het eerste gezicht niet met de proactieve houding uit de PE-doctrine. PE is ontwikkeld omdat het gros van de cyberaanvallen – die op ernstige wijze inbreken op de interne aangelegenheden van de VS – plaatsvindt onder het niveau van geweld en afkomstig is van buitenlandse actoren. Een gebied waar,[13] buiten de inlichtingendiensten, zowel de krijgsmacht als de nationale politiële of justitiële agentschappen niet van nature een mandaat hebben om op te treden.

Vooralsnog neemt Nederland dan ook nog geen assertieve houding aan om deze gevaren te mitigeren. Dit thema – het inzetten van machtsmiddelen in het buitenland onder het niveau van geweld – is controversieel, en levert veel juridische en ethische bezwaren op.[14]

9 Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland: Geïntegreerde Buitenland- En Veiligheidsstrategie 2018-2022' (2018) 19.
10 Ministerie van Defensie, 'Defensie Cyber Strategie 2018 - Investeren in Digitale Slagkracht' (2018) 6.
11 Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland', 38.
12 Handelingen van de Tweede Kamer 2011-2012, '33 321, Nr.1, Defensie Cyber Strategie; Brief Regering' (2012) 7.
13 Willemijn A. Bos en Peter B.M.J. Pijpers, 'Cyberoperaties in de Gray Zone - Juridische Overwegingen Omtrent de Rol Voor de Krijgsmacht', in: *Militaire Spectator* 190 (2021) (10) 519-521.
14 Max Smeets, 'US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection', in: *Intelligence and National Security* 35 (2020) (3) 444–53; Robert Chesney, 'The Domestic Legal Framework for US Military Cyber Operations', *Hoover Institution Aegis Paper* (2020).

FOTO INTERNATIONAAL STRAFHOF

Jaarlijkse vergadering van de verdragspartijen van het Internationaal Strafhof in Den Haag. Nederland investeert in de internationale rechtsorde, 'mede omdat dit een vorm van forward defense is'

Maar die constatering neemt de dreiging niet weg. De vraag is dan ook of Nederland niet een meer proactieve strategie tegen cyberaanvallen zou moeten omarmen,[15] of zelf PE zou moeten adopteren. Of zijn er, los van juridische en ethische overwegingen,[16] andere redenen waarom PE al dan niet past bij de Nederlandse context, zoals de strategische cultuur? Wells beschreef constanten in het Nederlandse buitenlandse beleid, zoals: het ontbreken van belangstelling om het territorium te vergroten; de desinteresse in het militaire bedrijf; en een voorkeur voor afzijdigheid en neutraliteit.[17] Het laatste komt tot uiting in de grote waarde die Nederland, als klein land, hecht aan een goed werkend internationaal rechtssysteem.[18] De constanten van het Nederlandse buitenlands beleid zijn pakkend samen te vatten in Joris Voorhoeves driewerf 'peace, profits and principles'.[19]

De vraag in dit artikel is dan ook, gelet op de GBVS en de DCS: 'In hoeverre past Persistent Engagement in cyberspace binnen de Nederlandse strategische cultuur?'

15 Diederik de Groot, 'Moet de Cyberaanval Onze Cyberverdediging Worden?', *BNR Podcast* (2021).

16 Jack Goldsmith en Alex Loomis, "'Defend Forward' and Sovereignty", *Aegis Series Paper*, nr. 2102 (2021) 15.

17 Aldus geparafraseerd uit: Yvonne Kleistra, 'De Constantenthese in de Studie van Het Nederlands Buitenlands Beleid', *B En M* 27, nr. 2 (2000) 103–11, 109.

18 Zie ook Andre Nollkaemper, 'Handel Naar Het Internationaal Recht En Erken de Staat Palestina', *NRC Handelsblad* (2021). Prof Nollkaemper geeft aan dat 'de stabiliteit van de internationale samenleving en de bescherming van de belangen van burgers wereldwijd hangt op een voortgaand respect voor een fragiel rechtssysteem. Internationaal recht is imperfect, maar het is het enige werkelijk wereldwijd aanvaarde normatieve kader waarop we ons met gezag kunnen beroepen'.

19 Joris J. C. Voorhoeve, *Peace, Profits and Principles: A Study of Dutch Foreign Policy* (Den Haag, Martinus Nijhoff, 1979).

Het toetsingskader van dit artikel – de strategische cultuur – wordt geoperationaliseerd door middel van een model van Alastair Johnston. Hierna beschrijven wij daarom eerst de kernelementen van strategische cultuur op basis van het model van Johnston. Daarna volgen de beschrijving van PE en de Nederlandse strategische cultuur, die we respectievelijk duiden met behulp van Johnstons kernelementen.

Strategische cultuur: het model van Johnston

Om de militaire (nucleaire) strategie van de Sovjet-Unie te kunnen interpreteren, introduceert Jack L. Snyder in de jaren '70 het begrip 'strategische cultuur',[20] waarbij hij de link legt tussen de cultuur en de politiek van een land binnen de moderne veiligheidsstudies. De cultuur van een land heeft unieke kenmerken, die direct of indirect te relateren zijn aan de historische en politieke context.

Vele, vaak contrasterende publicaties aangaande strategische cultuur volgen. Reden voor Johnston om de verschillende publicaties te groeperen.[21] Hij omschrijft de evolutie van de theorie van strategische cultuur aan de hand van drie generaties. De eerste generatie, van onder meer Snyder, legt vooral de nadruk op het belang van strategisch en cultureel relativisme,[22] in tegenstelling tot de onderzoeken van voor de jaren '70, die zich richtten op een rationele en technische benadering van strategie. De historische context is van wezenlijk belang voor het vormen van de cultuur. Snyder constateert dat 'historical processes that are particular to a specific country form a perceptual lens through which strategic issues are processed and thereby affect policy choices'.[23] Een veelgehoord punt van kritiek op de werken van deze eerste generatie is dat zij het fenomeen strategische cultuur niet konden operationaliseren,[24] waardoor het onbruikbaar was om landen te vergelijken.[25] De tweede generatie richt zich daarom initieel op de meer concrete militaire doctrine, en de relatie met hedendaagse sociale normen en waarden; zij legt minder de nadruk op de historische context.[26] Dit levert frictie op met de eerste generatie, waardoor een academisch discours ontstaat met als gevolg dat de tweede generatie zich vooral kenmerkt door het debat over waar strategische cultuur nu uit bestaat, en minder over de specifieke strategische cultuur van een land. De derde generatie grijpt enerzijds terug op de historische context van de eerste generatie, maar bouwt deze tegelijkertijd verder uit.[27] Deze generatie legt bij het duiden van de strategische cultuur, naast het belang van de historische context, ook de nadruk op recente ervaringen van de civiele elite binnen een land. Ook de derde generatie richt zich op de dynamiek van het veiligheidsbeleid, maar beperkt zich er niet toe.

Johnston ontwikkelt binnen deze derde generatie een raamwerk waardoor strategische cultuur wel kan worden getoetst.[28] Johnston hanteert hierbij drie 'basic assumptions about the orderliness of the strategic environment':[29] (1) *Frequency of conflict in human affairs* (de rol van oorlog in menselijke aangelegenheden); (2) *Zero-sum nature of conflict* (de aard van de tegenstander en de dreiging die deze vormt); en (3) *Efficacy of violence* (de effectiviteit van het gebruik van geweld). Afhankelijk van de overheersende perceptie ten aanzien van deze variabelen zal een land meer een strategische cultuur van harde *realpolitik* of zachte *idealpolitik* hanteren (zie Figuur 1).

20 Jack L. Snyder, 'The Soviet Strategic Culture: Implications for Limited Nuclear Operations', *Rand Corporation R-2154-AF* (1977) 8-9.

21 Alastair Ian Johnston, 'Thinking about Strategic Culture', in: *International Security* 19 (1995) (4) 32–64, 36.

22 Snyder, 'The Soviet Strategic Culture', 9; Johnston, 'Thinking about Strategic Culture', 36-39.

23 Kerry Longhurst, 'The Concept of Strategic Culture', in *Military sociology; The Richness of a Discipline* (2000), 301-310.

24 Rashed Uz Zaman, 'Strategic Culture: A "Cultural" Understanding of War', in: *Comparative Strategy* 28 (2009) (1) 68–88, 76.

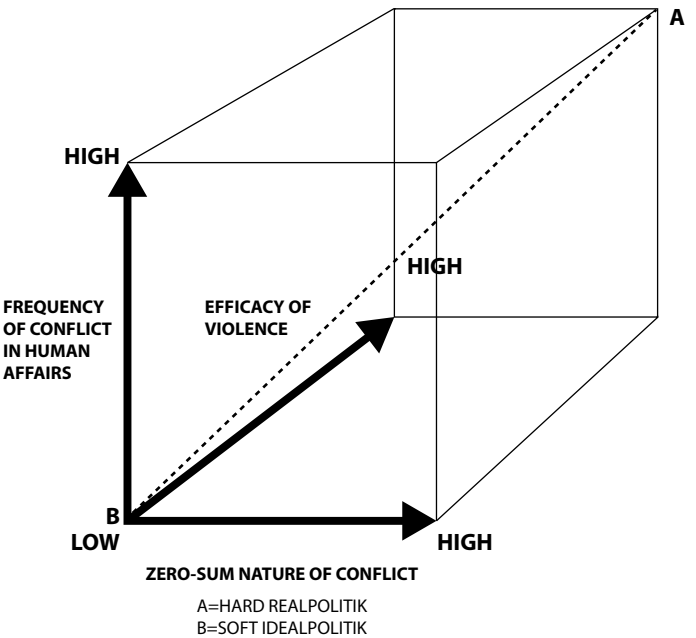
25 Jeannie L. Johnson, Kerry M. Kartchner, en Jeffrey A. Larsen, *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights into Comparative National Security Policymaking, Initiatives in Strategic Studies: Issues and Policies* (New York SE, Palgrave Macmillan, 2009) 33-54.

26 Uz Zaman, 'Strategic Culture', 77-78; Johnston, 'Thinking about Strategic Culture', 39-41.

27 Johnston, 'Thinking about Strategic Culture', 41-43.

28 Ibidem, 44-49. Het raamwerk van Johnston is niet vrij van kritiek. Zie onder andere Uz Zaman, 'Strategic Culture', 82-83.

29 Johnston, 'Thinking about Strategic Culture', 46. Johnston noemt deze drie respectievelijk: *the frequency of conflict, the nature of conflict;* en de *efficacy of violence.*



Figuur 1 The central paradigm of a strategic culture[30]

De eerste variabele – Frequency of conflict in human affairs – behelst de opvatting van een actor (staat) over het begrip conflict en oorlog binnen het internationale systeem.[31] Kort gesteld laat deze variabele zien of de actor oorlog ziet als onvermijdelijk of als een afwijking ten opzichte van het normale. Wanneer een actor oorlog ziet als een onvermijdelijke interactie tussen staten, dan is 'strijd' een instrument om conflicten op te lossen. Wanneer de actor oorlog als een keuze ziet en het daarmee classificeert als 'te voorkomen', zal oorlog niet direct onderdeel uitmaken van diens strategie. De tweede variabele – Zero-sum nature of conflict – geeft aan in hoeverre een land wil samenwerken met een ander land. Dit is te karakteriseren als een 'zero-sum' of een 'variable-sum game'. Bij deze tweedeling, afkomstig uit de *game theory,* houdt de 'zero-sum'-benadering in dat winst van de ene speler per definitie verlies van de andere speler tot gevolg heeft en samenwerking dus weinig zal opleveren. Bij 'variable-sum' hoeft winst van de ene speler niet noodzakelijk tot verlies bij de andere speler te leiden. Er is een keuze om te strijden tegen een opponent of ermee samen te werken; beide opties kunnen een gunstig resultaat tot gevolg hebben. De derde variabele – Efficacy of violence – geeft de relatie weer tussen het gebruik van geweld en diplomatie.[32] Hierbij beziet een actor of gebruik van geweld een waardevol instrument is dat voordelen biedt in bepaalde scenario's, of dat de actor gebruik van geweld slechts ziet als een laatste redmiddel.

Persistent Engagement

Persistent engagement is sinds 2018 de dominante cyberdoctrine van het Amerikaanse Cyber Command (USCYBERCOM).[33] 'Superiority through persistence seizes and maintains the initiative in cyberspace by continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver", aldus de visie van het USCYBERCOM. PE positioneert zichzelf daarmee 'seamlessly between defense and offense across the interconnected battlespace.'[34]

De VS heeft gekozen voor PE gezien eerdere pogingen om de veelvoorkomende aanvallen in cyberspace tegen te gaan zijn mislukt. Omdat het gaat om aanvallen onder het niveau van geweld heeft de VS zijn opponenten in eerste instantie willen 'afschrikken' door middel van afstraffingen in andere domeinen dan cyberspace, bijvoorbeeld door economische sancties.[35]

30 Ibidem, 47.

31 Een kanttekening bij deze variabele is dat Johnston een eerder dichotome perceptie heeft van oorlog en vrede, terwijl dit in de hedendaagse hybride conflicten of in de *gray-zone & multi domain competition* wellicht minder binair van toepassing is.

32 Voor 'use of force' in een cybercontext, zie onder andere Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', in: *Columbia Journal of Transnational Law* 37 (1999) (3) 885–938, 935.

33 Het USCYBERCOM is sinds 2018 een volwaardig *combatant command*, dat wil zeggen een militair commando van het Amerikaanse ministerie van Defensie op strategisch niveau dat bestaat uit eenheden afkomstig van twee of meer krijgsmachtdelen van de Amerikaanse strijdkrachten. Dit commando valt rechtstreeks onder de Amerikaanse minister van Defensie.

34 United States Cyber Command, 'Achieve and Maintain Cyberspace Superiority', beide citaten, 6.

35 In de strategie van 2011 spreekt de VS over: 'effective law enforcement; internationally agreed norms of state behavior; measures that build confidence and enhance transparency; active, informed diplomacy; and appropriate deterrence' als middelen om risico's in cyberspace te mitigeren. The White House, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (2011), 9.

FOTO U.S. AIR FORCE, J.M. EDDINS JR.

Amerikaanse militairen visualiseren cyberdreigingen. Amerikaanse cybereenheden zijn geen response force, maar voeren constant en preventief offensieve cyberoperaties uit

Daarnaast nam de VS sinds 2004 deel aan de VN-gesprekken in de 'UN Group of Governmental Experts' (UN GGE) om te komen tot gedeelde gedragsnormen en juridische kaders in cyberspace.[36] De voortgang bij deze processen is echter traag en de UN GGE kan regelmatig niet tot overeenstemming komen, zoals ook in 2017.[37] Het UN GGE platform vormde dus ook geen oplossing voor de acute problemen veroorzaakt door cyberaanvallen tegen de VS.

De VS concludeerde dat 'afschrikking' wel effectief was in het land-, lucht- en zeedomein, maar blijkbaar geen effect had in cyberspace, zoals ook Fischerkeller en Harknett krachtig verwoorden in hun artikel 'Deterrence is not a credible strategy for cyberspace.'[38] Healey maakt daarbij nog de nuance dat cyber-*deterrence* kan werken in een situatie van gewapend conflict, maar niet onder het niveau van 'death and destruction'.[39]

Rond 2017 treedt daarom een koerswijziging op. De idee is dat eigenschappen van cyberspace dusdanig afwijkend zijn van andere domeinen, dat de klassieke deterrence-doctrine minder effectief is.[40] De VS gaat daarom op zoek naar een meer geschikte doctrine binnen het cyberdomein die ook aanvallen onder het niveau van geweld kan tegengaan. Vanuit die optiek is PE eerder te

36 De UN GGE kende sinds 2004 zes iteraties waarbij in 2010, 2013, 2015 en ook dit jaar een zogeheten consensus-rapport is verschenen. Zie: United Nations GGE 2021 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - 6th 2021', *Advance Copy* (mei 2021).

37 Eneken Tikk and Mika Kerttunen, 'The Alleged Demise of the UN GGE: An Autopsy and Eulogy', *Jyväskylä: Cyber Policy Institute* (2017).

38 Michael P. Fischerkeller en Richard J. Harknett, 'Deterrence Is Not a Credible Strategy for Cyberspace', in: *Orbis* 61 (2017) (3) 381–93, 381-385.

39 United States House of Representatives Committee on Armed Services, 'Cyber Warfare in the 21st Century: Threats , Challenges, and Opportunities' (2017) 76.

40 Denk daarbij aan eigenschappen als snelheid, bereik, penetratiegraad maar ook de grenzenloosheid en dominantie van private actoren (Silicon Valley) in dit domein.

vergelijken met digitale sancties, of zelfs een soort 'anticipatory self-defence', maar dan onder het niveau van geweld. Het idee is om ervoor te zorgen dat de opponent zijn (op handen zijnde) aanval niet kan uitvoeren: een idee waarin elementen van *deterrence by denial* naar voren komen.[41] Het loslaten van het deterrence-denken blijkt lastig. De *National Cyber Strategy* van 2018 verwoordt dat de VS de mogelijkheid openhoudt 'to impose costs (…) to deter malign cyber actors',[42] maar dan onder het niveau van geweld.[43] Ook de PE-doctrine zelf verwijst naar het klassieke deterrence-denken wanneer het teruggrijpt op de idee van 'tacit bargaining'.[44] Hierin onderhandelen actoren niet op basis van multilaterale diplomatieke onderhandelingen, maar door middel van unilaterale acties of manoeuvres waar de opponent de intentie uit moet afleiden. PE is volgens Healey dan ook simpelweg een spiegelbeeld van wat de tegenstanders al in cyberspace doen.[45]

Met de PE-doctrine laat de VS zien dat het land kiest voor een proactieve houding waarbij het aanhoudend optreedt onder de drempel van het gebruik van geweld om de tegenstander proactief te verstoren. Dit betekent dat de VS ook buiten zijn eigen cybernetwerken en grenzen optreedt om het signaal af te geven dat inmenging in Amerikaanse binnenlandse aangelegenheden onacceptabel is, ook in cyberspace. De VS schroomt daarbij niet om elk netwerk te betreden waarin een vijandelijke actor controle heeft over een node. Het kan hierbij ook om Nederlandse netwerken met Russische aanwezigheid gaan en dus niet alleen om de netwerken in Rusland zelf.[46]

Ondanks deze proactieve houding van PE beschouwt de VS deze doctrine nog steeds als een vorm van verdedigen, en niet aanvallen: 'defending forward is nothing more than being active in your defense, just like the DoD has always done; fight forward, disrupt forward, deny forward'.[47] Deze houding is bij veel landen onverkort terug te vinden in de benadering van bedreigingen in de fysieke wereld; het deelnemen aan vredesmissies en crisisbeheersingsoperaties is daarmee vergelijkbaar met forward defense, om zo brandhaarden in de kiem te smoren.[48] Echter, ondanks de eufemistische bewoordingen van PE beperkt deze doctrine zich in onze ogen niet enkel tot verdedigen. USCYBERCOM kan door middel van PE altijd en overal in cyberspace 'manoeuvreren' om de dreiging tegen te gaan;[49] niet alleen door reactief terug te hacken, netwerken plat te leggen waarmee vermeende (cyber)terroristen onderling communiceren of betaalverkeer stop te zetten. Wanneer USCYBERCOM namelijk vermoedt dat een mogelijke tegenstander acties onderneemt in cyberspace, gericht tegen de VS, dan acteert het daarop. Sterker nog, Paul Nakasone, Commandant USCYBERCOM, heeft aangegeven geen *response force* meer te zijn, maar een eenheid die constant bezig is met het uitvoeren van (cyber)operaties onder het niveau van geweld.[50] Het is niet gezegd dat het offensief nemen en continu acties ontplooien het gedrag van de tegenstander direct zal veranderen. Het maakt het echter wel 'far more difficult for them to advance their goals over time', en dat stelt het USCYBERCOM in staat 'to degrade the capabilities our adversaries use to conduct attacks'.[51]

41 Michael J Mazarr, 'Understanding Deterrence', in: Frans P.B. Osinga en Tim Sweijs (red.), *Deterrence in the 21st Century - Insights from Theory and Practice: NL ARMS Netherlands Annual Review of Military Studies 2020* (2020) 14–27, 15.

42 Executive Office of the President of the United States, 'National Cyber Strategy of the United States of America', (september 2018) 2.

43 Fischerkeller en Harknett, 'Persistent Engagement and Tacit Bargaining'; Alexander Klimburg, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', in: *Survival* 62 (2020) (1) 107–30, 112-114.

44 Thomas C. Schelling, *The Strategy of Conflict*, *Harvard University Press*, 1980 ed (Cambridge, Mass, Harvard University Press, 1960) 53-54.

45 Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', 5-6.

46 Faessen and Lassche, 'Persistent Engagement in Het Cyberdomein', 637-639.

47 Aldus de plv. Commandant USCYBERCOM, Igen Vincent Stewart tijdens een lezing voor CyCon US in 2018, zie: Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', 5.

48 Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland', 38.

49 Waarbij 'manoeuvreren' een eufemistisch synoniem is voor offensief handelen, zie: Paul A.L. Ducheine, Jelle van Haaster, en Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment', in Paul A.L. Ducheine en Frans P.B. Osinga (red.), *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis - NL ARMS 2017* (2017).

50 Paul M. Nakasone, 'A Cyber Force for Persistent Operations', in: *Joint Force Quarterly* 92 (2019) (1) 10–14, 12. NB: Nakasone is naast commandant USCYBERCOM ook commandant van de inlichtingendiensten van het ministerie van Defensie, namelijk de National Security Agency (NSA) en Central Security Service (CSS).

51 Paul M. Nakasone en Michael Sulmeyer, 'How to Compete in Cyberspace: Cyber Command's New Approach', *Foreign Affairs* (2020).

Al met al concludeerde de VS dat normen in cyberspace gewenst zijn, maar dat inspanningen van onder meer de VN niet snel genoeg tot resultaat leiden. Het was tijd om andere opties te overwegen, zoals 'tacit bargaining' en 'agreed competition' in cyberspace, uitgaande van de idee dat gedrag in cyberspace uiteindelijk uitbalanceert door middel van een proces van *trial and error*. De VS sloeg echter eenzijdig deze weg in, zonder directe samenwerking met Cyber Commands van bondgenoten te zoeken. Dit gedrag tekent de houding van de VS, en is de opmaat voor het duiden van PE volgens de criteria van Johnston.

Voor Nederland zal een diplomatieke aanpak te allen tijde prevaleren boven een militaire, zelfs in tijden van conflict

De strategische cultuur van Persistent Engagement

De eerste variabele binnen het Johnston-paradigma is de rol van oorlog in menselijke aangelegenheden. USCYBERCOM gaat er met PE van uit dat in cyberspace ieders intenties min of meer vaststaan, dat onderhandelen hierover niet mogelijk is, en dat conflicten daarmee niet te voorkomen zijn. De kracht van PE, aldus de VS, is het voorkomen van escalatie van een conflict en daarmee nadelige gevolgen voor de VS. PE zorgt preventief en proactief voor het indammen van het anders onvermijdelijke conflict, door constant te 'jagen' op de tegenstander, zelf het initiatief te houden en een mogelijke cyberaanval in de kiem te smoren. Het is daarmee aannemelijk dat de PE hoog scoort op de eerste variabele van Johnston.

De tweede variabele gaat over de aard van de tegenstander en de dreiging die deze vormt, ofwel: zero-sum of variable-sum. Uit zowel de PE-doctrine als de *2018 National Cyber Strategy* komt naar voren dat, voor de VS, cyberspace geen arena voor politieke competitie is waar voor- en tegenstanders elkaar beïnvloeden. De VS acht diplomatie bedrijven aangaande cyberspace, en het streven naar een win-win optie, nobel maar niet realistisch. Illustratief zijn de UN GGE-sessies in 2017 waarbij de voortgang om te komen tot cybernormen stagneerde. De perceptie is dat samenwerking of coördinatie met anderen zelden iets oplevert waar ook de VS direct profijt van heeft, wat de variable-sum-benadering bemoeilijkt. Dit blijkt ook uit het eenzijdige besluit van de VS om een strategie en doctrine te ontwikkelen om zijn belangen te beschermen, los van de VN, en zodoende op een alternatieve weg tot cybernormen te komen. Deze overwegingen zijn indicatief voor hoe de VS internationale betrekkingen ziet en typeert PE eerder als een zero-sum game, met een hoge score binnen het Johnston-paradigma tot gevolg.

De effectiviteit van het gebruik van geweld is de derde variabele. PE is onderdeel van de defend forward-visie van de VS. Het houdt de tegenstanders buiten de eigen (Amerikaanse) netwerken door actief tegenstanders te verstoren, nog voordat er een cyberaanval plaatsvindt. Dit maakt dat PE een proactieve houding nastreeft ten opzichte van het gebruik van offensieve cyberactiviteiten. USCYBERCOM is geen response force, maar een eenheid die constant en preventief bezig is met het uitvoeren van offensieve cyberoperaties. Offensieve activiteiten zijn binnen PE geen 'last resort' waardoor PE ook op deze variabele eerder hoog scoort dan laag.

52 Nick Perre, 'Dutch Strategic Culture-A Case Study', Universiteit Leiden (2018), 19.
53 Voorhoeve, *Peace, Profits and Principles: A Study of Dutch Foreign Policy*, 45.

De Nederlandse strategische cultuur

De Nederlandse strategische cultuur in een internationale context komt het best tot uiting in het buitenland- en veiligheidsbeleid,[52] van de Gouden Eeuw tot aan de GBVS. En hoewel continuïteit volgens Wells een essentieel kenmerk is van het Nederlandse buitenlandse beleid, is een belangrijke breuk te onderkennen, voortvloeiend uit de Tweede Wereldoorlog.

De Nederlandse houding jegens andere landen kende lang een 'neutralist-abstentionalist tradition.'[53] Nederland heeft zich sinds de Gouden Eeuw buiten de machtsstrijd van de toenmalige (Europese) mogendheden gehouden, en was tot aan 1940 in meer of mindere mate neutraal. Dit is altijd een vrijwillige keus geweest, en had voordelen voor zowel Nederland als de omliggende landen. Omringende landen voelden zich niet verplicht Nederland te hulp te schieten wanneer deze neutraliteit werd geschonden[54] en Nederland nam geen formele positie in ten faveure of ten nadele van de overige landen, wat het abstentionisme verklaart.

Naast de traditie van neutralist-abstentionalist, had Nederland ook een traditie van internationaal idealisme. De nadruk op deze traditie komt voort uit de nadruk op (internationaalrechtelijke) regelgeving en het benadrukken van een moreel besef bij internationale relaties. Doordat Nederland zich echter onthield van de machtsstrijd in Europa in de negentiende en begin twintigste eeuw, was het minder bedreven in internationale *realpolitik*."[55]

Na de Tweede Wereldoorlog zou het neutralist-abstentionism gaan verdwijnen, maar bleef het international-idealism behouden. In de eerste jaren na de oorlog zijn de investeringen in een herijking van het Nederlandse buitenlandbeleid bescheiden omdat er onduidelijkheid was over de mate waarin de VS (financiële) hulp bood. Tussen 1945 en 1950 was de voorbode van het nieuwe Nederlandse buitenlandbeleid al zichtbaar, en in 1950 zag de eerste echte Defensienota het licht; Nederland verankerde zich in bondgenootschappen en werd een van grondleggers van organisaties zoals de VN (1945), de NAVO (1949), de (voorlopers van de) Europese Gemeenschap (1951) en de West-Europese Unie (1954). Bovendien was Nederland voorstander van de 'vorming van een geheel in het recht gegrondveste internationale orde' die werd omschreven als het uiteindelijke hoofddoel van het buitenlands beleid.[56] Het bevorderen van de internationale rechtsorde is opgenomen in de Grondwet,[57] is een van de drie hoofdtaken van Defensie,[58] en sinds 2013 een vitaal belang van de Nederlandse staat.[59]

De meest recente vertolking van de Nederlandse strategisch cultuur is te vinden in de GBVS, de DCS en de Nationale Cybersecurity Agenda (NCSA),[60] alle uit 2018. In de GBVS komt het internationaal idealisme terug in de fundamenten van het beleid: voorkomen, verdedigen en versterken; ook waar het gaat om het tegengaan van cyberdreigingen. Ten eerste werkt Nederland aan een internationaal normatief kader voor cyberactiviteiten,[61] om daarmee incidenten te voorkomen, dit deels ook in lijn met het gedachtengoed van de UN GGE. Ten tweede werkt Nederland aan het realiseren van cyberafschrikking met slagkracht ter verdediging,[62] ook in bondgenootschappelijk verband. Onder slagkracht verstaan we cyberinlichtingen en zowel defensieve als offensieve cybercapaciteiten ter bescherming tegen, in respons op en ter afschrikking van cyberaanvallen en spionage. Deze slagkracht bevindt zich onder meer binnen de inlichtingen- en veiligheidsdiensten,[63] het Defensie Cyber Commando (DCC) en het Nationaal Cyber Security Centrum (NCSC).[64]

54 Ibidem, 48.
55 Ibidem, 49.
56 Handelingen van de Tweede Kamer 1967-1968, '9635, No 1, Nota Inzake Het NAVO- En Het Defensiebeleid' (1968) 9.
57 Artikel 90 van de Grondwet voor het Koninkrijk der Nederlanden (2018).
58 Handelingen van de Tweede Kamer 1998-1999, '26 382, Nr 1, Hoofdlijnennotitie Defensienota 2000' (1999) 2.
59 Handelingen van de Tweede Kamer 2012-2013, '33 694, Nr 1, Internationale Veiligheidsstrategie' (2013).
60 NCTV, 'Nederlandse Cybersecurity Agenda: Nederland Digitaal Veilig' (2018).
61 Doel 4 uit de GBVS, Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland: Geïntegreerde Buitenland- En Veiligheidsstrategie 2018-2022', 29.
62 Doel 6 uit de GBVS, Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland', 33.
63 Nomen Nescio, 'Verdediging Door Spionage', in: *Militaire Spectator* 190 (2021) (7/8).
64 Ressorterend onder het Ministerie van J&V, met de NCTV als primaire opdrachtgeven. Zie ook: www.ncsc.nl.

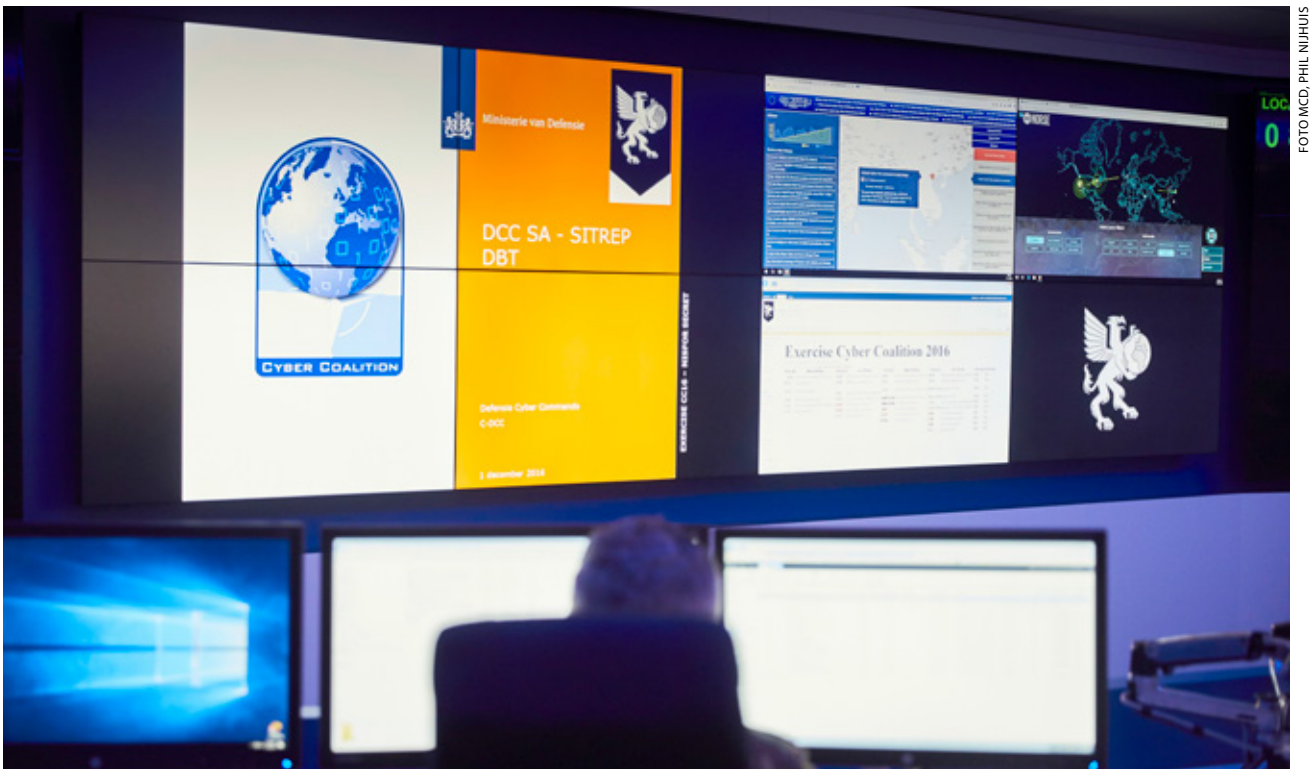


FOTO MCD, PHIL NIJHUIS

NAVO-cyberoefening, met deelname van het Defensie Cyber Commando (DCC). De Nederlandse cyberslagkracht bevindt zich onder meer in het DCC

Bovendien onderstreept ook de DCS het belang van het ontwikkelen van offensieve cybercapaciteit voor een geloofwaardige afschrikking, en geeft het NCSC aan de capaciteit om dreigingen en digitale aanvallen te signaleren en te verstoren structureel te versterken.[65] Tot slot, zonder direct aan cyberdreigingen te refereren, stelt de GBVS dat Nederland blijft investeren in het versterken van de internationale rechtsorde, 'mede omdat dit een vorm van *forward defense* is. Dit vergt specifieke militaire, civiele en diplomatieke capaciteiten die passen bij de toekomstige crisissituaties.'[66] Deze constatering is van belang, omdat Nederland hiermee impliciet aangeeft dat het internationale recht van toepassing is op cyberspace.[67]

De duiding van de Nederlandse strategische cultuur

Om de Nederlandse strategische cultuur in termen van Johnstons model te duiden, kijken we eerst naar de rol van oorlog in menselijke aangelegenheden. Al vanaf de eerste 'Defensienota' na de Tweede Wereldoorlog ziet Nederland oorlog als iets wat te voorkomen is (en dus geen voldongen feit is) en dat samenwerking van groot belang is bij conflictpreventie.[68] Deze eerste Defensienota is sterk beïnvloed door de context van dat moment: ondanks dat de bezetting net achter de rug is, was de kans dat opnieuw een oorlog uit zou breken niet onwaarschijnlijk. Zo laaide de Koude Oorlog op door de oorlog in Korea en wilde Nederland adequaat militair zijn toegerust. Militaire actie werd echter gezien als een reactie op het initiatief van een ander, bovendien zou actie

65 NCVT, 'Nederlandse Cybersecurity Agenda', 20.
66 Doel 11 uit de GBVS, Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland', 38.
67 Dit is later ook expliciet verwoord, zie: Ministry of Foreign Affairs, 'Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix: International Law in Cyberspace' (2019).
68 Handelingen van de Tweede Kamer 1950-1951, '1672, XII Rijksbegroting Voor Het Dienstjaar 1950, A Oorlog, Bijlage "Voorlopig Verslag"' (n.d).

FOTO NAVO

Het Cyber Defence Rapid Reaction Team van de NAVO legt zijn taken uit aan NAVO-ambassadeurs. Nederland is sterk gericht op samenwerking binnen een multilateraal veiligheidsstelsel, zoals het NAVO-bondgenootschap

primair in bondgenootschappelijk verband plaatsvinden.

De perceptie van het begrip oorlog verandert vanaf de jaren '60. De tekst in de Defensienota's die volgen in 1960, 1964, 1968 en 1974 redeneert eerder vanuit het vredesperspectief dan vanuit het concept van oorlog.[69] Ook het idee dat oorlog nog steeds een mogelijkheid is verdwijnt steeds verder naar de achtergrond. Illustratief is de opening van de Defensienota van 1984: 'Bijdragen aan het voorkomen van oorlog en het bevorderen van de vrede, bereid en in staat zijn de vrijheid en onafhankelijkheid van onze samenleving en ons grondgebied te verdedigen. Dat is het allesbeheersende motief voor het in standhouden van de defensie-inspanning. Vrede is zeker meer dan afwezigheid van oorlog.'[70]

Hoewel de aard van de dreiging is veranderd (van nucleaire dreiging vanuit de Sovjet-Unie tot aan de huidige terroristische- en cyberdreiging), veranderde de houding van Nederland niet. Nederland ziet oorlog als iets wat te voorkomen is, een afwijking op het normale. Ook de GBVS draagt het internationaal normatief kader,[71] en het investeren in cyberdiplomatie voor cyberactiviteiten, aan als een instrument om conflicten te voorkomen. Daarnaast is Nederland sterk gericht op samenwerking binnen een multilateraal veiligheidsstelsel, zoals dat gestalte krijgt via de VN en NAVO. Nederland vaart hierbij dus geen eigen koers, maar blijft de focus leggen op de samenwerking, zelfs als deze (in het geval van de VN) stagneert. Al met al scoort

69 Zie bijvoorbeeld: Handelingen van de Tweede Kamer 1967-1968, '9635, No 1, Nota Inzake Het NAVO- En Het Defensiebeleid'; Handelingen van de Tweede Kamer 1973-1974, '12 994, No 2 Defensienota 1974 "Om de Veiligheid van Het Bestaan"' (1974) 10-16.

70 Handelingen van de Tweede Kamer 1983-1984, '18 169 No 2, Defensienota 1984-1993' (1984) 7. De nota inzake het NAVO- en defensiebeleid van 1968 opent met een citaat van Aalmoezenier Rölling over vrede, en de defensienota van 1974 met een citaat van de Russische dissident Aleksandr Solzjenitsyn.

71 Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland'.

Nederland dus laag op de eerste variabele binnen het Johnston-paradigma en ziet het oorlog als een anomalie.

De tweede variabele is gerelateerd aan de aard van de tegenstander en de dreiging die deze vormt, en gaat over de vraag of Nederland internationale betrekkingen ziet als een zero-sum of variable-sum game. Vanaf 1950 benadrukt Nederland constant dat het een gelimiteerde militaire capaciteit heeft en dat het antwoord op dreigingen alleen in internationaal verband te vinden is. Hierbij introduceert Nederland de NAVO als hoeksteen van het buitenlands veiligheidsbeleid,[72] evenals de gedachte dat 'de veiligheid van Europa slechts in samenwerking tussen Noord-Amerika en Europa kan worden verzekerd'. Een gedachte die nog evenzeer van kracht is als toen in 1949 in het Noord-Atlantische Verdrag werd neergelegd.[73] Vanaf de Defensienota 1974 benoemt Nederland ook Europese samenwerking steeds vaker. Weliswaar als ondergeschikte van de Atlantische samenwerking, want Nederland ziet de NAVO nog steeds als primaire alliantie binnen het veiligheidsdomein, maar er is inmiddels meer nadruk op militaire samenwerking binnen Europa, zoals via het Gemeenschappelijke Buitenlands- en Defensiebeleid.[74] In algemene zin beschouwt Nederland samenwerking binnen internationale betrekkingen als voordelig voor alle partijen en neigt daarmee naar de variable-sum benadering. Nederland scoort hierdoor laag op de tweede variabele uit het Johnston-paradigma.

De effectiviteit van het gebruik van geweld is de derde variabele. De Nederlandse perceptie van de effectiviteit van het gebruik van geweld is gevoed door de Koude Oorlog en de (nucleaire) dreiging vanuit de Sovjet-Unie. Nederland benadrukt in deze periode, redenerend vanuit een NAVO-perspectief,[75] het belang van een robuust militair apparaat als politiek tegenwicht voor de agressieve houding van de Sovjet-Unie. Echter, ook na het vallen van de Muur blijft de Nederlandse krijgsmacht 'bij de uitvoering van haar hoofdtaken steeds in internationaal verband optreden.'[76] Nederland legt hierbij de nadruk op de schildfunctie van de NAVO – het creëren van een systeem van normen, regels, en samenwerkingsverbanden – en minder op de zwaardfunctie. Voor Nederland zal een diplomatieke aanpak te allen tijde prevaleren boven een militaire, zelfs in tijden van conflict.

De nadruk op diplomatie is ook van toepassing in cyberspace. Het is eenvoudiger om een dader van een cyberaanval diplomatiek aan te spreken, en dan het liefst vanuit een bondgenootschap, dan dit via militaire middelen te doen.[77] De GBVS en de DCS laten wel de mogelijkheid open om militaire slagkracht in te zetten als (cyber) afschrikking. Echter, het eventuele gebruik van geweld komt dan voort uit een defensieve grondhouding, is reactief van aard en heeft – bij inzet – het doel om een groter conflict te vermijden, zo ook in cyberspace. De GBVS, maar ook de DCS, geven aan dat het 'kabinet investeert in cyberinlichtingen en zowel defensieve als offensieve cybercapaciteiten, ter bescherming tegen, in respons op en ter afschrikking van cyberaanvallen en spionage'.[78] Nederland staat, sinds het zijn neutraliteit heeft moeten loslaten, op het standpunt dat het gebruik van geweld defensief en reactief van aard is, en enkel als laatste redmiddel te hanteren is. Op Johnstons derde variabele scoort Nederland dan ook wederom laag.

Past Persistent Engagement in onze strategische cultuur?

In dit deel komen we terug op de initiële vraagstelling van het artikel: 'In hoeverre past

72 Handelingen van de Tweede Kamer 1967-1968, '9635, No 1, Nota Inzake Het NAVO- En Het Defensiebeleid', 9.
73 Handelingen van de Tweede Kamer 1973-1974, '12 994, No 2 Defensienota 1974 "Om de Veiligheid van Het Bestaan"', 11.
74 Ministerie van Algemene Zaken, 'The EU: From the Power of Principles towards Principles and Power - Churchill Lezing van minister-president Rutte bij het Europa Instituut van de Universiteit van Zürich' (2019).
75 Handelingen van de Tweede Kamer 1967-1968, '9635, No 1, Nota Inzake Het NAVO- En Het Defensiebeleid' Deel I.
76 Handelingen van de Tweede Kamer 1998-1999, '26 382, Nr 1, Hoofdlijnennotitie Defensienota 2000' 2; Handelingen van de Tweede Kamer 1992-1993, '22 975, Nr 2, Prioriteitennota' (1993) 13.
77 Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland'.
78 Doel 6 in de GBVS, Ministerie van Buitenlandse Zaken, 'Wereldwijd Voor Een Veilig Nederland', 33; Ministerie van Defensie, 'Defensie Cyber Strategie 2018 - Investeren in Digitale Slagkracht', 7-8.

	Beschrijving variabele	Aspecten (Hoog (H) en Laag (L) uit Johnston paradigma)	Score NLD strategische cultuur op aspecten Johnston paradigma	Score persistent engagement op aspecten Johnston paradigma
1e variabele van Johnston	De rol van oorlog in menselijke aangelegenheden	Oorlog is onvermijdelijk (H) of Oorlog is een afwijking op het normale (L)	**LAAG** Oorlog is een afwijking op het normale	**HOOG** Oorlog is onvermijdelijk
2e variabele van Johnston	De aard van de tegenstander en de dreiging die deze vormt	Zero-sum (H) of variable-sum game (L)	**LAAG** Nederland ziet internationale betrekkingen als een variable-sum game	**HOOG** PE gaat uit van een zero-sum game
3e variabele van Johnston	De effectiviteit van het gebruik van geweld	Geweld als een vorm van gereedschap (H) of gebruik van geweld is een laatste optie (L)	**LAAG** Nederland ziet gebruik van geweld als een laatste optie	**HOOG** Geweld (met PE als uitingsvorm) is een vorm van gereedschap

Tabel 1 Persistent Engagement en Nederland geduid in de variabelen van Johnston

Persistent Engagement binnen de Nederlandse strategische cultuur?' Deze vraag beantwoorden wij op basis van de drie variabelen zoals verwoord door Johnston: (1) de rol van oorlog in menselijke aangelegenheden; (2) de aard van de tegenstander en de dreiging die deze vormt; en (3) de effectiviteit van het gebruik van geweld.

Het is niet te ontkennen dat, op het eerste gezicht, het verschil tussen de Amerikaanse PE-doctrine en de Nederlandse benadering inzake cyberdreiging groot is. Nederland scoort laag op alle variabelen van Johnston, terwijl PE drie hoge scores heeft, zoals Tabel 1 weergeeft.

Nederland scoort laag aangaande de rol van oorlog in menselijke aangelegenheden, omdat het benadrukt dat oorlog te voorkomen is. Kijkend naar de aard van de tegenstander en de dreiging die deze vormt, is te stellen dat Nederland een variable-sum game aanhangt: Nederland acht samenwerking als wederzijds voordelig en scoort daardoor laag op de tweede variabele. Tot slot ziet Nederland het gebruik van geweld als een 'last resort'. Daardoor scoort Nederland ook hier laag. Conform het paradigma van Johnston resulteert dit in een strategische cultuur van een meer zachte *idealpolitik* voor Nederland.

De Amerikanen hebben een meer realistisch of zelfs cynisch beeld van cyberspace waarbinnen weinig onderling vertrouwen heerst.[79] De intentie van de actoren die actief zijn liggen vast en een conflict is dan ook onvermijdelijk. Met de PE-doctrine proberen de Amerikanen een verdere escalatie van geweld te voorkomen. Zij doen dat door de dreiging preventief aan te pakken met cyberacties die 'het mes uit de handen van de aanvaller trappen',[80] waarmee zij hoog scoren op de eerste variabele van Johnston. De VS ervaart acute veiligheidsrisico's in en via cyberspace. Nadat initieel in gezamenlijk

79 Nakasone and Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach."

80 Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', 5.

verband is gezocht naar gedragsnormen in cyberspace, realiseerde de VS zich dat deze inspanning de acute problemen niet oploste, waarna het vanaf 2017 een eigen weg heeft gekozen. Dat wijst op een zero-sum game benadering. Waar Nederland, tot slot, sterk inzet op cyberdiplomatie, om daarmee de intenties van de opponent te beïnvloeden, ziet de VS dat anders. De VS is met de PE-doctrine bezig om 'vuur met vuur te bestrijden' waarbij ook het gebruik van geweld – naast diplomatie – een effectief instrument kan zijn. In Johnstons bewoordingen zou de VS met PE eerder *realpolitik* nastreven, terwijl Nederland kiest voor de *idealpolitik*.

De conclusie die hieruit te trekken is, is dat duidelijke strategische cultuurverschillen zichtbaar zijn tussen de Amerikaanse PE-doctrine en het Nederlandse buitenlandse beleid. Dit zijn verschillen die de argumenten in de juridische en ethische discussies van de inzet van PE versterken en vanuit die optiek zou het onlogisch, of zelfs onverstandig zijn voor Nederland om de PE-doctrine 'as is' over te nemen.

Een reflectie is, tot slot, op zijn plaats. De vraag die immers blijft is of de Nederlandse 'idealpolitik'-benadering afdoende is om de dreigingen in cyberspace te voorkomen of af te slaan. Moet Nederland toch een meer proactieve benadering kiezen en zijn oor te luisteren leggen bij de VS, of het VK?

De eerste aanzet hiertoe is al gegeven. De Nederlandse strategische cultuur is getoetst aan de hand van geldend, maar gedateerd beleid, met name de GBVS uit 2018. Door de (cyber) dreigingen die sinds 2018 hebben plaatsgevonden, denk daarbij aan het verstoren van de Russische OPCW-hack,[81] is het niet ondenkbaar dat Nederland een wat hardere houding inneemt in de volgende versie van de GBVS. De 'Churchill-rede'[82] van minister-president Rutte van 2019 laat zien dat de ietwat naïeve houding lijkt te draaien naar een houding die wat meer de 'realpolitik' benadert. Ook het regeerakkoord van 15 december 2021 zet de deur op een kier voor (een Nederlandse vorm van) PE. De inlichtingendiensten krijgen hierbij een belangrijke rol door beter in staat te moeten zijn hun slagkracht uit te breiden om nieuwe en toenemende digitale dreigingen en aanvallen assertief op te sporen en te bestrijden, met waarborgen voor goed en effectief toezicht en digitale burgerrechten.

Per slot van rekening kiest Nederland, zij het telkens in bondgenootschappelijk verband, ook in het fysieke domein voor een forward defense-benadering door deel te nemen aan expeditionaire missies om brandhaarden in de kiem te smoren en overloop van problemen naar Nederland te voorkomen. ■

FOTO U.S. ARMY CYBER COMMAND, JOSEF COLE

Amerikaanse militairen nemen deel aan een cyberoefening. Moet Nederland een voorbeeld nemen aan de VS en een meer proactieve cyberbenadering kiezen?

81 Netherlands Ministry of General Affairs, 'Joint Statement by Prime Minister May and Prime Minister Rutte on Cyber Activities of the Russian Military Intelligence Service, the GRU' (2018).

82 Ministerie van Algemene Zaken, 'The EU: From the Power of Principles towards Principles and Power'.