FOTO US ARMY CYBER COMMAND

Volgens critici schept de VS met persistent engagement een te simplistisch beeld van cyberspace

Persistent engagement in het cyberdomein: stabilisatie of escalatie?

*L.L.C. Faesen en D. Lassche MSc**

In het najaar van 2018 haalde het Cybercommando van de Verenigde Staten (CYBERCOM) de Russische trollenfabriek Internet Research Agency offline. Deze offensieve cyberactie wordt gezien als een eerste test van CYBERCOM's nieuwe strategie van persistent engagement. Volgens voorstanders zou het nieuwe optreden moeten leiden tot meer stabiliteit in cyberspace, geloofwaardigere afschrikking en het beter markeren van rode lijnen over wat wel en niet acceptabel is in cyberspace. Critici vrezen echter voor gebrek aan communicatie of overcommunicatie, misinterpretaties, escalatie en een ondermijning van de internationale rechtsorde. Als gevolg hiervan zou persistent engagement het algehele strategische landschap veranderen en de *deterrence posture* van kleine tot middelgrote landen zoals Nederland. Dit artikel beschrijft de inhoud van persistent engagement, de mogelijke gevolgen volgens voor- en tegenstanders en gaat in op wat het kan betekenen voor Nederland.

In het najaar van 2018 haalde het Cybercommando van de Verenigde Staten (CYBERCOM) het Internet Research Agency offline.[1] Deze door de staat gecontroleerde Russische trollenfabriek werd beschuldigd van het verspreiden van desinformatie tijdens de Amerikaanse presidentsverkiezingen van 2016 en de Congresverkiezingen van 2018. Het doel van de desinformatiecampagne zou zijn geweest om de Democratische Partij te ondermijnen, twijfel te zaaien over de betrouwbaarheid van de verkiezingsuitslagen en om reeds bestaande spanningen in de Amerikaanse samenleving te vergroten. CYBERCOM kwam in actie. De Russische trollen kregen bericht dat hun identiteit en online-activiteiten bekend waren. Op 6 november 2018, de dag van de Congresverkiezingen, werd het Internet Research Agency offline gehaald. Deze offensieve cyberactie wordt gezien als een eerste test van CYBERCOM's nieuwe strategie van *persistent engagement*. Dit artikel analyseert deze nieuwe – niet onomstreden – strategie van de Amerikanen. Wat houdt het precies in? Welke gevolgen voorspellen deskundigen? Gaat dit leiden tot stabilisatie of juist escalatie in het cyberdomein? En tot slot: welke mogelijke beleidsimplicaties heeft deze Amerikaanse koers voor Nederland?

Wat is persistent engagement?

CYBERCOM beschrijft persistent engagement als 'manoeuvring seamlessly between defense and offense across the interconnected battlespace'.[2] Het commando kondigt aan wereldwijd te gaan opereren 'as close as possible to adversaries and their operations.'[3] Dit maakt van CYBERCOM een proactieve kracht die niet langer wacht tot de juridische drempel van conflict is overschreden, maar die aanhoudend optreedt onder de drempel van een gewapende aanval om de tegenstander continu te verstoren.[4] Dit betekent dat er ook buiten de Amerikaanse cybernetwerken en grenzen opgetreden wordt, om het signaal af te geven dat inmenging in Amerikaanse binnenlandse aangelegenheden onacceptabel is, ook niet via het cyberdomein.[5] De VS maakt hierbij onderscheid tussen eigen netwerken (*blue space*), vijandige netwerken (*red space*), en andere netwerken (*grey space*).[6] De Amerikanen vatten red space ruim op, als elk netwerk waarin een vijandelijke actor controle heeft over een node. Het gaat hier dus niet alleen om de netwerken in Rusland, maar bijvoorbeeld ook om Nederlandse netwerken met Russische aanwezigheid. Deze indeling schept volgens critici een te simplistisch beeld van cyberspace: het is een omgeving die juist gekenmerkt wordt door haar dualistische karakter omdat zowel statelijke als niet-statelijke – militaire én civiele – partijen er gebruik van maken. Sterker nog, niet-militaire partijen beheren en gebruiken de meeste netwerken en infrastructuur.
Dat deze aanpak bij andere landen dus niet per se in goede aarde valt, is te begrijpen. Een Amerikaanse verstoring van een Nederlands netwerk heeft namelijk niet alleen gevolgen voor het Russische doelwit, maar ook voor de Nederlandse statelijke – en vooral niet-statelijke – actoren die het gebruiken. Maar de VS ziet dit als een

* Louk Faesen is strategisch analist bij het *The Hague* Centre for Strategic Studies (HCSS); Deborah Lassche is onderzoeker bij TNO.

1 E. Nakashima, 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms', in: *The Washington Post*, 27 februari 2019. Zie: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

2 US CYBERCOMMAND, *Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command* (Washington, D.C, april 2018) 6. Zie: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

3 Ibid.

4 Ibid., 2.

5 Dit wil niet zeggen dat de VS voor de aankondiging van de persistent engagement-strategie niet opereerde in de netwerken van zijn bondgenoten. Maar eerder gebeurde dat vooral om onder de radar inlichtingen te verzamelen of om toegang te verkrijgen tot vijandelijke doelwitten (zie onder meer: Max Smeets, 'US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection', in: *Intelligence and National Security* (2020), 444-453. Deze heimelijke inlichtingenoperaties vallen onder Amerikaanse en niet onder internationale wetgeving (zogeheten *Title 10 Authorities*). De operaties die CYBERCOM onder persisistent engagement uitvoert zijn anders want zij raken echt de netwerken zelf, namelijk door deze te verstoren. Daarom zijn dit *Title 50 Authorities*. Deze vallen wel onder internationaal recht en brengen in tegenstelling tot *Title 10*-operaties meer juridische zorgen, frictie en consequenties met zich mee. Voor meer informatie over Title 10 en Title 50, zie: A.E. Wall, *Demystifying the Title10-Title50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action* (2011), https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

6 Max Smeets, 'Cyber Command's Strategy Risks Friction with Allies', in: *Lawfare* (28 mei 2019). Zie: https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

FOTO US ARMY CYBER COMMAND

Volgens Commandant CYBERCOM generaal Paul Nakasone geloven Amerika's vijanden niet dat er consequenties vasthangen aan onverantwoordelijk gedrag

noodzakelijk kwaad om tegenstanders voldoende af te schrikken en baseert zich hierbij op argumenten uit de *deterrence theory*.[7]

Een nieuwe koers voor cyber deterrence?

Persistent engagement is beleidsmatig een vervolg op de *active defense*-doctrine en de in 2018 door het Amerikaanse ministerie van Defensie geïntroduceerde term *defending forward*.[8] De VS zelf ziet persistent engagement niet als offensief gedrag, maar als defensief in de zin van 'kicking the knife out of the hand of the attacker'.[9] Critici zien het minder onschuldig en omschrijven het als het meedogenloos volgen van tegenstanders en het steeds intensiever ondernemen van offensieve tegenmaatregelen.[10] Het doel van

7 Deterrence theory draait kortgezegd om het afschrikken van een tegenstander om iets te doen. Er zijn meerdere theoretische stromingen binnen het brede deterrence -gedachtegoed. Voor dit artikel gaat het te ver om deze alle te benoemen en uit te werken, maar de belangrijkste elementen ervan die nodig zijn voor het uiteenzetten van persistent engagement komen verderop aan bod.

8 *Defending forward* bestaat uit drie pijlers: positioneren, waarschuwen en beïnvloeden. CYBERCOM's strategie van persistent engagement bevat al deze pijlers. Het Pentagon omschrijft defending forward als: ' to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict (…) to halt or degrade cyberspace operations targeting the Department (…) by leveraging our focus outward to stop threats before they reach their targets (…) to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions'. (U.S. Department of Defense, *Cyber Strategy* (Washington, D.C., september 2018) 1,2 en 4; zie: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF).

9 Jason Healey, 'The implications of persistent (and permanent) engagement in cyberspace', in: *Journal of Cybersecurity* (Vol. 5, No 1., 2019) 5.

10 Greg Myre, 'Persistent Engagement': The Phrase Driving A More Assertive U.S. Spy Agency' (Washington, D.C., *NPR*, 26 augustus 2019). Zie: https://www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency?t=1581927765642.

persistent engagement is om zichzelf buiten de Amerikaanse netwerken te verdedigen door daar effecten te behalen (de zogeheten D5: *deceive*, *disrupt, deny, degrade* en *destroy*).[11] Daarmee kan een aanval in de voorbereidingsfase worden gestopt of de eigen verdediging worden voorbereid en uitgebreid. Tevens is het mogelijk door middel van offensieve cyberoperaties de zwakheden van de tegenstander uit te buiten voordat een aanval plaatsvindt, bijvoorbeeld door misleiding. Hierdoor hoopt de VS toekomstige aanvallers te snel af te zijn, af te schrikken, en/of te verslaan.[12]

Voorheen volgde de Amerikaanse afschrikkingsstrategie de logica van een escalatieladder waarbij verschillende vormen van deterrence elkaar opvolgen.[13] Deze ladder begint met *entanglement* (verwikkeling): de mate waarin de aanvaller mogelijk in de eigen vingers snijdt door onderlinge afhankelijkheden. Daarna volgt de realisatie van *normen*: de mate waarin diplomatieke overeenkomsten tussen staten, vooral binnen de Verenigde Naties, verantwoordelijk gedrag stimuleren. Vervolgens komt *denial* (ontzegging): de mate waarin de *resilience* (weerbaarheid of veerkracht)[14] of *cybersecurity* de aanvaller afschrikt omdat de beoogde effecten van een aanval tenietgedaan worden. Tot slot volgt *punishment* (afstraffing): de mate waarin potentiële tegenmaatregelen de aanvaller afschrikken.[15] Punishment omvatte voorheen vooral publieke attributie, het vervolgen van hackers en het opleggen van sancties. Dit valt onder de noemer *cross-domain deterrence*,[16] het reageren met machtsmiddelen uit andere domeinen dan waar de dreiging zich heeft geuit. CYBERCOM argumenteert dat punishment niet voldoende was om de vijand effectief af te schrikken. Dit zou mede veroorzaakt zijn door de 'passieve' houding van de VS en het gebrek van geloofwaardigheid van Amerikaanse tegenmaatregelen in cyberspace. Volgens Commandant CYBERCOM generaal Paul Nakasone geloven Amerika's vijanden[17] niet dat er consequenties vasthangen aan onverantwoordelijk gedrag.[18] Met andere woorden: de geloofwaardigheid van de Amerikaanse tegenmaatregelen is in het geding. Een pro-actieve opstelling in cyberspace in de vorm van persistent engagement moet hier een einde aan maken. De Amerikanen willen laten zien dat ze *fire with fire* kunnen bestrijden. Zoals een defensieambtenaar het verwoordde: 'The calculus for us here was that you're just pushing back in the same way that the adversary has for years. It's not escalatory. In fact, we're finally in the game.'[19]

De beoogde positieve effecten van persistent engagement

Voorstanders van persistent engagement hopen dat het tot geloofwaardigere afschrikking en/of ontwikkeling van normen leidt en daarmee tot meer stabiliteit in cyberspace.

11 John Reed, 'The five deadly Ds of the Air Force's cyber arsenal', in: *Foreign Policy* (12 april 2013). Zie: https://foreignpolicy.com/2013/04/12/the-five-deadly-ds-of-the-air-forces-cyber-arsenal/.

12 Tim Sweijs en Danny Pronk, *Strategic Monitor 2019-2020*. The Writing on the Wall (Den Haag, HCSS, 2020) 24.; Healey, 'The implications of persistent (and permanent) engagement in cyberspace', 1.

13 Joseph Nye beschrijft deze vier vormen van deterrence niet per se als een verticale escalatieladder, maar als vier horizontale begrippen die samen tot deterrence leiden.

14 Resilience is een term waarmee de veerkracht van een object wordt geduid. Bijvoorbeeld: een maatschappij met een hoge resilience veert na een aanval makkelijk terug naar haar oude staat.

15 Joseph Nye, 'Deterrence and Dissuasion in Cyberspace', in: *International Security* (Vol. 41, No. 3, Winter 2016/2017) 44-71.

16 Cross-domain betekent het uitoefenen van invloed via verschillende domeinen van macht. Die domeinen worden vaak aangeduid met het acroniem DIMIFEL: Diplomacy, Informational, Military, Intelligence, Financial, Economic en Law enforcement. Deze term dient niet verward te worden met Multi-Domain Operations (MDO), waarbij het gaat om de militaire domeinen van de landmacht, luchtmacht, marine, cyber en space.

17 Het cyberbeleidsdocument van het Amerikaanse ministerie van Defensie is vrij duidelijk over wie de Amerikaanse vijanden zijn in het cyberdomein: het gaat hier vooral om China, Rusland, Iran en Noord-Korea. Zie: *Cyber Strategy*, 1. Van China en Rusland wordt specifiek de dreiging benoemd: China is berucht vanwege het continu 'roven' van kwetsbare informatie van het Amerikaanse leger en Amerikaanse private partijen die van belang zijn voor de Amerikaanse economie. Rusland houdt zich in de ogen van de Amerikanen vooral bezig met cyberoperaties om de Amerikaanse opinie te beïnvloeden.

18 US CYBERCOMMAND, *Achieve and Maintain Cyberspace Superiority,* 2. Of dit daadwerkelijk het geval is, is voor een buitenstaander natuurlijk lastig te beoordelen.

19 Nakashima, 'U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms'. Het is interessant dat de Amerikanen hun houding binnen het cyberdomein in de afgelopen jaren classificeren als 'passief'. Dit valt ter discussie te stellen, zie bijvoorbeeld Alexander Klimburg, 'Mixed Signals: A Flawed Approach to Cyber Deterrence', in: *Survival* (Vol 62., No. 1, 2020) 107-130. Allereerst heeft de VS een lange geschiedenis van offensieve cyber- en inlichtingenoperaties, wat diverse recente lekken bevestigen. Daarnaast heeft de VS dure defensieve programma's die ook voor offensieve doeleinden gebruikt kunnen worden, zoals het *Comprehensive National Cybersecurity Initiative* met een begroting van 40 miljard dollar. Tot slot zijn er de voorbeelden van Amerikaanse cyberoperaties zoals Stuxnet en Flame.

Allereerst volgen velen de gedachtegang van *deterrence theory*. Uitgangspunt is dat persistent engagement een aanvulling is op de bestaande tegenmaatregelen en zal leiden tot het verder verhogen van de kosten van een aanval en daarmee een nieuw en effectiever niveau van afschrikking realiseert.[20] Klassieke deterrence theory richt zich op de kosten-batenafweging van een tegenstander en berust op twee elementen: er moet een geloofwaardige te verwachten tegenreactie zijn en een *denial*[21] van de voordelen van een aanval.[22] Hierdoor wordt de kosten-batenafweging negatief beïnvloed. Joseph Nye omschrijft het als: 'Deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit.'[23] Volgens Nakasone is het hier dus misgegaan: tegenstanders geloofden niet (meer) dat de kosten van een cyberaanval de voordelen zouden overstijgen. Persistent engagement moet dit corrigeren en meer handelingsperspectief bieden om aanvullende effecten te behalen zoals het vertragen, blokkeren of verstoren van een vijand.

Vanuit de persistent engagement stability theory[24] verwacht men een stabiliserend effect door middel van normen. Volgens deze theorie zal aanhoudende interactie (geplande aanval, geplande tegenreactie, nieuwe aanval) leiden tot het ontwaren van rode lijnen. Het continue aftasten realiseert een nieuwe gedragscode – dit accepteren staten wel van elkaar zonder escalatie, maar dat niet – waarbij de inzet van daadwerkelijk fysiek geweld gezien wordt als escalatie. Informatie uit de aanhoudende interactie zal volgens de theorie gebruikt worden om de verdediging te verbeteren en nieuwe cyberaanvallen af te schrikken, waarop tegenstanders hun acties naar beneden zullen schroeven. Dit alles zal volgens de optimisten leiden tot een meer stabiele cyberomgeving en een gecontinueerde superioriteit van de VS.[25]

Een dergelijk proces staat bekend als *agreed competition* of *agreed battle.*[26] Het achterliggende idee is dat er, in een escalatiesituatie waarin beide zijden toch expliciet of impliciet beperkingen accepteren, een stilzwijgende onderhandeling is (*tacit bargaining*). Deze overeenkomst hoeft niet voor beide partijen volledig duidelijk te zijn, of te berusten op een breed gedeeld begrip. Er hoeft ook geen quid pro quo te zijn. Men accepteert stilzwijgend rode lijnen omdat 'advantage can be gained through competitive interactions, rather than through the pursuit of escalation dominance.'[27] Dat voordeel bestaat uit het voorkomen van gewapend conflict, gebaseerd op de aanname dat gewapend conflict niemand voordeel oplevert. Cybermiddelen hebben juist hun strategische nut in het voorkomen hiervan. Als cyberoperaties dan wel leiden tot openlijk gewapend conflict, dan schieten cybermiddelen hun eigenlijke strategische nut voorbij.[28]

Men zou hierin de ontwikkeling van een norm kunnen zien, wat het gedrag van de spelers vormgeeft. Dit veronderstelt wel een hoge mate van consistente en eenduidige communicatie tussen de spelers, die er momenteel in het cyberdomein niet lijken te zijn. Critici wijzen daarom op het risico van ongewenste en ongecontroleerde escalatie en de mogelijk negatieve effecten van persistent engagement.

20 Healey, 'The implications of persistent (and permanent) engagement in cyberspace', 6.

21 Denial is een doctrinaire term die zich moeilijk naar het Nederlands laat vertalen. Het begrip kan omschreven worden als: zoveel macht uitoefenen dat je de ander de mogelijkheid ontzegt voordeel te halen uit zijn (door jouw ongewenste) handeling.

22 Joseph Nye, 'Deterrence and Dissuasion in Cyberspace', 54.

23 Ibid., 45.

24 Healey, 'The implications of persistent (and permanent) engagement in cyberspace', 5.

25 Ibid.

26 Michael Fischerkeller en Richard Harknett maken onderscheid tussen interactiedynamieken en escalatiedynamieken. Escalatiedynamieken zouden meer van toepassing zijn op potentieel en episodisch gevaar en daarmee niet op de voortdurende interactie die we zien in het cyberdomein. Zie: Michael Fischerkeller en Richard Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', in: *The Cyber Defense Review* (december 2019) 267-287.

27 Ibid., 268; Tijdens de Koude Oorlog was met de nucleaire afschrikking *escalation dominance* duidelijk het (eind)doel om voordeel te kunnen behalen. Voor cyber geldt dat niet.

28 Fischerkeller en Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', 274-275.

De mogelijke negatieve effecten van persistent engagement

Tegenstanders van persistent engagement vrezen juist voor escalatie door een aantal factoren:

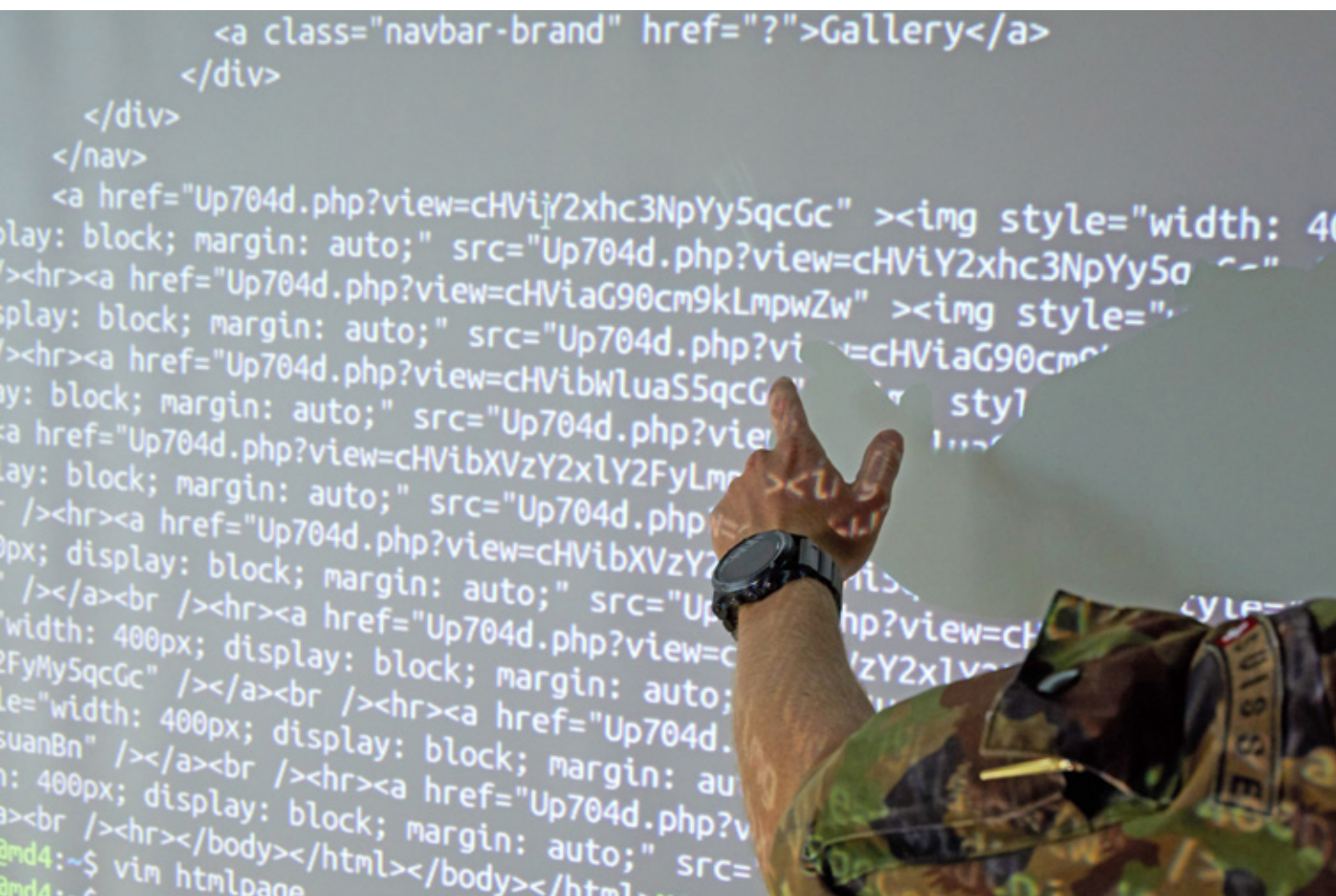
- de relatief slechte nationale cybersecurity van de VS
- de risico's op misinterpretatie door gebrek aan communicatie
- de risico's op misinterpretatie door overcommunicatie
- een evenwicht van cyberaanvallen dat hoger ligt dan nu
- normondermijning
- de onzekerheid die spill-over naar andere domeinen met zich meebrengt

Allereerst is er de slechte staat van de Amerikaanse nationale cybersecurity.[29] Er is een lage mate van weerbaarheid en er vloeien moeilijkheden voort uit het grote raakoppervlak van de VS: terwijl er binnen Nederland met honderden providers van kritieke infrastructuur gecoördineerd moet worden, moet er binnen de VS met tienduizenden worden samengewerkt.[30] Dit maakt samenwerking op het gebied van cybersecurity lastig. Vandaar waarschijnlijk de vlucht naar voren met de persistent engagement-strategie. Deze moeizame verdediging wordt een nog groter risico in een omgeving van constante competitie en aanval. Zoals hiervoor geschetst heeft persistent engagement een grote kans bij

29 Zie bijvoorbeeld de evaluaties van het U.S. Government Accountability Office over de cyber resilience van de Amerikaanse federale overheid en van het ministerie van Defensie (U.S. Government Accountability Office, 'Cybersecurity: DOD Needs to take Decisive Actions to improve Cyber Hygiene' (Washington, D.C., 13 april 2020). Zie: https://www.gao.gov/products/GAO-20-241); zie ook Klimburg, 'Mixed Signals', 107-130.

30 Klimburg, 'Mixed Signals', 118.

De persistent engagement stability theory richt zich op het creëren van nieuwe normen door een voortdurend aftasten FOTO MEDIATHEK VBS, JONAS KAMBLI



te dragen aan de ontwikkeling van een omgeving van constante interactie en competitie, met potentieel juist méér aanvallen voor de VS. Daarnaast zal een wapenwedloop op het gebied van cybercapaciteiten zich niet alleen zal beperken tot de landen waarvoor de nieuwe doctrine is bedoeld (Rusland, China, Iran en Noord Korea), maar ook andere landen in beweging brengen. Die kunnen met relatief eenvoudige offensieve capaciteiten nog steeds veel schade veroorzaken in de VS indien er sprake is van ondermaatse cybersecurity en weerbaarheid.

Bij persistent engagement is er een groter risico op misinterpretatie van de doelstelling van een Amerikaanse actie. Voor een effectieve toepassing van deterrence is het belangrijk te beseffen dat de kosten-batenafweging die de aanvaller maakt gebaseerd is op inschattingen. Die inschattingen berusten onder meer op percepties: interpretaties van de werkelijkheid.[31] Voor goed functionerende afschrikking moet de perceptie van kosten en baten helder zijn bij zowel de aanvallende als de verdedigende partij.[32] In het cyberdomein zijn een spionageactiviteit en de voorbereiding voor een aanval echter moeilijk van elkaar te onderscheiden. Intenties en percepties zijn nog minder eenvoudig te achterhalen dan in het conventionele militaire landschap. Chinese actoren die nu in een netwerk meekijken worden toch anders ervaren dan de Russen die via satellieten meekeken ten tijde van de wapenwedloop in de Koude Oorlog. Het onderscheid tussen dreigen en daadwerkelijk kwaad willen was toen duidelijker, net als de capaciteiten en de intenties, dan nu in het cyberdomein het geval is. Hierdoor is het risico op misinterpretatie en escalatie nu groter. Dit heet ook wel een *signaling*-probleem: de signalen die worden afgegeven met acties in het cyberdomein zijn niet duidelijk genoeg en voor meerdere interpretaties vatbaar.[33] Deze negatieve feedbackdynamieken leggen een zwakte van de persistent engagement stability theory bloot. Er wordt enkel via inlichtingen of militaire signalen gecommuniceerd en men negeert de middelen die voorheen door de VS werden gebruikt, zoals de vervolgingen door het ministerie van Justitie, sancties door het ministerie van Financiën, demarches, bilaterale gesprekken en normontwikkeling door het ministerie van Buitenlandse Zaken en uitspraken van de president of door hem gesloten overeenkomsten. Het alsnog interdepartementaal synchroniseren van deze signalen zal een gespannen en moeizaam proces zijn, wat leidt tot gemengde signalen en verwarde tegenstanders. Tevens is er geen neutrale zone om gedrag toe te lichten en afspraken te maken over de spelregels. Vertrouwenwekkende maatregelen die interstatelijke transparantie en crisiscommunicatie bevorderen lijken volgens critici onontbeerlijk om escalatie door persistent engagement te voorkomen.

Een derde punt waar tegenstanders op wijzen is het verschil tussen het belang van transparantie en het risico van overcommunicatie. Geloofwaardigheid binnen deterrence hangt af van transparantie over de middelen. Een vijand laat zich namelijk moeilijk afschrikken met geheime wapens. Transparantie is ook een noodzakelijke eerste stap voor wapenbeheersing: het zal leiden tot een discussie over de strategische oorlogvoeringcapaciteiten, meer openheid over de middelen, effecten en intenties om misverstanden te voorkomen en helpen bij het vaststellen van normen en andere vertrouwenwekkende maatregelen voor verantwoordelijk statelijk gedrag en communicatie. Dit zijn de pilaren die leiden tot stabiliteit. Maar met persistent engagement gaat CYBERCOM verder. Het commando communiceert niet alleen openlijk over haar capaciteiten, maar ook over haar activiteiten, zoals die tegen het Internet Research Agency. Het gesprek op het niveau van strategische oorlogvoeringscapaciteiten wordt hierdoor plotseling overschreeuwd door een

31 Andere elementen die een rol spelen zijn normen, doctrine, TTP's en de bereidheid om terug te slaan (Alexander Klimburg en Louk Faesen, 'A Balance of Power in Cyberspace' in: *European Cybersecurity Journal* (2018) 5.

32 Over de rol die perceptie speelt kan men het boek *Perception and Misperception in International Politics* uit 1976 van Robert Jervis raadplegen. Hij geeft ook specifieke voorbeelden in zijn artikel 'Deterrence and Perception', in: *International Security* (Vol. 7, No. 3, 1982/1983) 3-30.

33 Herbert Lin, 'Escalation Dynamics and Conflict Termination in Cyberspace', in: *Strategic Studies Quarterly*, (Fall 2012) 46-70; Healey, 2019; Jason Healey en S. Caudill, 'Success of Persistent Engagement in Cyberspace' in: *Strategic Studies Quarterly* (Spring 2020) 9-15.

Een zwakte van de persistent engagement stability theory is dat enkel via inlichtingen of militaire signalen gecommuniceerd wordt

FOTO US ARMY CYBER COMMAND, STEVEN STOVER

publieke discussie over cyberaanvallen die in vredestijd worden uitgevoerd. Volgens sommigen zal dit een averechts effect hebben. Het onthullen van details over geheime aanvallen gericht op tegenstanders bevordert volgens Alexander Klimburg normen van agressie in vredestijd en – in het geval van de operatie tegen de Russiche trollenfabiek – het beschouwen van het verspreiden van informatie als een kinetische aanval. Ook onderstreept dit volgens Alexander Klimburg het gebrek aan onderlinge communicatie op strategisch niveau: 'Unfortunately, the signaling mandated by persistent engagement has extended to over-communication in public – itself an example of weaponised information that [firstly] diminishes the benefits of the defend-forward strategy, [secondly] lends legitimacy to information-warfare operations as a form of conflict and [thirdly] simultaneously encourages an already accelerating cyber arms race.'[34]

Een volgend bezwaar tegen persistent engagement is dat stilzwijgende onderhandelingen (tacit bargaining) niet automatisch hoeven te leiden tot een evenwicht met een laag niveau van cyberaanvallen (het idee achter de persistent engagement stability theory). Het evenwicht kan ook uitkomen op een redelijk hoog aantal cyberaanvallen.[35] Dit is het risico van positieve feedback. Als de (preventieve) tegenmaatregelen potentiële tegenstanders niet afschrikken maar juist ergeren, zullen ze harder terugslaan. De competitie in het cyberdomein zal dan juist intensiveren.[36] Daarbij is het ook niet geheel duidelijk waarom een tegenstander zich zou laten inperken op een manier die in het voordeel is van de VS.

34 Klimburg, 'Mixed Signals', 109.

35 Fischerkeller en Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation', 276.

36 Healey, 'The implications of persistent (and permanent) engagement in cyberspace', 1-15. Healey maakt onderscheid tussen verschillende feedbackloops binnen depersistent engagement stability theory: on-net; off-net; en risico's voor het bredere systeem (blz. 7).

Tegenstanders wijzen er ook op dat de VS door de praktijk van persistent engagement reeds bestaande internationale normen kan ondermijnen, zoals de vrijheid van informatie.[37] In eerste instantie kan persistent engagement juist bijdragen aan de naleving van bestaande cybernomen: het levert duidelijk bewijs wat voor soort activiteiten een staat als onaanvaardbaar beschouwt, waardoor deze normen meer dan woorden op papier worden. Maar tegelijkertijd introduceert het ook nieuwe normen, bijvoorbeeld dat informatie niet een vrij goed is, maar iets wat als een aanval kan worden beschouwd. Zo zijn desinformatiecampagnes, zoals die van het Russische Internet Research Agency, niet geheel illegaal volgens internationaal recht. Door openlijk terug te slaan tegen de Russische trollenfabriek beschouwt de VS desinformatie wel degelijk als een aanval en behandelt het informatie op dezelfde manier als de Russen: als een potentieel wapen.[38] Rusland en China kunnen dan op hun beurt een soortgelijke aanval uitvoeren op westerse media – zoals CNN en de BBC – die kritisch zijn over hun regime. Daarnaast vergroot het aanmoedigen door persistent engagement van cyberconflicten het beeld dat een sterkere rol van de overheid in het cyberdomein noodzakelijk is om de orde te bewaren en dat dit 'gevaarlijke' domein een intergouvernementeel model nodig heeft om het te beheren.[39] Dit staat in schril contrast met de gevestigde normen en internationale rechtsorde die – mede door de VS – is gecreëerd binnen de Verenigde Naties en het *multi-stakeholder* model voor *internet governance*. Hierin is juist een grote rol weggelegd voor *civil society* en de private sector.

Tot slot stellen tegenstanders dat persistent engagement, als onderdeel van agreed competition, maximaal één domein kan omvatten om werkbaar te zijn.[40] De gedachte is dat, zodra een conflict zich uitbreidt naar andere domeinen (spill-over), de kosten- en batenafwegingen van alle spelers grondig door elkaar worden geschud. Risico's, kosten en uitdagingen zijn dan niet langer helder, wat wel een noodzakelijke voorwaarde is voor agreed competition. De consequentie hiervan is volgens Michael Fischerkeller en Richard Harknett: 'It would no longer be agreed competition, but conflict, and potentially war.'[41] Dit is vooral relevant in relatie tot cross-domain deterrence. Het lijkt er immers op dat de VS en zijn tegenstanders ook nog steeds buiten het cyberdomein reageren, bijvoorbeeld door juridische vervolgingen en (economische) sancties.[42] Op basis van analyse van eerdere gebeurtenissen kan in twijfel worden getrokken of de uitkomsten van cyberconflict beperkt kunnen blijven tot het eigen domein.[43] Indien dit niet zo is, betekent dit dat het gevaar van escalatie toeneemt.

Samenvattend positioneert CYBERCOM zich met persistent engagement als een soort special operations commando dat onder de drempel van gewapend conflict opereert en dat gekenmerkt wordt door een hoge mate van flexibiliteit, een zelfstandig optreden door speciaal daarvoor getrainde militairen en een speciaal besluitvormingsproces. Dit faciliteert de mogelijkheid voor een meer proactieve en offensieve tegenreactie ten tijde van hybride oorlogvoering, maar brengt een hoog risico van overcommunicatie, misinterpretatie en daarmee escalatie met zich mee. Door niet alleen de ontwikkeling, maar ook de inzet van offensieve cyber capaciteiten te stimuleren verandert het van continue cyberspionage naar continue cyberaanvallen. Dit zet de kwetsbaarheid van de Amerikaanse netwerken onder nog meer druk. Daarbij presenteert de VS cyberagressie als een legitiem

37 Klimburg, 'Mixed Signals', 120-123.

38 Faesen e.a., 'From Blurred Lines to Red Lines: How Countermeasures and Norms Shape Hybrid Conflict', 74.

39 Klimburg, 'Mixed Signals', 107-130.

40 Fischerkeller en Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Esclation', 267-287.

41 Ibid., 274.

42 U.S. Department of Justice, 'Press Release - Russian National Charged with Interfering in U.S. Political System', 19 oktober 2018. Zie: https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system; U.S. Department of the Treasury, 'Press Release - Treasury Targets Assets of Russian Financier who Attempted to Influence 2018 U.S. Elections', 30 september 2019. Zie: https://home.treasury.gov/news/press-releases/sm787.

43 Cyberexperts Brandon Valeriano en Benjamin Jensen concluderen, gebaseerd op een grote historische dataset van cyberoperaties, dat zulke operaties op zichzelf zelden leiden tot concessies. Veel vaker is het nodig om zulke operaties te vergezellen van andere acties, zoals diplomatieke handreikingen, om tot resultaat te komen. Zie Brandon Valeriano en Benjamin Jensen, 'The Myth of the Cyber Offense' (15 januari 2019) https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

machtsinstrument in vredestijd. Dit zal het reeds grote grijze gebied in moderne conflictvoering, met de steeds vagere drempel tussen vredestijd en oorlogstijd, verder vergroten en de strategische compressie in het cyberdomein versterken waardoor langetermijnbelangen uit het oog verloren kunnen worden.[44]

Implicaties voor Nederland?

De ontwikkelingen rondom persistent engagement zijn nog te vers om met zekerheid de gevolgen te beschrijven voor de Nederlandse context. Zo is er onenigheid tussen het Amerikaanse ministerie van Defensie (met name CYBERCOM) en het Witte Huis over de daadwerkelijke intentie van de nieuwe strategie, wat leidt tot gemengde en soms zelfs tegenstrijdige signalen naar de buitenwereld.[45] Toch is het een poging waard te schetsen welke drie effecten van persistent engagement waarschijnlijk Nederland gaan raken en wat mogelijke antwoorden hierop kunnen zijn.

Ten eerste moet Nederland zich afvragen welke communicatie van de Amerikanen verlangd wordt voorafgaand aan een Amerikaanse offensieve operatie en hoe. Terwijl er voorheen interdepartementaal overleg en presidentiële goedkeuring nodig was voor offensieve cyberspace-operaties, heeft CYBERCOM nu meer autoriteit en handelingsperspectief.[46] Zonder duidelijke communicatie van de Amerikaanse intenties vooraf aan een missie (wat voorheen

44 Klimburg, 'Mixed Signals', 107-130. Strategische compressie is het fenomeen dat de onderverdeling in strategisch, operationeel en tactisch niveau steeds verder verdwijnt en dat het strategische niveau zeer dicht tegen de uitvoering aan komt te zitten. Zie ook de *Joint Doctrine Publicatie 5 Commandovoering* (Den Haag, ministerie van Defensie, 2012).

45 US CYBERCOM ziet persistent engagement als een defensieve strategie, terwijl het Witte Huis het ziet als een offensieve strategie. Zie ook: Healey, 'Success of Persistent Engagement in Cyberspace', 11.

46 Op 15 Augustus 2018 heeft president Donald Trump Presidential Policy Directive 20 vervangen door het National Security Presidential Memorandum 13 (NSPM-13). Het is een vertrouwelijk document, waardoor het nog onduidelijk is hoe het nieuwe autorisatieproces voor offensieve cyberoperaties eruit ziet. Het lijkt erop dat er nu beslissingen op lager niveau worden genomen door het hoofd van CYBERCOM zonder formele interdepartementale goedkeuring van het ministerie van Buitenlandse Zaken. Dat ministerie keek vooral naar de toepassing van internationaal recht en normen (Center for Security Studies, 'Trend Analysis The Evolution of US Defense Strategy in Cyberspace (1988-2019)' (Zürich, ETH, 2019). Zie: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf.

CYBERCOM presenteert zich met persistent engagement meer als een soort special operations commando, met als kenmerken flexibiliteit en zelfstandig optreden door speciaal getrainde militairen

FOTO US ARMY CYBER COMMAND

Nederland moet zich onder meer afvragen in hoeverre het persistent engagement kan steunen vanuit het perspectief van de internationale rechtsorde

FOTO MCD, PHIL NIJHUIS

niet vaak gebeurde bij inlichtingenoperaties)[47] is het onwaarschijnlijk dat bondgenoten – en ook Nederland – de Amerikaanse offensieve operaties in hun netwerken zullen verwelkomen. Overigens is er zelfs met duidelijke communicatie vooraf nog de cognitieve dissonantie tussen de VS, die hun optreden tot dusver als te passief en defensief ervaren, en de Europeanen, die het Amerikaanse optreden als proactief en offensief zien. Europese bondgenoten, waaronder Nederland, zullen deze cyberoperaties waarschijnlijk beschouwen als escalerend, indringend en onwenselijk. Dit wordt gevoed door een gebrek aan vertrouwen in de legitimiteit van Amerikaanse extraterritoriaal offensief optreden, ook al is de uitkomst soms in het voordeel van de Europese bondgenoten.

Daarnaast zal wellicht deconflictie nodig zijn: Amerikaanse offensieve operaties kunnen zich richten op hetzelfde doelwit als die van een bondgenoot, maar voor verschillende doeleinden. Als Nederland bijvoorbeeld heimelijk inlichtingen verzamelt over een bepaald doelwit in zijn netwerk (of daarbuiten), kan deze inlichtingenoperatie abrupt gestopt worden door een Amerikaanse aanval. Persistent engagement

47 Zie bijvoorbeeld de zaak rondom het afluisteren van de Duitse bondskanselier Angela Merkel door het National Security Agency: 'Bespioneren van 'vrienden' gaat gewoon door', in: *Trouw,* 28 oktober 2013. Zie: https://www.trouw.nl/nieuws/bespioneren-van-vrienden-gaat-gewoon-door~b91cb351/.

heeft daarom implicaties voor Nederlandse inlichtingenoperaties binnen en buiten Nederlandse netwerken. Communicatie is dus van belang. Een optie hiervoor is volgens Max Smeets het opstellen van memoranda van overeenstemming voor offensieve cyberoperaties die worden uitgevoerd in de netwerken en systemen van bondgenoten.[48] Nederland moet zich afvragen of het een dergelijke constructie zou willen en waar deze aan zou moeten voldoen, ook in het kader van mogelijke eigen cyberoperaties.

Nederland moet zich ten tweede buigen over de vraag in hoeverre het de Amerikanen wil steunen in hun keuze voor persistent engagement vanuit het perspectief van de internationale rechtsorde. Nederland profileert zich als een land dat hier de focus op legt en het belang ervan onderstreept, met Den Haag als internationale stad van vrede en recht. Persistent engagement kan bijdragen aan een statenpraktijk die bestaande cybernormen versterkt door gevolgen op te leggen aan overtredingen. Dit kan de naleving van bestaand internationaal recht en normen bevorderen die in lijn zijn met de Nederlandse buitenlandse belangen en inzet. Tegelijkertijd heeft de VS er met persistent engagement CYBERCOM als nieuwe norm-entrepreneur bij. Die lijkt met statements zoals 'We voeren een oorlog waar geen internationale normen bestaan' juist afbreuk te doen aan het internationale recht.[49] Deze mogelijke gevolgen moeten worden meegenomen in een waarden- en risicoafweging van handelingsperspectieven binnen de Nederlandse cyberstrategie. Hoe ver kan bijvoorbeeld inlichtingenondersteuning van de AIVD en MIVD aan Amerikaanse persistent engagement gaan zonder dat Nederland zijn diplomatieke positie en toewijding aan het internationaal recht in gevaar brengt? Of wordt persistent engagement wel bevorderend geacht voor de internationale rechtsorde?

Ten derde moet Nederland bepalen of en hoe het asymmetrisch deterrence-voordeel te benutten. Klimburg voorspelt dat kleine tot middelgrote landen zoals Nederland – met een offensieve cybercapaciteit behorend tot de *next 30 cyber nations* en een hogere resilience dan de VS, China of Rusland – dankzij persistent engagement een geostrategisch belangrijkere positie zullen innemen dan eerst. Zoals Klimburg zegt: 'The next-30 cyber nations may therefore possess something which was previously unavailable to them: not just a strategic-weapons capability – a virtual strike force no less potent than a wing of bombers or ballistic missiles – but also a defensive advantage towards larger foes'.[50] Landen als Nederland hebben misschien niet dezelfde offensieve superioriteit als de VS, maar ze kunnen nog steeds effecten en straffen met gevolgen opleggen aan een potentiële agressor in het cyberdomein, zoals het tijdelijk platleggen van de kritieke infrastructuur. Tegelijkertijd verhogen ze door hun relatief betere verdediging de kosten voor een aanval van een mogelijke agressor in dit domein.[51] Volgens deze redenering neemt het aantal kleine tot middelgrote landen dat vanuit een betere verdediging een grootmacht geloofwaardig en wederzijds via het cyberdomein kan bedreigen toe. Als gevolg verandert persistent engagement het algehele strategische landschap en de manier waarop deze landen in hun eigen veiligheid voorzien: in plaats van afhankelijk te zijn van grotere bondgenoten hebben vele nu hun eigen *deterrence by punishment*-capaciteit die door persistent engagement wordt aangemoedigd. Nochtans blijft het asymmetrische voordeel van kleine tot middelgrote landen grotendeels onbesproken in de meeste conventionele cyberpoweranalyses en deterrencemodellen. Vanuit het perspectief van landen zoals Nederland zal de integratie van het asymmetrische voordeel in cyber deterrence in een bredere operationele *whole-of-society deterrence*-opstelling een van de belangrijkste geopolitieke vraagstukken zijn. Gaat Nederland hier gebruik van maken? ■

48 Smeets, 'US cyber strategy of persistent engagement & defend forward', 444-453; Healey en Caudill, 'Success of Persistent Engagement in Cyberspace', 9-15.

49 Zie bijvoorbeeld uitlatingen van U.S. CYBERCOMMAND op Twitter: https://twitter.com/US_CYBERCOM/status/1229926329254064134.

50 Klimburg, 'Mixed Signals', 119.

51 Zie voor een vergelijking de National Cyber Security Index: https://ncsi.ega.ee/. Dit is een wereldwijde index die de gereedheid van landen meet om cyberdreigingen te voorkomen en om cyberincidenten te managen. Nederland staat op plaats 10, De VS op 12, Rusland op 27 en China op 80.