FOTO U.S. AIR FORCE, BARRY LOO

Verdediging door spionage

Waarom U.S. Cyber Command in feite een contra-inlichtingenstrategie uitvoert

De auteur is werkzaam voor de Militaire Inlichtingen- en Veiligheidsdienst en kan om veiligheidsredenen zijn naam niet noemen.*
Dit artikel is geschreven op persoonlijke titel.

De commandant van het Amerikaanse U.S. Cyber Command (USCYBERCOM), generaal Paul Nakasone, verklaarde recent voor de Amerikaanse Senaat dat: 'USCYBERCOM conducted more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020'.[1] Deze operaties passen in de nieuwe strategie van USCYBERCOM uit 2018 om *cyberspace superiority* te verkrijgen en vijandelijke cyberdreigingen tegen te gaan.[2,3] Voorheen was de *countercyber*-strategie van de Amerikaanse krijgsmacht enerzijds gebaseerd op verdedigen binnen de eigen militaire en andere belangrijke ICT-netwerken en anderzijds dreigen met reactieve vergelding van succesvolle vijandelijke cyberoperaties. Sinds 2018 wordt in plaats daarvan geprobeerd om vijandelijke cyberdreigingen proactief te verstoren, voordat deze zich kunnen manifesteren. USCYBERCOM zou daarbij voortdurend proberen om zo dicht mogelijk bij of zelfs in vijandelijke netwerken te opereren, om zo vijandelijke cyberoperaties al te kunnen zien aankomen voordat deze gelanceerd worden. Deze Amerikaanse strategie draait daarmee om twee centrale uitgangspunten: *persistent engagement* en *defend forward*.[4]

Sinds 2018 probeert USCYBERCOM vijandelijke cyberdreigingen proactief te verstoren, voordat deze zich kunnen manifesteren

USCYBERCOM heeft hiermee een stevig academisch en beleidsmatig debat gestimuleerd. Veel reacties van zowel critici als voorstanders hebben daarbij drie dingen gemeen. Ten eerste zien zij persistent engagement en defend forward als een conceptuele innovatie in het tegengaan van cyberdreigingen. Ten tweede analyseren zij deze strategie desalniettemin in termen en kaders die zijn ontleend aan traditionele paradigma's op oorlogvoering en strategische afschrikking. Ten derde buigen zij zich daardoor vooral over de vraag of persistent engagement en defend forward leiden tot afschrikking en stabiliteit of juist tot escalatie en een wapenwedloop in het cyberdomein.

Dit artikel betoogt daarentegen dat de strategie van persistent engagement en defend forward juist *niet* bedoeld is als vorm van afschrikking die tot meer stabiliteit moet leiden. Tevens vormt deze strategie geen conceptuele innovatie, maar betreft het in feite een gedigitaliseerde variant van een klassieke contra-inlichtingenbenadering. Spionnen vang je immers met spionnen.

Dit artikel laat eerst zien dat de bedenkers en uitvoerders van persistent engagement en defend forward juist afstand van de paradigma's van oorlogvoering en afschrikking proberen te nemen. Daarna wordt toegelicht waarom het cyberconflict tussen de VS en zijn geopolitieke tegenstanders beter te verklaren is als een strategische competitie onder de drempel van gewapend conflict in combinatie met een *intelligence contest*. Daardoor wordt duidelijk dat USCYBERCOM in feite acteert als een inlichtingendienst in plaats van een militaire manoeuvre-eenheid. Vervolgens wordt betoogd dat de escalatierisico's van persistent engagement en defend forward beperkt zijn. Intelligence contests en strategische competities draaien namelijk juist om het behalen van cumulatieve en relatieve voordelen ten opzichte van een tegenstander zonder daarbij openlijk te provoceren of directe dwang uit te oefenen. Tot slot wordt gesteld dat de logica van afschrikking en stabiliteit alleen een functie heeft ten aanzien van de dreiging van strategische cybersabotage in de context van een ernstige politiek-militaire crisis.

Paradigmawisseling: van oorlog en afschrikking naar strategische competitie en intelligence contest

De VS, zijn bondgenoten en zijn tegenstanders zijn al decennialang verwikkeld in een conflict in het cyberdomein, waarbij voortdurend over en weer cyberoperaties worden uitgevoerd die schade veroorzaken door spionage, beïnvloeding en sabotage. Al even lang debatteren academici en beleidsmakers over wat precies de aard is van dit cyberconflict en hoe staten zich het beste tegen statelijke cyberdreigingen kunnen verdedigen. Invloedrijke invalshoeken waren daarbij het gebruik van cyberspace als domein voor militaire operaties en de toepassing van het internationaal oorlogsrecht op cyberoperaties,[5] alsmede de mogelijkheden om met behulp van afschrikking tot meer stabiliteit in het cyberdomein te komen.[6]

* De naam van de auteur is bekend bij de redactie van de *Militaire Spectator*.

1 Maggie Miller, 'Cyber Command chief says dozens of cyber operations carried out to defend 2020 elections', in: *The Hill*, 25 maart 2021. Zie: https://thehill.com/policy/cybersecurity/544993-cyber-command-chief-says-dozens-of-cyber-operations-carried-out-to.

2 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, april 2018. Zie: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

3 Er moet benadrukt worden dat USCYBERCOM naast het tegengaan van vijandelijke cyberdreigingen tegen Amerikaanse militaire en andere strategische belangen ook een aantal andere taken en verantwoordelijkheden heeft. Zo is USCYBERCOM verantwoordelijk voor het ondersteunen van andere U.S. Combatant Commands met cyber- en informatieoperaties en draagt USCYBERCOM bij aan de Amerikaanse strategische afschrikking van andere dreigingen dan die in het cyberdomein. Dit artikel behandelt echter alleen de strategie van USCYBERCOM tegen vijandelijke cyberdreigingen.

4 *Persistent engagement* is de term die in academische kringen en informeel door USCYBERCOM gebruikt wordt. *Defend forward* is de formele term die in de *U.S. Department of Defence Cyber Strategy* uit 2018 wordt gebruikt. De eerste term benadrukt dat het tegengaan van cyberdreigingen continu een proactieve benadering vereist, terwijl de tweede duidelijk maakt dat daarbij zo dicht mogelijk bij of in de netwerken van de tegenstander moet worden opgetreden. Ondanks het feit dat deze termen voor een groot deel overlappen worden zij vanwege deze verschillende connotaties en nuances naast elkaar gebruikt in dit artikel.

5 Het rapport *Digitale Oorlogvoering* van de Adviesraad Internationale Vraagstukken en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken uit 2011 vormt hier nog steeds een goed voorbeeld van. Zie: https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2011/12/16/digitale-oorlogvoering.

6 Zie voor een overzicht bijvoorbeeld Stefan Soesanto en Max Smeets, 'Cyber Deterrence: The Past, Present, and Future', in: F. Osinga en T. Sweijs (red.), *Netherlands Annual Review of Military Studies 2020* (Den Haag, T.M.C. Asser Press, 2021). Zie: https://doi.org/10.1007/978-94-6265-419-8_20.

Het is dan ook niet verwonderlijk dat de concepten persistent engagement en defend forward, uitgedragen door USCYBERCOM en omarmd in de *Cyber Strategy* van het U.S. Department of Defense (DoD) uit 2018, ook in die termen besproken zouden worden.[7] Voormalig nationale veiligheidsadviseur John Bolton stelde bijvoorbeeld dat offensieve cyberoperaties op basis van deze nieuwe strategie de 'structures of deterrence' zouden creëren.[8] De Cyber Solarium Commission van het Amerikaanse Congres probeerde in 2020 persistent engagement te koppelen aan een strategie van 'layered cyber deterrence'.[9] Jason Healey ontwaart in de Amerikaanse militaire cyberstrategie 'persistent engagement *stability* theory', maar twijfelt daarentegen of de VS daadwerkelijk naleving van bepaalde internationale normen en daarmee stabiliteit kan afdwingen.[10] In hun recente artikel in de *Militaire Spectator* omschrijven Louk Faesen en Deborah Lassche persistent engagement ook als een vorm van afschrikking, waarbij zij wijzen op het risico dat deze Amerikaanse strategie juist tot destabilisering en meer wederzijdse cyberoperaties zal leiden.[11] Een Duitse analyse uit 2019 interpreteerde persistent engagement op soortgelijke wijze als een poging tot afschrikking.[12]

Echter, de geestelijk vaders van persistent engagement en defend forward, Michael Fischerkeller en voormalig *scholar-in-residence* bij USCYBERCOM Richard Harknett, distantieerden zich in 2017 juist expliciet van afschrikking met een artikel getiteld 'Deterrence is Not a Credible Strategy for Cyberspace'.[13] De geestelijk moeder, Emily Goldman, betoogde eerder al dat: 'Persistence is the 180 degree opposite of deterrence'.[14] In de twaalf pagina's van de *USCYBERCOM Command Vision* uit 2018 wordt de term afschrikking slechts twee keer plichtmatig genoemd, waarvan één keer in de uitzonderlijke context van strategische afschrikking van gewapend conflict in den brede.[15] De *Cyber Strategy* van het DoD uit 2018 acht afschrikking vooral nuttig tegen zeer zeldzame 'malicious cyber activities that constitute a use of force'.[16] In een recent artikel van USCYBERCOM-commandant Nakasone en Michael Sulmeyer komt het begrip afschrikking zelfs helemaal niet voor.[17]

FOTO FORT GEORGE G. MEADE

Generaal Paul Nakasone, de commandant van USCYBERCOM en directeur van de National Security Agency

7 Temeer daar USCYBERCOM is voortgekomen uit het U.S. Strategic Command, de hoeder en primaire uitvoerder van de nucleaire afschrikkingsstrategie van de VS.

8 'Bolton: Offensive cyber operations create "deterrence"', in: *The Washington Post*, 31 oktober 2018. Zie: https://www.washingtonpost.com/video/world/bolton-offensive-cyber-operations-create-deterrence/2018/10/31/2552976c-dd44-11e8-8bac-bfe01fcdc3a6_video.html.

9 Zie het rapport van de U.S. Cyberspace Solarium Commission: https://www.solarium.gov/report.

10 Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', in: *Journal of Cybersecurity* 5 (2019) (1). Zie: https://doi.org/10.1093/cybsec/tyz008.

11 L.L.C. Faesen en Deborah Lassche, 'Persistent engagement in het cyberdomein: stabilisatie of escalatie?', in: *Militaire Spectator* 189 (2020) (12) 636-647. Zie https://www.militairespectator.nl/thema/operaties/artikel/persistent-engagement-het-cyberdomein-stabilisatie-escalatie; Hugo Vijver, 'Escalatie, offensieve cybermiddelen en internationaal recht nader bezien' en de reactie van L.L.C. Faesen en Deborah Lassche hierop, in: *Militaire Spectator* 190 (2021) (2). Zie: https://www.militairespectator.nl/thema/meningen-van-anderen/artikel/meningen-van-anderen-discussie-over-persistent-engagement.

12 Matthias Schulze, 'Cyber Deterrence is Overrated: Analysis of the Deterrent Potential of the New US Cyber Doctrine and Lessons for Germany's "Active Cyber Defence"', *Stiftung Wissenschaft und Politik Comment*, augustus 2019. Zie: https://www.swp-berlin.org/10.18449/2019C34/.

13 Michael P. Fischerkeller en Richard J. Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace', in: *Orbis* 61 (2017) (3) 381-393. Zie: https://doi.org/10.1016/j.orbis.2017.05.003.

14 Combined Action Group, USCYBERCOM, *How Understanding Cyberspace as a Strategic Environment Should Drive Cyber Capabilities and Operations*, 26 februari 2013. Zie: https://www.cybercom.mil/Portals/56/Documents/FOIA%20Reading%20Room%20Docs/2013-02-26_Cyberspace_Strategic_Environment_Brief.pdf?ver=2020-01-24-095935-310.

15 USCYBERCOM, *Command Vision*.

16 U.S. Department of Defense, *Summary: Cyber Strategy*, 2018. Zie: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

17 Paul Nakasone en Michael Sulmeyer, 'How to Compete in Cyberspace: Cyber Command's New Approach', in: *Foreign Affairs*, 25 augustus 2020. Zie: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity. Nakasone noemde de term afschrikking bijvoorbeeld ook niet in zijn bijdrage aan de USCYBERCOM Legal Conference 2021. Sulmeyer schreef eerder het artikel 'How the U.S. Can Play Cyber-Offense: Deterrence Isn't Enough', in: *Foreign Affairs*, 22 maart 2018. Zie: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense?cid=soc-tw-rdr.

Persistent engagement en defend forward interpreteren als een vorm van afschrikking is daarom het tegenovergestelde van wat de bedenkers en primaire uitvoerders daarmee bedoelden.

Als alternatief voor het paradigma van oorlogvoering of afschrikking stellen Richard Harknett en Max Smeets dat cyberconflict primair een vorm is van strategische competitie onder de drempel van gewapend conflict.[18] Cyberoperaties worden daarbij nauwelijks ingezet als dwangmiddel in uitzonderlijke crisissituaties.[19] In plaats daarvan is sprake van constante interactie tussen tegenstanders waarbij via *salami slicing tactics* en *death by a thousand cuts* uiteindelijk cumulatieve diplomatieke, informationele, militaire of economische voordelen worden behaald. Of waarbij juist wordt verhinderd dat een tegenstander dergelijke voordelen behaalt. Eerder dan de permanente dreiging van verticale escalatie naar het gebruik van militair geweld draait deze strategische competitie om het bereiken van *faits accomplis* zonder dat een tegenstander dit überhaupt doorheeft of zodanig geprovoceerd wordt dat hij sterk moet reageren.[20]

Een intelligence contest in de context van cyberconflict is te definiëren als een voortdurende competitie om een betere relatieve informatiepositie te behalen ten opzichte van de tegenstander

Een complementair paradigma stelt dat cyberconflict onder de drempel van gewapend conflict (oftewel: vrijwel ál het cyberconflict tot nu toe) het beste als een *intelligence contest* kan worden begrepen, in plaats van als een vorm van oorlog.[21] Dennis Broeders en Sergei Boeke wezen er in 2018 al op dat de literatuur en beleidsdebatten zich te veel op militaire cybercommando's richten, terwijl interstatelijk cyberconflict voornamelijk gevoerd wordt door inlichtingendiensten.[22] Joshua Rovner, een andere voormalige USCYBERCOM-scholar-in-residence, definieert een intelligence contest in de context van cyberconflict als een voortdurende competitie om een betere relatieve informatiepositie te behalen ten opzichte van de tegenstander. Inlichtingendiensten doen dit door meer en betere informatie dan de tegenstander te vergaren, door het moreel, de instituties en de bondgenootschappen van de tegenstander heimelijk te ondermijnen via misleiding, beïnvloeding, verstoring en sabotage, en door inlichtingencapaciteiten te prepositioneren voor een potentieel gewapend conflict.[23] Intelligence contests verlopen echter volgens een andere logica dan gewapende conflicten, al was het maar omdat, zoals Michael Poznansky stelt: 'While wars require some kind of end point, intelligence contests can go on indefinitely'.[24]

Voorstanders van het paradigma van strategische competitie, zoals Harknett en Smeets en

18 Richard J. Harknett en Max Smeets, 'Cyber Campaigns and Strategic Outcomes', in: *Journal of Strategic Studies*, 4 maart 2020. Zie: https://www.tandfonline.com/doi/full/10.1080/01402390.2020.1732354.

19 Bijvoorbeeld Borghard en Lonergan ontwikkelden een theoretisch framework voor hoe cyberoperaties als vorm van dwang (*coercion*) kunnen worden ingezet, maar zij geven tegelijkertijd toe dat dit vooralsnog moeilijk in de praktijk te brengen is. Zie Erica D. Borghard en Shawn W. Lonergan, 'The Logic of Coercion in Cyberspace', in: *Security Studies* 26 (2017) (3) 452-481. Zie: https://doi.org/10.1080/09636412.2017.1306396.

20 Michael P. Fischerkeller, 'The Fait Accompli and Persistent Engagement in Cyberspace', in: *War on the Rocks*, 24 juni 2020. Zie: https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/.

21 Jon R. Lindsay, 'Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-scale Intelligence Problem, in: *Intelligence and National Security* 36 (2021) (2) 260-278. Zie: 10.1080/02684527.2020.1840746.

22 Sergei Boeke en Dennis Broeders, 'The Demilitarisation of Cyber Conflict', in: *Survival* 60 (2018) (6). Zie: https://www.iiss.org/publications/survival/2018/survival-global-politics-and-strategy-december2018january2019/606-09-broeders-and-boeke.

23 Joshua Rovner, 'Cyber war as an intelligence contest', in: *War on the Rocks*, 16 september 2019. Zie: https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

24 Michael Poznansky, 'Covert Action, Espionage, and the Intelligence Contest in Cyberspace', in: *War on the Rocks*, 23 maart 2021. Zie: https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/.

bijvoorbeeld Michael Warner, accepteren de centrale rol van inlichtingenoperaties, maar stellen wel dat cyberconflict meer is dan enkel een intelligence contest. Waar spionage, beïnvloeding en sabotage voorheen een relatief kleinschalige en ondersteunende rol speelden, kunnen zij in het cyberdomein kwantitatief op een dermate grote schaal worden ingezet dat dit een kwalitatief verschil vormt en een strategische impact heeft.[25] Uiteindelijk benadrukken zij echter, net als de auteurs die cyberconflict als een intelligence contest zien, dat deze twee benaderingen goed met elkaar te verenigen zijn.[26] Tevens vormen deze paradigma's een meer accurate beschrijving van de empirische werkelijkheid van cyberconflict tot nu toe dan de benadering van cyberoperaties als dwangmiddel ten behoeve van oorlogvoering of strategische afschrikking.[27]

Persistent engagement en defend forward als contra-inlichtingenstrategie

Hoe passen persistent engagement en defend forward in deze twee benaderingen en hoe brengt USCYBERCOM dit in de praktijk? Zowel in de media als het academisch debat gaat de aandacht tot nu toe vooral uit naar de offensieve USCYBERCOM-operaties waarmee verstoring of sabotage wordt uitgevoerd in het netwerk van een tegenstander, en naar de signaalwerking die daarvan uitgaat. Een meer genuanceerde omschrijving is echter dat persistent engagement en defend forward vooral een continue strijd zijn om het initiatief en een informatievoordeel ten opzichte van de tegenstander. De strategie is daarmee eigenlijk gericht op het inbreken in de OODA-loop van de tegenstander.[28] Daardoor kan intern geanticipeerd worden op vijandelijke activiteiten door de verdediging van de eigen netwerken aan te passen. Extern kan frictie worden veroorzaakt in de operaties van de tegenstander. Het uitvoeren van offensieve verstorings- of sabotageoperaties vormt daarom slechts een klein onderdeel van persistent engagement en defend forward. In plaats daarvan is USCYBERCOM voornamelijk bezig met het verzamelen, analyseren en verspreiden van inlichtingen. Het voortdurend bijstellen van de eigen informatiebeveiliging, het verspreiden van beveiligingsadviezen, het jagen op hackers in netwerken van bondgenoten en het delen van bijvoorbeeld Russische malware met cybersecurityonderzoekers zijn daarmee even karakteristiek voor persistent engagement en defend forward als bijvoorbeeld het uitvoeren van een DDoS-aanval tegen de cyberoperateurs van de Noord-Koreaanse inlichtingendienst.[29]

Persistent engagement en defend forward zijn daarmee primair gericht op het continu actief of passief verstoren of saboteren van de *activiteiten* en *capaciteiten* van een tegenstander. Slechts indirect en na verloop van tijd kan mogelijk een effect op de *intenties* en *besluitvorming* van de tegenstander verwacht worden, in wat Fischerkeller *tacit bargaining* noemt.[30] Zoals Goldman al stelde is dit dus eigenlijk precies het tegenovergestelde van afschrikking, wat juist primair gericht is op het beïnvloeden van die intenties en besluitvorming door het communiceren van een dreigement tot vergelding. Als de strategie van USCYBERCOM toch in de mal van afschrikking geperst moet worden, dan lijkt het door het oogmerk van weerbaarheidsverhoging en het ondermijnen van de capaciteiten van de tegenstander nog het meest op *deterrence-by-denial* in plaats van *deterrence-by-punishment*.

25 Harknett en Smeets, 'Cyber Campaigns and Strategic Outcomes'; Michael Warner, 'A Matter of Trust: Covert Action Reconsidered', in: *Studies in Intelligence* 63 (2019) (4). Zie: https://www.cia.gov/static/d61827122b5a1b8023e0f11678c2edce/Covert-Action-Reconsidered.pdf.

26 Zie het verslag van de 'Policy Roundtable: Cyber Conflict as an Intelligence Contest' van de *Texas National Security Review* van 17 september 2020: https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/#article.

27 Zie bijvoorbeeld Brandon Valeriano *et al.*, *Cyber strategy: the evolving character of power and coercion* (New York, NY Oxford University Press, 2018).

28 OODA: Observe, Orient, Decide, Act.

29 Karen DeYoung *et al.*, 'Trump signed presidential directive ordering actions to pressure North Korea', in *The Washington Post*, 1 oktober 2017. Zie: https://www.washingtonpost.com/world/national-security/trump-signed-presidential-directive-ordering-actions-to-pressure-north-korea/2017/09/30/97c6722a-a620-11e7-b14f-f41773cd5a14_story.html.

30 Michael P. Fischerkeller, *Persistent Engagement and Tacit Bargaining: A Strategic Framework for Norms Development in Cyberspace's Agreed Competition*, Institute for Defense Analysis, 2018. Zie: https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-and-tacit-bargaining-a-strategic-framework-for-norms-development-in-cyberspaces-agreed-competition/d-9282.ashx.

Persistent engagement en defend forward zijn primair gericht op het continu actief of passief verstoren of saboteren van de activiteiten en capaciteiten van een tegenstander

FOTO FORT GEORGE G. MEADE

'Everything old is new again'

Praktisch gezien vormen persistent engagement en defend forward daarom eigenlijk een klassieke contra-inlichtingenstrategie, maar dan toegepast in het cyberdomein.[31] De VS definiëert contra-inlichtingen als: 'identifying, assessing, and neutralizing foreign intelligence activities and capabilities'. Dat USCYBERCOM dit beoogt te doen door zo dicht mogelijk bij of in vijandelijke netwerken te opereren is niks nieuws. In de inlichtingenwereld wordt al eeuwenlang ingezien dat vijandelijke inlichtingenactiviteit niet alleen binnen de te beschermen belangen en organisaties opgespoord moet worden. Het is ook nodig om bronnen te ontwikkelen binnen de vijandelijke inlichtingenorganen waarvan de dreiging uitgaat. Zoals de geschiedenis van cyberconflict laat zien, proberen inlichtingendiensten elkaar al decennialang te hacken of anderszins te compromitteren, om zo *upstream* zicht te krijgen op vijandelijke intenties, activiteiten en capaciteiten, zodat deze *downstream* gemitigeerd kunnen worden.[32] Wie het initiatief en het informatievoordeel heeft, kan dit doen zonder dat die tegenstander hier erg in heeft.

Ogenschijnlijk voegt USCYBERCOM twee nieuwe componenten toe aan deze moderne contra-inlichtingenstrategie, namelijk strategische communicatie en *offensive cyber effects operations* (OCEO). Toch is het de vraag of dit werkelijk kwalitatieve veranderingen zijn.

USCYBERCOM zoekt weliswaar openlijk het contact met de politiek, academische wereld, media en bondgenoten, maar ook de Amerikaanse inlichtingendiensten hebben achter de schermen soortgelijke contacten. Ook laten zij

31 National Counterintelligence and Security Center, *U.S. Counterintelligence Strategy*. Zie: https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022_Executive_Summary.pdf.

32 Zie onder andere Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, Harvard University Press, 2020), Jason Healey en Karl Grindal (red.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013, en Fred Kaplan, *Dark Territory: The Secret History of Cyberwar* (New York, Simon & Schuster, 2016).

de laatste jaren vaker openbaar van zich horen met rapportages over vijandelijke cyber-operaties, malware en modus operandi.[33]

Ook de OCEO die USCYBERCOM uitvoert zijn weliswaar omkleed met de terminologie van militaire *fires and maneuvres*, maar zijn in feite inlichtingenoperaties. Deze operaties zijn vrijwel volledig afhankelijk van de onderliggende inlichtingenpositie, worden grotendeels heimelijk uitgevoerd en zijn gericht op het creëren van bijvoorbeeld onzekerheid, misleiding, vertraging, verstoring en sabotage. Daardoor liggen zij dichter bij traditionele inlichtingenactiviteiten als *covert action* of *active measures* dan bij conventionele militaire operaties.[34] USCYBERCOM opereert weliswaar onder Title 10 (militaire operaties), maar heeft van het Congres de autoriteit gekregen om heimelijk op te treden opdat: 'the role of the United States Government is not apparent or to be acknowledged'.[35] Oftewel: USCYBERCOM kan in het cyberdomein alleen effectief optreden omdat het zich identiek kan gedragen als een inlichtingendienst die onder Title 50 (inlichtingen) opereert.

De USCYBERCOM-operaties tegen vijandelijke cyberactoren die sinds 2018 in de media bekend zijn geworden verschillen dan ook nauwelijks van bijvoorbeeld uitgelekte operaties die de NSA en CIA al langer uitvoerden. Niet toevallig zou onder de Trump-regering ook de CIA, net als USCYBERCOM, ruimere bevoegdheden voor digitale covert action hebben ontvangen.[36] Daarmee zou de CIA bijvoorbeeld een *hack-and-leak*-operatie hebben uitgevoerd tegen een bedrijf dat nieuwe malware ontwikkelde voor de Russische veiligheidsdienst FSB.[37] Ook zou de CIA de identiteit, persoonsgegevens en *hacking tools* van Iraanse hackers verspreid hebben op sociale media.[38] Daardoor werden Russische en Iraanse cyberoperaties tijdelijk verstoord, omdat de cybersecuritygemeenschap ineens op deze nieuwe aanvalstechnieken kon anticiperen. Deze heimelijke operaties zijn dus perfecte voorbeelden van persistent engagement en defend forward, maar toch worden zij noch door de Amerikaanse overheid noch door de media of academici zo omschreven. Politici, ambtenaren, journalisten en wetenschappers lijken geen noodzaak te voelen om deze covert action in een nieuwe terminologie te vatten, omdat dit immers reeds een traditionele inlichtingentaak van de CIA is.

Er zit dus vrijwel geen verschil tussen datgene wat USCYBERCOM sinds 2018 doet en modern contra-inlichtingenwerk tegen vijandelijke cyberdreigingen. USCYBERCOM presenteert zich als een militaire manoeuvre-eenheid, maar opereert met persistent engagement en defend forward praktisch gezien als een inlichtingendienst.[39] Gezien het feit dat USCYBERCOM nog

FOTO FORT GEORGE G. MEADE

Een militair van de Amerikaanse 780th Military Intelligence Brigade houdt toezicht op een operatie. Deze brigade levert een offensieve component aan USCYBERCOM

33 Zie bijvoorbeeld de Twitteraccounts van de NSA (@NSACyber), CIA (@CIA) en UK-NCSC (oftewel GCHQ, @NCSC).

34 Zie bijvoorbeeld Thomas Rid, *Cyber War Will Not Take Place* (Londen, C. Hurst & Co., 2013). Overigens worden ook conventionele en speciale militaire operaties de laatste decennia in steeds sterkere mate door inlichtingen gedreven.

35 Robert Chesney, 'Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate', *Lawfareblog*, 14 december 2018. Zie: https://www.lawfareblog.com/offensive-cyberspace-operations-ndaa-and-title-10-title-50-debate.

36 Zach Dorfman *et al.*, 'Secret Trump order gives CIA more powers to launch cyberattacks', *Yahoo News*, 15 juli 2020. Zie: https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html.

37 Zak Doffman, 'Putin's Secret Intelligence Agency Hacked: Dangerous New "Cyber Weapons" Now Exposed', *Forbes*, 21 maart 2020. Zie: https://www.forbes.com/sites/zakdoffman/2020/03/21/putins-secret-intelligence-agency-hacked-dangerous-new-cyber-weapons-target-your-devices/#2e712396778a.

38 Catalin Cimpanu, 'Source code of Iranian cyber-espionage tools leaked on Telegram: APT34 hacking tools and victim data leaked on a secretive Telegram channel since last month', *ZDNet*, 17 april 2019. Zie: https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/.

39 Lindsay, 'Cyber Conflict vs. Cyber Command'.

Persistent engagement en defend forward zijn niet zo zeer gericht op het behouden of creëren van stabiliteit, maar erkennen dat instabiliteit een fundamentele eigenschap is van het cyberdomein

steeds nauw verbonden is met de National Security Agency (NSA) mag dit geen verbazing wekken. Ook is het bijvoorbeeld geen toeval dat de offensieve component die U.S. Army Cyber Command aan USCYBERCOM bijdraagt gevormd wordt door de 780th Military *Intelligence* Brigade.[40]

Escalatierisico's van persistent engagement en defend forward

Onder meer Jason Healey en Robert Jervis hebben gewaarschuwd dat de assertievere Amerikaanse strategie van persistent engagement en defend forward in bepaalde scenario's kunnen leiden tot horizontale escalatie, oftewel méér wederzijdse cyberoperaties; of verticale escalatie, waarbij cyberoperaties in potentie tot gewapend conflict leiden.[41] Ook zou deze strategie mogelijk de Amerikaanse diplomatieke positie en relaties met de wereldwijde ICT-sector kunnen ondermijnen.[42]

De strategie van persistent engagement en defend forward ziet het cyberconflict tussen de VS en zijn tegenstanders echter niet primair als het potentiële begin van een gewapend conflict, dat dus steeds beheersbaar gehouden moet worden. In plaats daarvan redeneert de nieuwe Amerikaanse benadering vanuit het 'constante contact' dat door digitalisering bestaat tussen geopolitieke tegenstanders.[43] In een langdurige strategische competitie moet cyberconflict daarom ook constant op een steeds fluctuerend intensiteitsniveau gevoerd worden. Zoals eerder werd geconcludeerd is cyberconflict als een vorm van een intelligence contest dan ook niet inherent eindig, maar in potentie permanent. Persistent engagement en defend forward zijn daarom in de kern niet zo zeer gericht op het behouden of creëren van stabiliteit, maar erkennen juist dat een zekere mate van instabiliteit een fundamentele eigenschap is van het cyberdomein. USCYBERCOM accepteert en omarmt die instabiliteit, en benadrukt juist daarom dat engagement *persistent* moet zijn om de primaire doelen van het behouden van het initiatief en het informatievoordeel te kunnen realiseren. Daarmee vergeleken is het bevorderen van strategische stabiliteit door middel van de 'persistent engagement stability theory' die Healey ontwaart[44] of de theorie van 'tacit bargaining' die Fischerkeller oppert[45] hoogstens een afgeleid en secundair doel, voor zover de Amerikaanse overheid dit überhaupt onderschrijft.

USCYBERCOM is zich dus van de escalatierisico's bewust, maar werpt tegen dat het tot nu toe juist de zelfopgelegde terughoudendheid en onderreactie van de VS waren die meer vijandelijke cyberoperaties uitlokten. Daardoor zou de VS al decennialang cumulatieve schade lijden in de strategische competitie waarin het land verwikkeld is. Zoals een Amerikaanse defensiemedewerker zei: 'It's not escalatory. In fact, we're finally in the game.'[46] Wellicht dat dit standpunt inderdaad nadelig zou kunnen uitpakken voor de *soft power* van de VS, maar de

40 Zie de website van de 780th Military Intelligence Brigade van U.S. Army Intelligence and Security Command en U.S. Army Cyber Command: https://www.inscom.army.mil/MSC/780MIB/index.html.

41 Zie bijvoorbeeld Faesen en Lassche, 'Persistent engagement in het cyberdomein: stabilisatie of escalatie?' en Jason Healey en Robert Jervis 'The Escalation Inversion and Other Oddities of Situational Cyber Stability', in: *Texas National Security Review* 3 (2020) (4) 30–53. Zie: https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

42 Faesen en Lassche, 'Persistent engagement in het cyberdomein: stabilisatie of escalatie?'; Vijver, 'Escalatie, offensieve cybermiddelen en internationaal recht nader bezien'.

43 Fischerkeller en Harknett, 'Deterrence is Not a Credible Strategy for Cyberspace'.

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

45 Fischerkeller, *Persistent Engagement and Tacit Bargaining*.

46 Ellen 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.

VS neemt dat kennelijk op de koop toe. Met andere woorden: de risico's van inactie worden gezien als groter dan de risico's van actie.

Ten aanzien van de Amerikaanse relaties met bondgenoten wijst het paradigma van cyberconflict als een intelligence contest daarbij overigens wel op een factor die in elk geval de diplomatieke risico's beperkt. Healey schetst een scenario waarbij USCYBERCOM eigenstandig in bijvoorbeeld Nederlandse infrastructuur of netwerken zou opereren tegen vijandelijke statelijke actoren.[47] Afgezien van het feit dat dit geen accurate weerspiegeling van de operationele realiteit vormt, mag hierboven duidelijk geworden zijn dat het voor USCYBERCOM ondoenlijk zou zijn zich te onttrekken aan de praktijk van reguliere inlichtingensamenwerking. Hugo Vijver wijst daar ook op in zijn recente reactie in de *Militaire Spectator*.[48]

Daardoor zou de Nederlandse soevereiniteit bij operaties van USCYBERCOM adequaat gewaarborgd worden.

Ten aanzien van de Amerikaanse interactie met tegenstanders omvat de logica van intelligence contests ook een factor die escalatierisico's beheersbaar houdt of zelfs beperkt. Persistent

47 Jason Healey, 'The implications of persistent (and permanent) engagement in cyberspace', in: *Journal of Cybersecurity* 5 (2019) (1). Zie: https://doi.org/10.1093/cybsec/tyz008.

48 Vijver, 'Escalatie, offensieve cybermiddelen en internationaal recht nader bezien'.

Amerikaanse militairen oefenen met cyberoperaties. Wat betreft cyberoperaties ziet de VS tegenwoordig de risico's van inactie als groter dan de risico's van actie

FOTO FORT GEORGE G. MEADE

engagement en defend forward zijn niet alleen zélf in feite inlichtingenactiviteiten, maar zijn ook gericht tégen vijandelijke inlichtingenactiviteiten als cyberspionage en digitale active measures. Die activiteiten worden heimelijk en onder voorwaarde van *plausible deniability* uitgevoerd, juist omdat een tegenstander daarmee het risico van escalatie wil verkleinen.[49] Als deze heimelijke activiteiten onverhoopt toch onderkend worden biedt plausible deniability genoeg ambiguïteit om een rem op escalatie te vormen, zelfs als die ontkenning niet geloofwaardig is.[50] Het is maar de vraag of de twee ogenschijnlijke innovaties van USCYBERCOM, strategische communicatie en OCEO, een dusdanig effect hebben op de operationele realiteit en dynamiek van het inlichtingendomein dat grotere escalatierisico's zullen ontstaan. Harknett en Fischerkeller benadrukken dan ook dat: 'The two frameworks [of strategic competition and intelligence contests] agree that escalation is not the dominant strategic interaction dynamic in the cyberspace strategic environment'.[51]

Met die inzichten valt een en ander af te dingen op de interpretatie van Faesen en Lassche van de operatie van USCYBERCOM tegen de Russische trolfabriek Internet Research Agency (IRA) in 2018.[52] Het is bijvoorbeeld de wereld op zijn kop om te suggereren dat het de VS was die hierdoor het risico op escalatie en de legitimering van de 'weaponization of information' veroorzaakt. Het is juist Rusland dat zich onder Poetin verwikkeld acht in een 'informatieconfrontatie' met het Westen en al jarenlang op grote schaal desinformatie en propaganda verspreidt om de cohesie en solidariteit van de NAVO en EU te ondermijnen.[53] Het is juist Rusland dat een 'norm van agressie in vredestijd' tegen het Westen gecreëerd heeft met zijn vele cybersabotageoperaties. De Amerikaanse verstoring of sabotage van de IRA was hierop een reactie, niet de oorzaak. De operatie van USCYBERCOM kan juist gezien worden als signaal dat het gebruik van informatie als wapen níet acceptabel is. Daarnaast zijn er voor zover bekend geen Russische vergeldingsacties uitgevoerd in reactie op deze Amerikaanse verstoringsoperatie en is escalatie dus uitgebleven. Omgekeerd is het effect van USCYBERCOM op de IRA waarschijnlijk ook zeer beperkt en tijdelijk geweest, gezien bijvoorbeeld het aantal IRA-beïnvloedingscampagnes dat Facebook sinds 2018 is blijven identificeren en verwijderen.[54] Geen van beide partijen kan deze strijd op deze manier winnen. Het meeste waar zij op kunnen hopen is dat zij er zo vaak mogelijk in zullen slagen om een tijdelijk voordeel te behalen in dit permanente kat-en-muisspel.

Afschrikking en vergelding op basis van inlichtingenoperaties

Afschrikking in de school van Herman Kahn en Robert Jervis kan mogelijk wel een functie hebben als antwoord op de dreiging van grootschalige cybersabotage van vitale infrastructuur.[55] Dit is een van de weinige vormen van cyberoperaties waarbij wel vergelijkbare effecten als kinetische gewapende aanvallen voorstelbaar zijn.[56]

Rusland treft bijvoorbeeld middels zijn offensieve cyberprogramma doorlopend voorbereidingshan-

49 Poznansky, 'Covert Action, Espionage, and the Intelligence Contest in Cyberspace'.

50 Zie bijvoorbeeld Rory Cormac en Richard J. Aldrich, 'Grey is the new black: covert action and implausible deniability', in: *International Affairs* 94 (2018) (3) 477–494. Zie: https://doi.org/10.1093/ia/iiy067.

51 Michael P. Fischerkeller and Richard J. Harknett, *'Cyber Persistence, Intelligence Contests, and Strategic Competition', Policy Roundtable: Cyber Conflict as an Intelligence Contest*, 17 september 2020. Zie: https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

52 De IRA is inmiddels ook bekend onder de naam Федеральное агентство новостей (Federal News Agency, FAN).

53 Zie bijvoorbeeld Keir Giles, *Handbook of Russian Information Warfare*, NATO Defense College, 2015. Zie: https://www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare.

54 Zie de serie uitstekende onderzoeksrapporten die het bedrijf Graphika hierover heeft gepubliceerd op basis van data van Facebook: https://graphika.com/. Hypothetisch zou overigens gespeculeerd kunnen worden of deze onthullingen door Facebook niet deels tot stand zijn gekomen op basis van informatie die USCYBERCOM aan Facebook heeft doorgesluisd. Dat zou een representatievere en effectievere toepassing van de strategie van persistent engagement en defend forward zijn dan een enkele openlijke DDoS-operatie op de IRA.

55 Zie bijvoorbeeld Herman Kahn, *On escalation: metaphors and scenarios* (Praeger, 1965) en Robert Jervis, 'Deterrence and Perception', in: *International Security* 7 (1982) (3) 3-30. Zie: http://www.jstor.org/stable/2538549.

56 Voor een illustratie van hoe deze dreiging er in de praktijk uitziet, zie bijvoorbeeld Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar - Blackouts in Ukraine were just a trial run. Russian hackers are learning to sabotage infrastructure and the US could be next', in: *Wired*, 20 juni 2017. Zie: https://www.wired.com/story/russian-hackers-attack-ukraine/.

De strijd in de schaduw tussen heimelijke Russische prepositionering voor cybersabotage en westerse tegenmaatregelen is het beste te begrijpen als een intelligence contest

delingen voor dergelijke sabotage tegen Europa.[57] De VS is dit volgens *The New York Times* pas de afgelopen jaren ook tegen Rusland gaan doen.[58] Continentale Europese staten doen dit voor zover bekend echter niet tegen Rusland.[59] Dit zorgt voor een strategische asymmetrie die Rusland kan uitbuiten in een (naderende) politiek-militaire crisis. Omdat continentale Europese staten deze trede op hun escalatieladder missen, kunnen zij niet symmetrisch reageren op Russische cybersabotage. Dit maakt hen kwetsbaar voor de Russische dreiging of zelfs inzet van cybersabotage ten behoeve van afschrikking en escalatiecontrole ('escalate to de-escalate') om een politiek-militaire crisis in een vroeg stadium in het voordeel van Rusland te beslechten.

Het wegnemen van die asymmetrie lijkt op het eerste gezicht wellicht een traditionele militaire taak in plaats van een inlichtingenkwestie, maar het ligt gecompliceerder. Waar bijvoorbeeld nucleaire afschrikking berust op de angst die ingeboezemd wordt door kernraketten die passief op afstand in een onaantastbare raketsilo of onderzeeër paraat staan, is dat in het cyberdomein onmogelijk. De benodigde angst kan alleen gecreëerd worden door de vereiste digitale toegangsposities in vijandelijke vitale infrastructuur via inlichtingenoperaties te verkrijgen en voortdurend actief in stand te houden. Op basis van deze toegang moet vervolgens een expliciet of impliciet dreigement aan de tegenstander geuit worden zonder de onderliggende inlichtingenposities in gevaar te brengen. Omgekeerd kan de angst die een tegenstander veroorzaakt namelijk worden weggenomen door zijn inlichtingenoperaties op te sporen en te mitigeren. Zolang een politiek-militaire crisis zich nog niet aandient, is de strijd in de schaduw tussen heimelijke Russische prepositionering en westerse tegenmaatregelen daarom nog steeds het beste te begrijpen als een intelligence contest. Omdat de voortdurende strijd om het initiatief en het informatievoordeel zorgt voor permanente onzekerheid over de betrouwbaarheid van de sabotagecapaciteit kan er daarnaast in plaats van *mutually assured destruction* hoogstens sprake zijn *mutually uncertain disruption*.

Overigens hoeft USCYBERCOM uiteraard niet enkel volgens de strategie van persistent engagement of defend forward te opereren. De heimelijke OCEO die de Amerikanen naar verluidt zouden plannen als antwoord op de Russische SolarWinds-campagne zouden bijvoorbeeld beter gezien kunnen worden als een poging tot afschrikking door vergelding.[60]

57 Zie bijvoorbeeld het Dreigingsbeeld Statelijke Actoren van de NCTV, AIVD en MIVD: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren en de recente jaarverslagen van de MIVD en AIVD.

58 David E. Sanger and 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.

59 Klinkenberg en Dieker laten bijvoorbeeld zien dat Nederland met de Defensie Cyberstrategie 2018 weliswaar een ambitie heeft uitgesproken op dit gebied, maar deze nog onvoldoende uitgewerkt heeft: J.C. Klinkenberg en J.B. Dieker, 'Geloofwaardige afschrikking in het cyberdomein? Nederland moet doorpakken met strategie tegen cyber én hybride conflictvoering', in: *Militaire Spectator* 190 (2021) (1) 20-27. Zie: https://www.militairespectator.nl/thema/cyberoperations-strategie/artikel/geloofwaardige-afschrikking-het-cyberdomein.

60 David E. Sanger, Julian E. Barnes, Nicole Perlroth, 'Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China', in: *The New York Times*, 7 maart2021. Zie: https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html. Het is op het moment van schrijven overigens nog onduidelijk of dit artikel accuraat is en of de VS werkelijk een heimelijke vergelding zal uitvoeren. Ook blijft de vraag of dergelijke cyberspionage via *supply chains* wel succesvol is af te schrikken, laat staan of dit verstandig is gezien het feit dat de VS waarschijnlijk soortgelijke cyberoperaties tegen Rusland uitvoert.

Conclusie

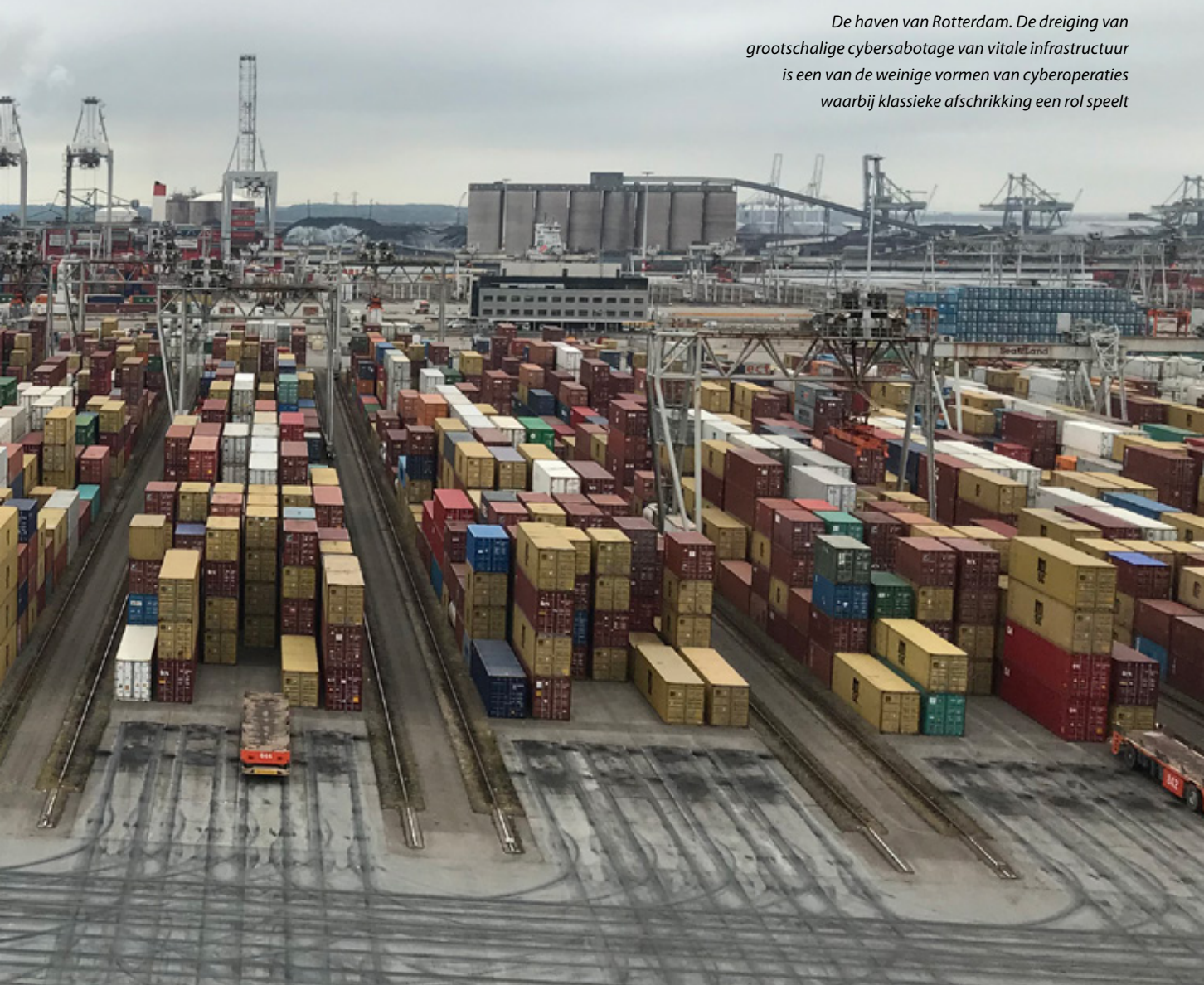
Vanuit het perspectief van inlichtingendiensten is de nieuwe strategie van USCYBERCOM al met al nauwelijks een conceptuele vernieuwing, maar grotendeels juist heel herkenbaar. De meest in het oog springende elementen van persistent engagement en defend forward zijn de intensievere strategische communicatie van USCYBERCOM en het uitvoeren van OCEO. Dit artikel beoogde echter toe te lichten waarom die elementen slechts een relatief beperkt en niet-representatief onderdeel zijn van wat in feite grotendeels een assertieve contra-inlichtingenstrategie is die ook wordt toegepast door bijvoorbeeld de CIA. Het analyseren van persistent engagement en defend forward vanuit de logica van een intelligence contest wijst tegelijkertijd op een van de potentiële problemen voor de strategie van USCYBERCOM die zich de komende tijd kan manifesteren. Succesvolle contra-inlichtingenoperaties leveren reeds grote voordelen op. Kan USCYBERCOM garanderen dat de korte-termijneffecten die het bereikt met openlijke strategische communicatie en OCEO opwegen tegen de aanvullende risico's die dit oplevert voor de onderliggende inlichtingenposities? Deze vraag heeft niet alleen consequenties voor USCYBERCOM zelf, maar ook voor de contra-

FOTO RIJKSOVERHEID

inlichtingenoperaties van andere Amerikaanse inlichtingendiensten.

Een andere vraag is of Nederland actieve steun zou moeten verlenen aan de strategie van USCYBERCOM, of hier eigenstandig gebruik van moet maken, bijvoorbeeld met Europese bondgenoten in het kader van 'strategische autonomie'? Of kan Nederland beter een eigen alternatieve strategie ontwikkelen voor strategische competitie en intelligence contests onder de drempel van gewapend conflict? Als het paradigma van oorlog, dwang en afschrikking minder relevant is voor de huidige strategische omgeving en als escalatierisico's daardoor beperkter zijn dan gedacht, kan Nederland dan wellicht samen met bondgenoten binnen en buiten het cyberdomein assertiever optreden? Welke rol ziet Nederland dan nog voor afschrikking van cyberdreigingen en hoe kan dat worden geoperationaliseerd?

Ongeacht of persistent engagement en defend forward gezien worden als een innovatieve militaire strategie of als een vorm van contra-inlichtingen heeft USCYBERCOM daarom wel een handschoen neergeworpen waarvan gehoopt mag worden dat Defensie deze met verve zal oppakken. ■



De haven van Rotterdam. De dreiging van grootschalige cybersabotage van vitale infrastructuur is een van de weinige vormen van cyberoperaties waarbij klassieke afschrikking een rol speelt