All about access

Inzichten en implicaties van MIVD-cyberoperaties voor digitale slagkracht

De auteurs zijn werkzaam voor de Militaire Inlichtingen- en Veiligheidsdienst en kunnen om veiligheidsredenen hun namen niet noemen.

'Never get involved in a land war in Asia, never go against a Sicilian when death is on the line, and never hack the Dutch.'[1]

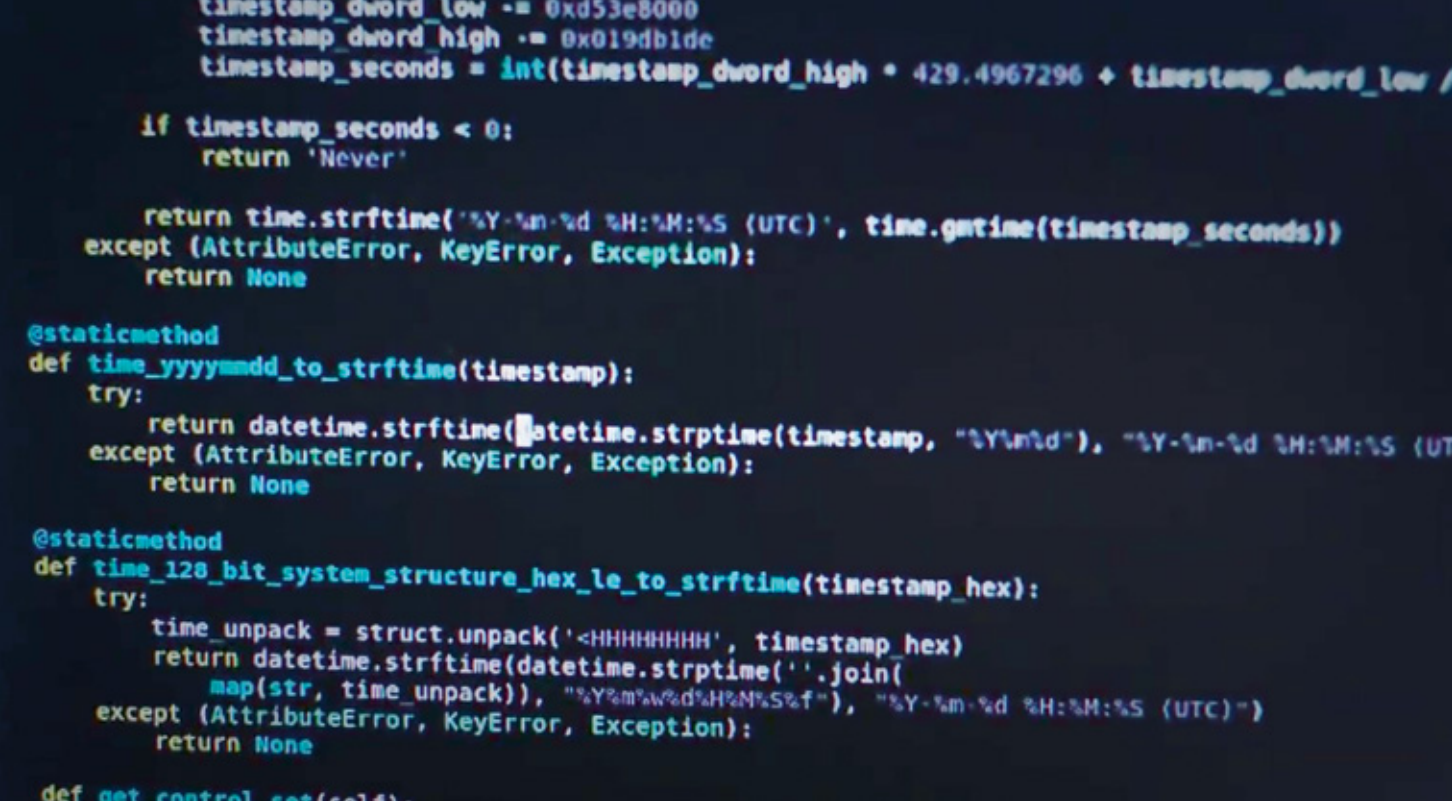
'Also never give them any excuse to hack you. Just don't f-ck with the Dutch in general.'[2]

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en het Defensie Cyber Commando (DCC) hebben in navolging van de *Defensie Cyber Strategie* uit 2018 de samenwerking geïntensiveerd door middel van Cyber Missie Teams (CMT's). De MIVD was al sinds de publicatie van de eerste *Defensie Cyber Strategie* uit 2012 – inmiddels ruim tien jaar geleden – intensief bezig met het uitvoeren van cyberoperaties. In die tijd zijn veel successen geboekt en waardevolle lessen geleerd. Deze inzichten hebben bijgedragen aan het besef dat de verdere operationalisering van het cyberdomein door de krijgsmacht baat heeft bij een nauwere samenwerking. De details daarvan kunnen we normaliter slechts in zeer kleine kring delen omdat we wettelijk verplicht zijn onze bronnen en methoden te beschermen. Toch willen we met dit artikel een aantal ervaringen van de MIVD over het uitvoeren van cyberoperaties delen. Zo hopen we een bijdrage te leveren aan de discussie binnen de krijgsmacht over de conceptuele aard van cyberoperaties en de optimale organisatiestructuur die nodig is voor de uitvoering daarvan.

Dit artikel presenteert daarvoor eerst een aantal inzichten die de MIVD heeft opgedaan tijdens de uitvoering van cyberoperaties voor inlichtingendoeleinden in de afgelopen jaren. Op basis van deze inzichten uit dit type cyberoperaties identificeren we vervolgens een aantal implicaties voor andere typen militaire cyberoperaties. Tot slot wordt vanuit deze inzichten en implicaties het model van de nieuwe Cyber Missie Teams (CMT's) toegelicht, waarin de MIVD en het Defensie Cyber Commando op basis van de *Defensie Cyber Strategie 2018* (DCS2018) zijn gaan samenwerken.

Met dit artikel willen we de aandacht vestigen op de centrale rol die heimelijke inlichtingenactiviteiten spelen in de uitvoering van alle typen militaire cyberoperaties. Wij beargumenteren dat het juist de onderliggende inlichtingen en *access*-posities zijn die de operationele processen en mogelijkheden grotendeels definiëren.

We benadrukken echter graag dat we niet beweren dat het inlichtingenperspectief en de CMT's het enige juiste model voor alle militaire cyberoperaties zijn. Integendeel, wij zijn zeer geïnteresseerd in andere operationele benaderingen van het cyber- en informatiedomein, zoals bijvoorbeeld die van de nieuwe Cyber and Electro-Magnetic Activities (CEMA)-compagnie[3] of het Land Information Maneuver Centre



Access-posities definiëren grotendeels de operationele processen en mogelijkheden van militaire cyberoperaties FOTO WERKEN BIJ DEFENSIE

(LIMC)[4] van de landmacht. Om als krijgsmacht optimaal van de vele mogelijkheden van het cyber- en informatiedomein gebruik te kunnen maken zijn meer van dit soort innovatieve perspectieven nodig. Wij geloven dat ook een normaliter gesloten organisatie als de MIVD daaraan moet bijdragen.

Zes inzichten uit MIVD-cyberoperaties

De MIVD is op grond van artikel 45 van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 bevoegd tot het 'binnendringen van geautomatiseerde werken', oftewel het hacken van netwerken en systemen. Het doel hierbij is om de juiste toegang tot een doelwit te verkrijgen en te behouden waarmee aan een inlichtingenbehoefte kan worden voldaan: de zogenaamde *access*-positie. Dergelijke cyberoperaties worden ook Computer Network Exploitation (CNE) genoemd. Deze cyberoperaties worden uitgevoerd door multidisciplinaire MIVD-inlichtingenteams waar onder andere personeel van de Joint SIGINT Cyber Unit onderdeel van is (de JSCU, die gezamenlijk met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) is opgebouwd). Deze cyberoperaties zijn onderdeel van een *all-source*-inlichtingenproces en kunnen worden ondersteund met andere algemene en bijzondere bevoegdheden, zoals het gebruik van open bronnen, de inzet van agenten en het plaatsen van taps. De MIVD doet dit om inlichtingen te verkrijgen voor onderzoeksopdrachten die zijn geformuleerd door regering en krijgsmacht. De MIVD voert alleen cyberoperaties uit met de goedkeuring van de minister van Defensie en de onafhankelijke Toetsingscommissie Inzet Bijzondere Bevoegdheden (TIB) en onder toezicht van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Hieronder presenteren we een aantal inzichten die in de loop der jaren over dit soort cyberoperaties zijn opgedaan door de MIVD.

1. Cyberoperaties zijn altijd specifiek

Net zoals bij het samenstellen en gereedstellen van eenheden voor een missie is een op maat gemaakte oplossing noodzakelijk die past bij de

1 Joseph Menn, 'Twitter Post', *Twitter*, 16 februari 2021. Zie: twitter.com/josephmenn/status/1361744241291010048.
2 Andy Greenberg, 'Twitter Post', *Twitter*, 16 februari 2021. Zie: mobile.twitter.com/a_greenberg/status/1361748350039646208.
3 Ministerie van Defensie, *Landmacht versterkt met cyber- en elektromagnetische capaciteit*, nieuwsbericht van 9 juli 2021. Zie: https://www.defensie.nl/actueel/nieuws/2021/07/09/landmacht-versterkt-met-cyber--en-elektromagnetische-capaciteit.
4 Ministerie van Defensie, *Land Information Manoeuvre Centre helpt Defensie anticiperen*, nieuwsbericht van 16 november 2020. Zie: https://www.defensie.nl/actueel/nieuws/2020/11/16/land-information-manoeuvre-centre-helpt-defensie-anticiperen.

CEMA-oefening in Marnewaard. Om als krijgsmacht optimaal van de vele mogelijkheden van het cyber- en informatiedomein gebruik te kunnen maken zijn meerdere innovatieve perspectieven nodig

FOTO MCD, JARNO KRAAYVANGER

specifieke omgeving en eigenschappen van het doelwit of het operatiegebied. In het algemeen zijn er geen *one size fits all*-oplossingen en geen *fire-and-forget*-cybercapaciteiten beschikbaar. Een *multirole*-cybercapaciteit, die met kleine variaties in de *payload* overal ter wereld inzetbaar is, is erg zeldzaam in het cyberdomein. Dit betekent dat iedere operatie in feite een individueel en specifiek toegespitst ontwikkeltraject vereist voor de capaciteiten en aanvalstechnieken die ingezet moeten worden.

Het publieke debat en de literatuur over cyberoperaties richten zich vaak op bepaalde *exploits*,[5] *malware* of andere cybercapaciteiten of aanvalstechnieken, omdat derden deze kunnen observeren en onderzoeken. Dergelijke aspecten vormen in de praktijk echter slechts een klein onderdeel van een cyberoperatie. Als het doelwit daadwerkelijk gebruik blijkt te maken van een kwetsbare versie van hardware, software of dienstverlening waar een capaciteit of aanvalstechniek tegen bestaat om binnen te dringen, werkt die meestal slechts tegen één aspect van één verdedigingsschil in één tussenstap richting één doelwit of verzameling van doelwitten. Meestal moet een bepaalde cybercapaciteit of aanvalstechniek daarom worden aangepast of gecombineerd met een grote hoeveelheid andere middelen, of moeten deze zelfs nieuw ontwikkeld worden. De notie van generieke 'cyberwapens', die met beperkte aanpassing tegen een grote hoeveelheid doelwitten in te zetten zijn, is daarom grotendeels incorrect en irrelevant in de praktijk.[6]

5 Een *exploit* is een mogelijkheid om een kwetsbaarheid in software te misbruiken.

6 P.A.L. Ducheine, 'Defensie in Het Digitale Domein', in: *Militaire Spectator* 186 (2017) (4) 164; Thomas Rid en Peter Mcburney, 'Cyber-Weapons', in: *The RUSI Journal* 157 (2012) (1) 6-13; Dale Peterson, 'Offensive Cyber Weapons: Construction, Development, and Employment', in: *Journal of Strategic Studies* 36 (2013) (1) 120-124; E. Tyugu, *Situation Awareness and Control Errors of Cyber Weapons,* IEEE, 2013, 143-148; L. Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations,* IEEE, 2012, 1-19.

2. Cyberoperaties vergen vaak een complexe indirecte benadering

In veel cyberoperaties is het nodig om indirect, via secundaire doelwitten,[7] bij het primaire doelwit uit te komen, omdat dat vaak niet direct benaderbaar is. De reden daarvoor kan zijn dat een doelwit bijvoorbeeld niet direct aan het internet gekoppeld is, of dermate goed beveiligd is dat daar geen kansen liggen. Soms is de reden echter simpelweg dat de technische kenmerken, zoals het IP-adres, in eerste instantie onbekend zijn, of omdat de precieze identiteit van het doelwit überhaupt onduidelijk is. Het verkrijgen van één access-positie om inlichtingen te kunnen verzamelen over een primair doelwit, zoals een vijandelijk communicatiesysteem, kan op deze manier een heel scala aan afzonderlijke all-source-inlichtingenoperaties tegen secundaire doelwitten vereisen. Deze noodzaak tot indirect handelen en het moeten combineren van verschillende suboperaties maakt het operationele proces daarom vaak bijzonder complex.

3. Cyberoperaties zijn tijdrovend

Net zoals een verkenningseenheid met een Unmanned Aerial Vehicle (UAV) een tijdrovend gereedstellingstraject kent van fysieke, conceptuele tot mentale component, vergt een cyberoperatie meestal ook een lang voorbereidingstraject. Er moet verkend worden welke kwetsbaarheden er in de netwerken en apparaten van een doelwit zitten, de vereiste toestemmingen moeten aangevraagd worden, de technische handelingen moeten worden gepland en uitgevoerd, de access-posities moeten verkregen en uitgebouwd worden, er moet bestudeerd worden hoe het netwerk of systeem van een doelwit is geconfigureerd en men moet uitzoeken waar de ene naald in een hooiberg te vinden is die de volgende operationele stap mogelijk maakt of de inlichtingenbehoefte vervult. Vanwege de noodzaak van een indirecte benadering zoals hierboven beschreven moet dit proces vaak parallel worden doorlopen, tegen meerdere doelwitten tegelijk.

De vele stappen in dit proces, gecombineerd met de hierboven genoemde specificiteit en complexiteit van cyberoperaties, zorgen voor vele onderlinge afhankelijkheden en operationele knelpunten, die bijna per definitie veel tijdverlies creëren. Er zijn altijd uitzonderingen en soms kan er wel zeer snel gehandeld worden als er reeds een solide basis ligt. De meeste cyberoperaties kosten echter maanden, zo niet jaren om succesvol uit te voeren.

De notie van generieke 'cyberwapens' is grotendeels incorrect en irrelevant in de praktijk

4. Cyberoperaties vereisen permanent geïntegreerd werken

De integratie die (samengestelde) militaire eenheden op missie kennen op stafniveau is ook een vereiste voor het uitvoeren van cyberoperaties: planning, techniek, uitvoering en analyse zijn niet van elkaar te scheiden. Juridische toestemming om te hacken op basis van artikel 45 Wiv 2017 kan bijvoorbeeld alleen worden verkregen en behouden op basis van gedetailleerde kennis van het doelwit, de omgeving en volledig begrip van de eigen technische capaciteiten. De inzet van deze bijzondere bevoegdheid wordt immers alleen toegestaan als de operatie zo gericht mogelijk is en er een juiste afweging van noodzakelijkheid, proportionaliteit en subsidiariteit plaats heeft gevonden. Dit noopt tot nauwe en intensieve technische, (data-)analytische en operationele samenwerking tussen verschillende betrokken afdelingen in de planningsfase van een cyberoperatie. Ook betekent dit dat de ervaring, creativiteit en langdurige inzet van het betrokken personeel doorslaggevend is.

7 In de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (Wiv 2017) staat dit bekend als een zogeheten *non-target* of 'derde'.

Succesvolle cyberoperaties draaien daarom om intrinsieke, impliciete kennis die slechts in beperkte mate in expliciete vorm overdraagbaar is. Deze intrinsieke, impliciete kennis bestaat bijvoorbeeld uit de ervaring met de (historische) configuratie van het doelwitnetwerk of systeem, de variabele datastromen daarbinnen, het digitale gedrag van gebruikers, de veiligheidsmaatregelen die getroffen worden binnen een systeem en de wijze waarop gebruikers communiceren.

5. Cyberoperaties kennen altijd hoge politieke afbreukrisico's

Bij een cyberoperatie is de kans groot dat de primaire en verscheidene secundaire doelwitten zich op verschillende plekken in de wereld bevinden en gebruik maken van verschillende wereldwijde communicatiestromen. Dit is een van de redenen dat er vaak meerdere ondersteunende cyberoperaties en andere all-source-inlichtingenoperaties tegelijkertijd uitgevoerd worden met een uitwerking in verschillende geografische locaties en dus verschillende nationale jurisdicties. Tevens is altijd een kans aanwezig op onbedoelde *spillover*-effecten, de mogelijkheid van onderkenning van onze heimelijke activiteiten en (digitale) nevenschade bij het hacken van netwerken en systemen van primaire en secundaire doelwitten in verschillende landen. Doordat data(verkeer) op internet en binnen netwerken en systemen van het doelwit zo makkelijk gelogd en bewaard kan worden kunnen cyberoperaties ook lang na afloop nog onderkend worden ('the internet does not forget').

Een MIVD-inlichtingenteam opereert vanuit Nederland wereldwijd in het cyberdomein, maar bij onderkenning zijn de MIVD of andere Nederlands belangen andersom ook vanuit de hele wereld via het cyberdomein aan te grijpen. Om al deze redenen is bijna per definitie sprake van hoge politiek-bestuurlijk afbreukrisico's die zich wereldwijd en tot ver in de toekomst kunnen manifesteren.

6. Heimelijk optreden is altijd een vereiste

Omdat het succesvol verkrijgen en in stand houden van een access-positie praktisch gezien alleen mogelijk is als het doelwit hiervan onwetend is, bestaat net zoals bij sommige andere inlichtingensensoren bij cyberoperaties de sterke relatie tussen heimelijkheid en effectiviteit. Een access-positie kan daarbij het beste vergeleken worden met een heimelijke observatiepost op een doelwit van bijvoorbeeld special operating forces (SOF). Als een access-positie eenmaal onderkend is, kan deze betrekkelijk eenvoudig onschadelijk gemaakt worden door een doelwit.

De relatie tussen heimelijkheid en effectiviteit bij de cyberoperatie of heimelijke observatiepost is anders dan bij een inlichtingensensor zoals een fotoverkenningssatelliet of UAV, die een tegenstander weliswaar kan ontwijken door zijn fysieke verplaatsingen aan te passen, maar die hij in vredestijd zelf meestal niet zomaar uit kan schakelen. Met dergelijke inlichtingensensoren kunnen tevens openbare effecten gegenereerd worden zonder dat dit de effectiviteit van de capaciteit negatief beïnvloedt, bijvoorbeeld door het tonen van *imagery intelligence* (IMINT) in een sessie van de VN-Veiligheidsraad. Een dergelijk onderscheid tussen effectiviteit en heimelijkheid bestaat niet bij cyberoperaties. Daar is de afstand tussen de inlichtingensensor, de access-positie, en het doelwit bijna nul.

Het in stand houden van heimelijkheid is niet alleen noodzakelijk om het succes van één operatie in het heden, maar ook het eigen voortzettingsvermogen in de toekomst te garanderen door de eigen modus operandi te beschermen. Op niet-herleidbare of niet-merkbare wijze optreden is ook noodzakelijk om de hoge politieke-bestuurlijke afbreukrisico's beheersbaar te houden, zowel in Nederland als richting buitenlandse partners. Heimelijkheid is daarmee van fundamenteel belang om succesvol in het cyberdomein te kunnen opereren.

Zeven implicaties voor andere militaire cyberoperaties

MIVD-cyberoperaties zijn dus vaak complex, specifiek ontworpen, tijdrovend, politiek gevoelig en kennen een noodzaak tot perma-

Het verkrijgen van één access-positie die inlichtingen kan verzamelen over een primair doelwit kan een heel scala aan afzonderlijke all-source-inlichtingenoperaties tegen secundaire doelwitten vereisen

FOTO WERKEN BIJ DEFENSIE

nente integratie van disciplines en het gebruik van heimelijkheid. Dit zijn niet alleen inherente eigenschappen van cyberoperaties die bedoeld zijn om inlichtingen te vergaren (CNE-operaties), maar ook van andere soorten cyberoperaties waarbij op afstand, in meerdere jurisdicties, gedurende langere periode tegen omvangrijke en complexe doelwitten geopereerd moet worden. Deze eigenschappen gaan grotendeels ook op voor de *Computer Network Attack* (CNA)-operaties die binnen de doelstelling van het Defensie Cyber Commando vallen. Ook is de verwachting dat deze inzichten relevant zijn voor cyberoperaties die gericht zijn op het creëren van andersoortige militaire effecten, zoals hypothetische *cyber-enabled*-informatieoperaties en psychologische operaties die de krijgsmacht mogelijk in de toekomst wil kunnen uitvoeren. De implicaties van bovenstaande inzichten onderstrepen echter dat dergelijke cyberoperaties op een aantal cruciale punten afwijken van traditionele fysieke militaire operaties.

1. Cyberoperaties draaien om access-posities

Net zoals bij kinetische militaire operaties is het effect leidend, bij cyberoperaties dicteert de access-positie de effecten die behaald kunnen worden. Zonder toegang kun je niets. Access-posities zijn daarom de *conditio sine qua non* bij de inzet van cyberoperaties om een effect te kunnen bereiken. Of dat nu gaat om het verkrijgen van bepaalde vertrouwelijke militaire informatie van een tegenstander, het misleiden van een tegenstander, of het loslaten van een destructief virus dat alle harde schijven in een communicatienetwerk wist zodat een tegenstander niet meer kan functioneren. Dat betekent dat de juiste access-positie de bepalende factor is die de operatie definieert, vormgeeft en dicteert welke effecten behaald kunnen worden.

Offensieve cyberoperaties zijn daarom eerst en vooral inlichtingenoperaties; dat wil zeggen, operaties gericht op het heimelijk verkrijgen van

een access-positie. Volgens verschillende modellen van cyberoperaties bestaat 83 tot 94 procent van een cyberoperatie uit het verkrijgen van een access-positie (CNE-operatie).[8] In de overige 6 tot 17 procent vindt differentiatie plaats naar gelang het gewenste effect, bijvoorbeeld het verkrijgen van inlichtingen, verstoring of manipulatie (CNA-operatie).[9] Op basis van bijna 10 jaar cyberoperaties kan de MIVD deze percentages beamen.

2. Access-posities zijn moeilijk over te dragen

De afhankelijkheid van intrinsieke, impliciete kennis maakt dat een CNE-access-positie van een MIVD-inlichtingenteam niet zomaar over te dragen is aan een effectbrenger die een CNA-operatie wil uitvoeren of CNE-operatie wil overnemen. De CMT's uit de DCS2018 worden gezien als een mogelijke oplossing voor dit probleem. Het overdragen is gecompliceerd omdat dit bijvoorbeeld geen kwestie is van het overdragen van de inloggegevens en werking van een *command-and-control*-server (C2-server) waarmee een doelwitnetwerk is gepenetreerd door de MIVD. Dergelijke expliciete informatie is alleen bruikbaar in combinatie met de langdurig opgebouwde impliciete kennis over het doelwit en zijn omgeving. De effectbrenger is in zo'n geval bekend met de inrichting en de werking van het netwerk of systeem van het doelwit, heeft de vereiste ervaring met heimelijk opereren in dit netwerk, en kent de bredere context en de relaties van het doelwit met secundaire doelwitten. Geïntegreerde samenwerking is noodzakelijk om opeenvolgende CNE- en CNA-operaties succesvol te laten uitvoeren.

3. Ook CNA vereist heimelijk optreden

De noodzaak van niet-herleidbaar en niet-merkbaar optreden geldt ook voor cyberoperaties die bedoeld zijn om een merkbaar effect te veroorzaken, zoals CNA. Zelfs voor het concept van *loud cyber*, waar de laatste jaren over gediscussieerd is in de literatuur, is dit onontbeerlijk.[10] Bij loud cyber communiceert een actor zijn vermogen om een effect te genereren in een vijandelijk netwerk of neemt een actor politieke verantwoordelijkheid voor het effect van een operatie. Of wordt bijvoorbeeld relatief openlijk gedreigd dat de vitale infrastructuur van een ander land gehackt is en gesaboteerd kan worden.[11] De heimelijkheid van de gebruikte modus operandi tot het verkrijgen van de gebruikte access-positie blijft echter cruciaal, zelfs als een cyberoperatie onderdeel is van een relatief openlijke militaire missie. Indien de directe tegenstander of derde partijen met sterke SIGINT-capaciteiten te veel zicht krijgen op de gehanteerde modus operandi heeft dit namelijk direct impact op de mogelijkheid tot uitvoering van het aangekondigde effect, het voortzettingsvermogen van andere gelijktijdige cyberoperaties en het uitvoeren van toekomstige cyberoperaties.

Op het eerste gezicht vormen *Distributed Denial of Service*-operaties (DDoS) hierop wellicht een uitzondering. Daarmee hoeft niet in de netwerken of systemen van een doelwit binnengedrongen te worden om een acces-positie te verkrijgen. In plaats daarvan kan bijvoorbeeld een website of internetverbinding van een doelwit tijdelijk onbruikbaar gemaakt worden door deze van buitenaf te overspoelen met grote hoeveelheden dataverkeer. DDoS-operaties

8 Zie: Eric M. Hutchins, Michael J. Cloppert en Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains* (Washington, D.C., Academic Conferences and Publishing International Limited, 17-18 Maart, 2011); Marc Laliberte, 'A Twist on the Cyber Kill Chain: Defending Against a Javascript Malware Attack', *Darkreading*, 21 september 2016. Zie: www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952; Corey Nachreiner, 'Kill Chain 3.0: Update the Cyber Kill Chain for Better Defense', *Helpnetsecurity*, 10 februari 2015. Zie: www.helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chain-for-better-defense/; Blake D. Bryant en Hossein Saiedian, 'A Novel Kill-Chain Framework for Remote Security Log Analysis with SIEM Software', in: *Computers & Security* 67 (2017); MITRE, 'ATT&CK: Tactics', MITRE. Zie: www.attack.mitre.org/tactics/enterprise/; Paul Pols, 'The Unified Kill Chain: Designing a Unified Kill Chain for Analyzing, Comparing and Defending Against Cyber Attacks', Cyber Security Academy, 2017.

9 Pols, 'the Unified Kill Chain'.

10 Zie bijvoorbeeld: Max Smeets en Herbert Lin, 'Offensive Cyber Capabilities' (Tallinn, NATO CCD COE Publications, 10th International Conference on Cyber Conflict, 2018) 63; Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', in: *Strategic Studies Quarterly* 12 (2018) (3) 100; Herbert Lin, 'Attribution of Malicious Cyber Incidents: From Soup to Nuts', in: *Aegis Paper Series* (2016) (1607) 44; Herbert Lin, 'Still More on Loud Cyber Weapons', *Lawfareblog*, 19 oktober 2016. Zie: www.lawfareblog.com/still-more-loud-cyber-weapons; Timothy M. Goines, 'Overcoming the Cyber Weapons Paradox', in: *Strategic Studies Quarterly* 11 (2017) (4) 86-111, 87-88; Nicole Softness, 'How Should the U.S. Respond to a Russian Cyber Attack?', in: *Yale Journal of International Affairs* 12 (2017) (Spring) 105.

11 David E. Sanger en Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid', *The New York Times*, 15 juni 2019.

kunnen juist wel snel en op ad-hocbasis ingezet worden. Echter, om de benodigde hoeveelheid dataverkeer te kunnen genereren moet een actor ofwel een groot aantal systemen van willekeurige derde partijen hacken en in een botnet[12] samenbrengen, ofwel deze capaciteit van criminele actoren huren, ofwel de medewerking afdwingen van grote telecommunicatieaanbieders. Met andere woorden: ook een DDoS-capaciteit berust op een aantal access-posities die met heimelijke inlichtingenoperaties moeten worden opgebouwd.

De heimelijkheid van modus operandi tot het verkrijgen van access-posities blijft cruciaal

4. Cyberoperaties vereisen andere planningscycli

De uitvoering van een complexe cyberoperatie is in tijd vergelijkbaar met een complexe langlopende militaire operationele inzet. Cyberoperaties hebben geen planningscycli van uren, dagen of weken. Na de tijdrovende gereedstelling en ontplooiing kan een onderzeeboot in relatief korte tijd binnen een operatiegebied manoeuvreren en daar een verscheidenheid aan doelwitten onschadelijk maken. Een soortgelijke inzet is voor cyberoperaties nauwelijks voorstelbaar. Alleen wanneer *ex ante* reeds een hoogstaande access-positie is bewerkstelligd bij een doelwit kunnen cyberoperaties een effect sorteren in een tijdspanne die vergelijkbaar is met die van een gereedgesteld en ontplooid fysiek wapensysteem. Het ex-ante-element is in de regel echter zo tijdrovend dat dit beter te vergelijken is met de inzet van het logistieke, juridische, operationele plannings- en trainingsproces dat maanden van tevoren start om die onderzeeboot op de juiste tijd in het operatiegebied te krijgen.

5. Cyberoperaties overstijgen gebruikelijke militaire mandaten

De bovenstaande implicaties betekenen dat cyberoperaties zowel in tijd als ruimte het beste vergeleken kunnen worden met een complexe langlopende militaire operationele inzet, zoals een meerjarig artikel-100-mandaat.[13] Het is immers nodig om ruim voortijds te kunnen starten met de opbouw van de juiste access-posities. Aangezien dit een inlichtingenoperatie betreft is dit momenteel alleen maar mogelijk onder de Wiv 2017. Heimelijk optreden is voor de rest van de krijgsmacht weliswaar mogelijk tijdens een militaire operatie, bijvoorbeeld onder artikel 100 of via de MKSO-procedure,[14] maar de structurele en wereldwijde inzet van het soort bijzondere bevoegdheden die voor een cyberoperatie nodig zijn blijft in de huidige juridische context voorbehouden aan de MIVD.[15]

Het is daarom een operationele realiteit dat het verkrijgen en behouden van de vereiste CNE-access-posities om een militair CNA-effect te genereren in de huidige juridische context alleen mogelijk is voor de MIVD onder de Wiv 2017.

6. Traditionele niveaus van optreden zijn beperkt relevant bij cyberoperaties

21e-eeuwse militaire doctrine heeft het gebruik van de napoleontische niveaus van militair optreden geïnstitutionaliseerd en het operationele niveau toegevoegd.[16] Zoals omvat in het

12 Een botnet is een groep gehackte systemen (bots) die door een actor als één geheel kan worden aangestuurd, bijvoorbeeld om een DDoS-operatie uit te voeren.

13 Artikel 100 Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815; Artikel 51 Handvest van de Verenigde Naties; Artikel 5 Noord-Atlantisch Verdrag.

14 P.A.L. Ducheine en K. Arnold, 'Besluitvorming Bij Cyberoperaties', in: *Militaire Spectator* 184 (2015) (2).

15 Het mandaat van een militaire operatie is immers geografisch beperkt.

16 Ministerie van Defensie, *Nederlandse Defensie Doctrine* (Den Haag, Ministerie van Defensie, 2019) 27-33; Martin Dunn, 'Levels of War: Just a Set of Labels?'. Zie: www.clausewitz.com/readings/Dunn.htm; Larence M. Doane, 'It's just Tactics: Why the Operational Level of War is an Unhelpful Fiction and Impedes the Operational Art', *Small Wars Journal*, 24 september 2015. Zie: www.smallwarsjournal.com/jrnl/art/it%E2%80%99s-just-tactics-why-the-operational-level-of-war-is-an-unhelpful-fiction-and-impedes-the-.

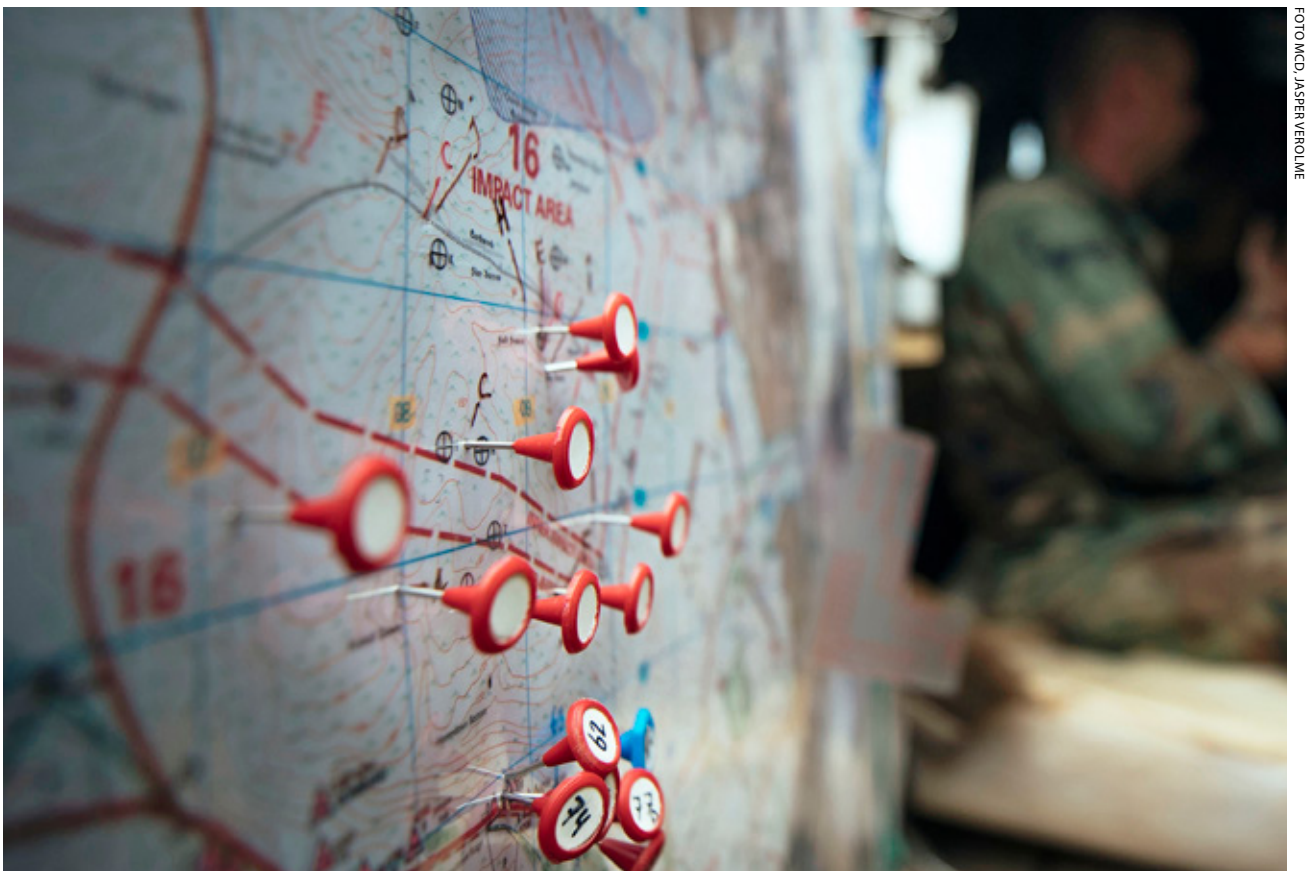


FOTO MCD, JASPER VEROLME

Cyberoperaties zijn slechts in beperkte mate te vatten in geografische of chronologische afbakeningen

controversiële maar veelgebruikte concept van de *strategic corporal*[17] is de categorisering van militaire activiteiten naar niveau van optreden onder druk van technologie echter steeds gecompliceerder geworden (strategische compressie). Het onderscheid tussen enerzijds een afgebakende, op zichzelf staande 'strategische' cyberoperatie, en anderzijds een 'operationele' of 'tactische' cyberoperatie, waarvoor de verantwoordelijkheid gedelegeerd kan worden naar een lager commandovoeringniveau is daardoor regelmatig problematisch. In de praktijk wordt meestal op al deze drie niveaus tegelijkertijd geopereerd bij het soort cyberoperaties dat we hier behandelen (uitgevoerd op afstand, in meerdere jurisdicties, gedurende langere periodes, tegen omvangrijke of complexe doelwitten). Het onderscheid in niveaus verliest hierdoor sterk aan betekenis.[18] Zoals hierboven aangegeven zijn dit soort cyberoperaties ook slechts in beperkte mate te vatten in geografische of chronologische afbakeningen. Daardoor zijn militair-doctrinaire constructen die militaire activiteiten vatten in 'tijd en ruimte', en daardoor ook de verdeling in niveaus van optreden,[19] vaak betekenisloos in het kader van dergelijke cyberoperaties. Voor het succesvol integreren

17 Charles C. Krulak, 'The Strategic Corporal: Leadership in the Three Block War', in: *Marines Magazine* (1999); Franklin Annis, 'Krulak Revisited: The Three-Block War, Strategic Corporals, and the Future Battlefield', *Modern War Institute*, 3 februari 2020. Zie: https://mwi.usma.edu/krulak-revisited-three-block-war-strategic-corporals-future-battlefield/; Walter Dorn en Michael Varey, 'Fatally Flawed: The Rise and Demise of the "Three-Block War" Concept in Canada', in: *International Journal* 63 (2008) (4) 967-978.

18 Voor de internationaalrechtelijke discussies omtrent soevereiniteit is deze geografische afbakening wel van invloed, zie bijvoorbeeld: Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, Cambridge University Press, 2017) 11-27.

19 Koninklijke Landmacht, *Doctrine Publicatie 3.2: Landoperaties* (Amersfoort, Land Warfare Centre, 2014) 6-21 tot 6-27.

van cybercapaciteiten in de krijgsmacht moeten de niveaus van optreden als organisatiemodel waar nodig losgelaten kunnen worden.[20]

7. Cyberoperaties zijn geen *silver bullet*

Tot slot vormen de inzichten die de MIVD heeft opgedaan een waarschuwing voor onrealistische verwachtingen. Vrijwel ieder aspect van onze maatschappij is gedigitaliseerd, waardoor volgens de wet van Hypponen in theorie ook alles kwetsbaar wordt: 'Whenever an appliance is described as being smart, it's vulnerable'.[21] In de praktijk bestaat er echter een directe relatie tussen enerzijds de benaderbaarheid en kwaliteit van de beveiliging van een doelwit, en anderzijds de tijd en moeite die het kost om hierbinnen te dringen. Juist de meest aantrekkelijke doelwitten voor militaire cyberoperaties,[22] zoals wapen- en C4ISR-systemen, maar ook vitale infrastructuur, zijn in de praktijk vaak niet direct benaderbaar, zijn zeer goed beveiligd en hebben een zeer obscure interne werking, waardoor het zeer veel tijd en moeite kost om de benodigde access-posities te verkrijgen om deze ook aan te kunnen grijpen. Cyberoperaties zijn bij sommige doelwitten niet kosten-efficiënt uit te voeren, omdat de vereiste capaciteit en operationele mogelijkheden simpelweg ontbreken.

Vier voordelen geïntegreerde samenwerking

In de DCS2018 is gekozen voor een nieuw samenwerkingsmodel dat zowel MIVD als DCC beter in staat moet stellen zijn rol te vervullen. Voorstelbare militaire cyberoperaties stellen immers andere eisen aan de organisatiestructuur omdat zij in hoge mate gedefinieerd worden door de onderliggende access-posities, grotendeels heimelijk moeten worden uitgevoerd, andere planningscycli kennen, traditionele geografische en chronologische mandaatkaders overstijgen en de vereiste impliciete kennis niet makkelijk overdraagbaar is van de inlichtingencomponent naar de uitvoerende component.

Het integratiemodel van het CMT weerspiegelt deze eigenschappen en maakt het daarom significant realistischer om daadwerkelijk tijdig de gewenste digitale slagkracht te leveren. Door een CMT te vormen waarin operationele capaciteit van het DCC samengevoegd is met een MIVD-inlichtingenteam, kan de CNE-operatie ten behoeve van het verkrijgen van de access-positie voor een CNA-operatie geïntegreerd plaatsvinden. Figuur 1 beschrijft dit proces. Dit model maakt zo ook steeds een goede juridische waarborging mogelijk, omdat het verkrijgen en behouden van de allesbepalende access-posities onder de Wiv 2017 plaatsvindt en daardoor het toezichtstelsel van toepassing is. Wij identificeren hieronder vier voordelen die mogelijk worden door dit CMT-samenwerkingsmodel.

1. Realisme in voorbereidingstijd

Door het CMT-samenwerkingsmodel kunnen de militaire CNA-effecten die de krijgsmacht nodig heeft, zoals het aangrijpen van C4ISR-systemen en wapensystemen, gegenereerd worden vanuit access-posities die ruim vóór een missie zijn verkregen. Dit kan enkel op basis van gezamenlijke CNE-operaties onder de Wiv 2017. De 'offensieve component' is beperkt tot de fase waarin het CNA-effect daadwerkelijk gegenereerd wordt: de eerdergenoemde differentiatiefase die 6 tot 17 procent van een cyberoperatie beslaat. Daarna moet het geïntegreerde team terugvallen op de Wiv 2017 aangezien de *battle damage assessment* (BDA) van een CNA-operatie waarschijnlijk alleen plaats kan vinden vanuit access-posities verkregen door CNE-operaties onder de Wiv.

2. Integratie in militaire planning

In dit samenwerkingsmodel kunnen gewenste militaire cybereffecten in een zo vroeg mogelijk stadium en via de reguliere procedures vertaald

20 Hierbij is het overigens ook voor ons nog de vraag hoe de cyberoperaties van de CEMA-compagnie van de landmacht zich precies verhouden tot het soort cyberoperaties die de MIVD uitvoert.

21 Mikko Hypponen, 'Hypponen's Law', *Twitter*, 12 december 2016. Zie: twitter.com/mikko/status/808291670072717312.

22 Ministerie van Defensie, 'NAVO-Top: Nederland Nog Altijd Achter Halen 2%-Norm', *Ministerie van Defensie*, 11 juli 2018; Marno de Boer en van Teeffelen Kristel, 'Een Brug Kun Je Hacken in Plaats Van Bombarderen', *Trouw*, 25 maart 2017; Ministerie van Defensie, 'Defensie Vergroot Slagkracht Tegen Cyberdreiging', *Ministerie van Defensie*, 12 november 2018.

Verregaande strategische samenwerking tussen DCC en MIVD is de beste weg voorwaarts voor offensieve digitale slagkracht

worden naar een inlichtingenbehoefte door de Commandant der Strijdkrachten (CDS), die kan worden opgenomen in de meerjarige operationele planning van de MIVD én DCC. Een geïntegreerd CMT van MIVD en DCC werkt dan met een planningselement, vanaf een zo vroeg mogelijk stadium samen met de CDS, zodat het te verwachten cybereffect vervolgens daadwerkelijk in de militaire planning geïntegreerd kan worden.

3. Integrale ervaring- en kennisopbouw
De MIVD en DCC-samenwerking in volledig geïntegreerde CMT's onder het mandaat van de Wiv 2017 vormt een oplossing voor fysieke, culturele en organisatorische hordes en institutionele afstand tussen DCC en MIVD. Door volledig geïntegreerd samen te werken wordt de vereiste intrinsieke, impliciete kennis van een access-positie opgebouwd bij de MIVD én het DCC; en het personeel van het DCC levert niet alleen tijdens, maar ook voor en na een militaire cyberoperatie een betekenisvolle bijdrage.

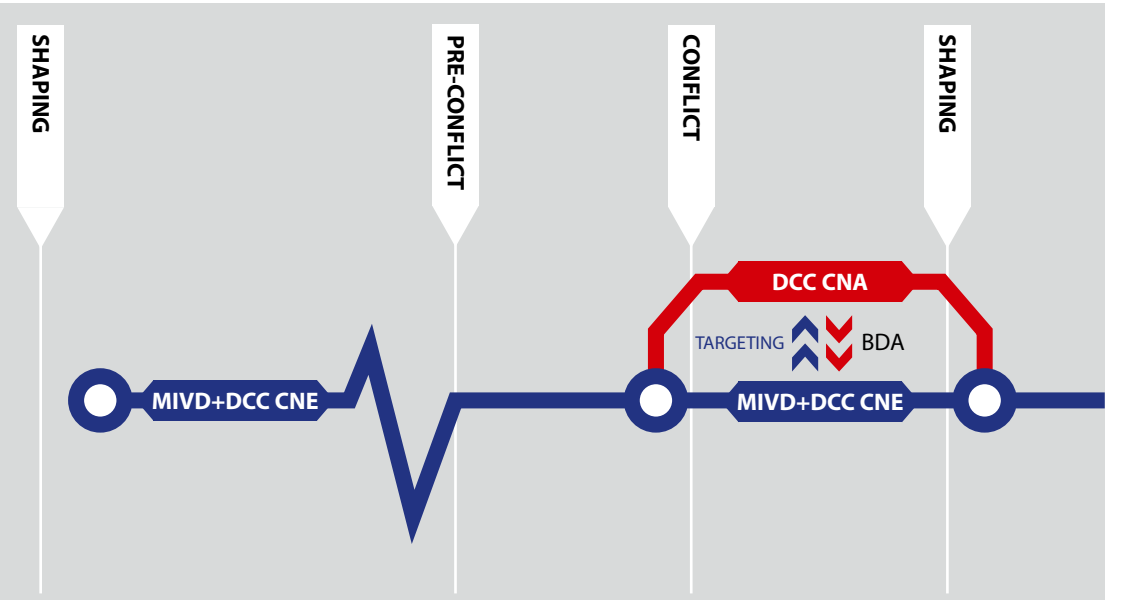
4. Versterking offensieve digitale slagkracht
Ten vierde leidt de intensivering van de samenwerking tussen het DCC en de MIVD tot een toename van de beschikbare cybercapaciteit binnen zowel het DCC als de MIVD. Het resultaat van een dergelijke integratie zal meer zijn dan de som der delen. Bovenal kan op deze manier het DCC militair cybervermogen en digitale slagkracht genereren voor de krijgsmacht als geheel. Ook stelt het de MIVD beter in staat zijn onderzoeksopdrachten te vervullen.

Conclusie

Gezien de geschetste inzichten uit de praktijkervaring van de MIVD en de implicaties daarvan voor andere militaire cyberoperaties zijn de gezamenlijke DCC-MIVD CMT's een ontwikkeling in de juiste richting die grote voordelen biedt. CMT's zijn wat ons betreft niet de beste oplossing, maar wel de enige manier in de bestuurlijk context ten tijde van de DCS2018. Het integratiemodel van het CMT omarmt de inherente eigenschappen van het cyberdomein, in plaats van dat hier met traditionele organisatiestructuren tegenin gegaan wordt. Verregaande strategische samenwerking tussen DCC en MIVD is de beste weg voorwaarts om de gewenste offensieve digitale slagkracht voor de krijgsmacht te genereren. Zo draagt het DCC effectief bij aan het verkrijgen van de access-posities via CNE-operaties die het later tijdens een inzet nodig zal hebben ten behoeve van SOF voor effecten in of via cyberspace. Wij zien daarnaast geen inherente redenen waarom dit samenwerkingsmodel niet ook mogelijk is voor andere krijgsmachtonderdelen, zoals SOF- of JISTARC-eenheden.

Wij gaan uit van eigen kracht en een oplossing die is toegesneden op de specifieke Nederlandse context. Wij zijn hierboven dan ook bewust niet ingegaan op de organisatie- en samenwerkingsmodellen die in andere landen gebruikt worden. Dat laat overigens onverlet dat de bondgenoten aan wie Nederland zich spiegelt een samenwerkingsmodel volgen waarbij cybercommando's nagenoeg volledig geïntegreerd zijn bij de respectievelijke inlichtingen en/of veiligheidsdiensten. Met andere woorden: die hebben nog diepere samenwerking dan het CMT-samenwerkingsmodel.

Nergens anders ter wereld, bij onze bondgenoten noch bij onze tegenstanders, staan de CNE- en de



Figuur 1 Het voorgestelde samenwerkingsmodel MIVD en DCC waarbij gezamenlijk in een CMT CNE-operaties voorbereid worden voor, tijdens en na conflict ten behoeve van, onder andere, DCC CNA-operaties. Vanuit de lopende CMT CNE-operaties worden mogelijkheden ontwikkeld voor CNA-operaties die door de DCC-component binnen het geïntegreerde team worden uitgevoerd tijdens een mogelijk conflict. Als de CNA-operatie het Wiv-mandaat overstijgt, vindt de CNA-operatie plaats onder 'CDS-mandaat'. De impliciete intrinsieke kennis voor targeting-doeleinden vloeit voort uit de CMT CNE-operaties en voedt de CNA-operaties, het zijn immers dezelfde personen die samen de CNE-operatie hebben opgezet. De battle damage assessment (BDA) wordt na de CNA-operatie hoogstwaarschijnlijk gedaan vanuit de CMT CNE-operaties.

CNA-component van offensieve digitale slagkracht op zulke grote institutionele afstand van elkaar als in Nederland. Nederland is op andere cyberveiligheidsterreinen op dit moment een van de meest vooruitstrevende en volwassen landen ter wereld, zoals het bevorderen van publiek-private samenwerking, het bijdragen aan de (door)ontwikkeling van een internationaal normatief kader, én het leveren van cyberinlichtingen.[23] Dat is voor een groot deel te danken aan het pragmatisme, het realisme en de gerichtheid op operationele effectiviteit die Nederland meestal eigen zijn.

Het CMT-samenwerkingsmodel uit de DCS2018 beoogt hetzelfde mogelijk te maken voor het genereren van offensieve digitale slagkracht. Het verkleinen van de institutionele afstand tussen MIVD en DCC door de ontwikkeling en implementatie van geïntegreerde CMT's kan wel nog sneller en intensiever. Daarvoor hebben we heel de krijgsmacht nodig. Zowel het DCC als de MIVD wordt namelijk deels gevuld met personeel uit de OPCO's. Om traditionele kaders los te laten en de CMT's tot een succes te maken is begrip nodig van de onderliggende ontwikkelingen en inzichten die aan de DCS2018 ten grondslag hebben gelegen. Dit artikel beoogt aan dat begrip en de verdere conceptuele discussie binnen de krijgsmacht bij te dragen. Zodat DCC en MIVD zich ten behoeve van de krijgsmacht, Nederland en onze bondgenoten nog meer kunnen richten op datgene wat uiteindelijk het hoogste belang zou moeten zijn: operationele effectiviteit en digitale slagkracht in het cyberdomein. ■

23 'The Hague Program for Cyber Norms', *The Hague Program for Cyber Norms*. Zie: www.thehaguecybernorms.nl/about-us; Schmitt, *Tallinn Manual 2.0*, 2-6; 'Bevelhebber Krijgsmacht: Nederland in Champions League Cyberwereld', *Security.nl*, 9 december 2019. Zie: https://www.security.nl/posting/634606/Bevelhebber+krijgsmacht%3A+Nederland+in+Champions+League+cyberwereld; Huib Modderkolk, *Het is Oorlog Maar Niemand Die Het Ziet* (Amsterdam, Podium, 2019).

* Saskia Pothoven is promovendus bij de Nederlandse Defensie Academie en werkt hiernaast bij de Bestuursstaf van het ministerie van Defensie. Dit artikel met een specifiek Nederlandse invalshoek is voortgekomen uit een uitgebreider Engelstalig artikel van de auteur over hetzelfde onderwerp voor een internationaal publiek, getiteld: 'Producer-Client Paradigms for Defence Intelligence'. Dit artikel is in juni gepubliceerd in *Defence Studies: Journal of Military and Strategic Studies*.