Cyber: 'People, people, people'

Vragen over het DDC en het inzetten van cyberactiviteiten

Max Smeets

Dit artikel is een reactie en vooral toevoeging op 'Hackers, wiz kids, en offensieve cyberoperaties. Uitdagingen voor het Defensie Cyber Commando' door Sergei Boeke in de vorige editie van dit tijdschrift.

De bespiegelingen van Sergei Boeke over de uitdagingen van het Defensie Cyber Commando (DCC) vormen een bedachtzaam stuk over het uitvoeren van cyberactiviteiten. Het artikel is een bruikbaar startpunt over dit onderwerp. Boeke gaat in zijn beschouwing voornamelijk in op één vlak waar het DCC lijkt te onderpresteren: 'governance'. Meer specifiek is de stelling dat het DCC te maken heeft met diverse uitdagingen rondom het integreren van inlichtingen en oorlogvoering in het cyberdomein. Dit vormt inderdaad een kritiek punt zonder een 'perfecte' oplossing — ik heb eerder over dit organisatorische dilemma een presentatie gehouden op de *NATO CCD COE CyCon* en een gereviseerd artikel over deze kwestie gepubliceerd in Defense Studies.[1]

Er worden echter diverse kwesties door Boeke onbesproken gelaten die wel degelijk het bekijken waard zijn. Ik richt me op enkele van de belangrijkste operationele overwegingen die een rol spelen bij het beoordelen van het functioneren van het DCC.

People, People, People

Op een conferentie van het Royal United Services Institute (RUSI) twee jaar geleden verklaarde een militaire cybercommandant dat het grootste probleem bij het uitvoeren van effectieve operaties bestaat uit 'people, people, and people'.[2] Voor een overheid is het aantrekken van de meest talentvolle mensen niet goedkoop — vooral niet als iemand de kans krijgt om voor een veel hoger salaris in de commerciële sector te werken. Signal intelligence-eenheden zijn altijd op zoek naar mensen die technisch goed onderlegd zijn — zelfs vóór het digitale tijdperk. Bovendien is de vraag naar mensen die code kunnen interpreteren en schrijven in de laatste decennia uitzonderlijk gestegen. Aangezien banen voor coderen in vele sectoren populair zijn, kunnen deze mensen eenvoudig overstappen naar de private sector. Hierdoor is het voor de overheid veel moeilijker om deze mensen te behouden.

Het is tevens lastig om de beste en meest ingevoerde hackers te 'kopiëren'. Zoals John Lospinoso, momenteel de technisch directeur van de eenheid voor toolontwikkeling van US Cyber National Mission Force, verklaart: "Er is sprake van een grote aanwas van latente aanleg en motivatie in de pool van technische talenten in de militaire sector. De beste militaire hackers hebben jarenlang nachten en weekenden besteed aan het lezen en schrijven van blogs, het bijdragen aan open-source softwareprojecten, het bijwonen van

conferenties en cursussen, lezen van boeken en vooral het uitvoeren van talloze missies. Niemand heeft nog uitgedokterd hoe zo'n mix van vaardigheden en ervaring op welke manier dan ook kan worden gekopieerd, afgezonderd van training on-the-job".[3] Dit probleem bestaat niet alleen in de Verenigde Staten. Het aanbieden van een doorlopend, intensief ontwikkelingsprogramma voor militaire functionarissen zonder een flinke technische achtergrond is voor alle overheden een kostbare zaak — Nederland vormt daarop geen uitzondering.

Herken de beperkingen van de private sector

Gezien dit tekort en de kosten om deskundigheid aan te trekken, is het DCC afhankelijk van input vanuit de private sector om effectief in het cyberdomein werkzaam te zijn. Na een training gevolgd te hebben bij het bedrijf Fox-IT, worden opgeleide hackers vervolgens een jaar geplaatst bij een organisatie in de private sector om meer praktische ervaring te verkrijgen voordat ze bij het DCC in dienst komen. Het DCC heeft ook samenwerkingsverbanden met bedrijven als Thales, KPN en Certified Secure en bouwt op reserve-eenheden: deze bestaan uit civiele 'cyberspecialisten' waar het DCC op kan rekenen als het hulp nodig heeft.

Vaak is er niets mis om samen te werken met de private sector — in sommige gevallen is het inderdaad uitermate wenselijk, zoals diverse onderzoekers en beleidsmakers al hebben aangetoond. Maar we moeten duidelijk zijn over de beperkingen en risico's bij het te veel vertrouwen op dit soort invloed vanuit deze sector. Het voornaamste punt is het aanzienlijke verschil tussen nationale cyberactiviteiten en pentesten (binnendringingstest) of zogeheten red-teaming die in de sector worden uitgevoerd.

Een aanzienlijke ontwikkeling in de afgelopen twee decennia betreft de opkomst van commercieel beschikbare 'exploit frameworks' en andere specifieke hulpmiddelen voor het helpen standaardiseren van processen. In 2003 creëerde H.D. Moore het bekende Metasploit Project om de threat intel sector een open-sourcetool te bieden voor het ontwikkelen van exploits en hulpmiddelen. Het project leidde tot het Metasploit Framework, een geavanceerd en gratis open-sourceplatform dat een grote verzameling van exploits, payloads en andere activiteiten integreert om diverse taken voor de aanvaller te automatiseren. Andere varianten bestaan, zoals Canvas van Immunity en Core Impact van Security Technologies. Enkele van deze platforms zijn gratis, andere zijn commercieel beschikbaar.

Het financiële district in New York. Voor een overheid die wil investeren in cybercapaciteit is het moeilijk om te concurreren met de private sector (foto: Jason Thibault)

Afbeelding: Flickr/Blogtrepeneur

Er zijn ook veel kleinere hulpmiddelen op de markt die het automatiseren van onderdelen van het aanvalsproces ondersteunen.

Maar deze tools zijn vaker wel dan niet beperkt inzetbaar voor een meer ontwikkeld militair cybercommando. Op de eerste plaats wordt een tool die wijdverspreid beschikbaar komt ondertekend en sneller opgemerkt door diverse antivirus- of Endpoint Detection and Response (EDS)-hulpmiddelen in het doelnetwerk.

Ten tweede zit er een andere bedoeling achter het toolontwerp en -gebruik. Standaardisatie is belangrijk voor de private sector, aangezien bedrijven werken met factureerbare uren en de reikwijdte van het project meestal beperkt is. In zo'n wereld zijn de tijdsbesparingen van 'exploit frameworks' en andere tools van onschatbare waarde. Bij geavanceerde nationale activiteiten vormt tijd niet de bepalende factor: het behouden van de geheimhouding en flexibiliteit wordt hoger ingeschaald. Bij frameworks die worden gebruikt door de private sector is dit een stuk moeilijker.

Ook zullen indien vereist meer volwassen organisaties hun eigen frameworks gebruiken om opsporing te voorkomen en deze afstemmen op hun specifieke behoeften. In 2016 en 2017 was er een groep genaamd de Shadow Brokers, naar men zegt verbonden aan de Russische overheid, die diverse hulpmiddelen voor hacking van de NSA lekte, waaronder een krachtig framework als Fuzzbunch. Het framework heeft diverse eenvoudig toepasbare plug-ins die worden onderverdeeld in verschillende categorieën. Fuzzbunch heeft veel modulaire mogelijkheden, waardoor het eenvoudig is om modules toe te voegen en te verwijderen.

Dit betekent in het beste geval dat wanneer pentesters (of andere getrainde experts die eerder geplaatst waren bij bedrijven in de private sector) worden ingeschakeld, zij moeten wennen aan de nieuwe operationele omgeving. In het slechtste geval kunnen mensen uit de private sector die een organisatie binnenstappen geen 'slechte' gewoonten afleren en zijn ze als onderdeel van de nationale overheidsactiviteiten niet in staat zich aan te passen aan de verschillende elementen van de taak. De National Security Agency (NSA), een geheime dienst op nationaal niveau van het Amerikaanse ministerie van Defensie, maakt zich hier zorgen om en leidt klaarblijkelijk liever ingenieurs en wiskundigen op tijdens meerjarige programma's.

Het DCC heeft te maken met extra operationele overwegingen als het gaat om het inzetten van reserves. De sleutel voor het effectief opereren in cyberspace ligt in het beter begrijpen van netwerken dan je tegenstander (er bestaat simpelweg geen gouden 'tool' of 'functie' voor een ultieme cyberverdediging of -aanval).[4] Het beveiligen van een systeem vereist veel kennis van het systeem dat wordt verdedigd. Zodra reserve-eenheden worden ingezet, zullen ze veel tijd moeten spenderen om goed ingevoerd te raken in de netwerken die worden verdedigd voordat ze een waardevolle bijdragen kunnen bieden. Zoals een rapport van RAND verklaart, vereisen "aanvallende cyberspace-activiteiten regelmatig veel voorbereiding, maar moeten ze bij aanvang van het conflict [...] buiten beschouwing worden gelaten. Er zijn beperkingen rondom het soort hulp dat een externe groep kan aanbieden bij het volledig geïnformeerd raken."[5] Hoewel het in het algemeen aanlokkelijk is om reserve-eenheden op te roepen om het personeelstekort van DCC op te vangen, is het veel moeilijker dan vaak wordt erkend om deze expertise efficiënt toe te passen.

DCC-vereisten

Het is belangrijk om te contextualiseren wanneer Nederland begon te denken over 'cyber offense'. In 2013-2014 bereikte het budget van de Nederlandse krijgsmacht een historisch dieptepunt (zelfs lager dan na de Beurskrach van 1929),

toen de uitgaven aan defensie slechts net boven één procent van het bruto nationaal product uitmaakten. Na decennialang snijden in defensie-uitgaven besloot de overheid om Taskforce Cyber (DCC's voorganger) op te richten, dat verantwoordelijk was voor het coördineren en opzetten van een eerste militaire eenheid om aanvallende cyberactiviteiten uit te voeren.

De brief van toenmalig minister van Defensie Hans Hillen op 8 april 2011 aan de Tweede Kamer biedt waarschijnlijk de beste beschrijving van de context waarin het Nederlandse standpunt over militaire cyberactiviteiten naar voren kwam. De brief begint als volgt: "Het niveau van het nationale budget dwingt de overheid om drastische maatregelen te nemen."[6] De brief vermeldt vervolgens een waslijst van diverse besparende maatregelen. Maar de minister van Defensie verklaart dat "Een krijgsmacht die zich niet op de toekomst voorbereidt, kwetsbaar is. Daarom is het belangrijk om ook in de komende jaren ruimte voor intensiveringen en innovatie te scheppen." Een van de voornaamste oplossingen: 'cyber'. In de woorden van minister Hillen: "Cyber is voor de krijgsmacht een wapensysteem in ontwikkeling. Om de inzetbaarheid van de Nederlandse krijgsmacht te waarborgen en zijn effectiviteit te verhogen, zal defensie haar digitale weerbaarheid de komende jaren versterken en het vermogen ontwikkelen tot het uitvoeren van cyberactiviteiten."

In 2012 werd aangekondigd dat Taskforce Cyber verspreid over vier jaar 50 miljoen euro zou ontvangen.[7] De meeste officiële documenten suggereren dat het jaarbudget van het DCC niet boven de 15-20 miljoen euro uitkomt. Het doel van het DDC is om een personeelsbestand van maximaal 200 mensen te hebben. Maar zoals Boeke desalniettemin al opmerkte, zit het huidige aantal daar ver onder (ca. 80-100 medewerkers, inclusief reserves).

Dat is een uiterst beperkt budget en team om effectief in deze sector actief te zijn (er zijn natuurlijk vele andere vereisten voor het DCC om efficiënt te opereren, waaronder de juiste tools en infrastructuur).

Neem alleen de personeelsvereisten in ogenschouw. Het DCC moet ontwikkelaars in dienst nemen die malware moeten 'maken', bouwen en inzetten, voor toolkits etc. Ze hebben operators nodig voor het gebruik van de malware. Systeembeheerders zijn nodig voor betrouwbaar onderhoud, configuratie en het beheren van computers en servers. Ondersteuning vanuit de frontoffice is belangrijk om bij de activiteiten van de hierboven genoemde teams te assisteren — bijvoorbeeld voor het aanmaken van accounts of online de mogelijkheden op te zoeken. Het DCC heeft ook een 'leger' van analisten (zowel kwantitatief als kwalitatief), administratieve krachten (voor human resources, samenwerkingen met andere overheidsfunctionarissen, media etc.), juridische deskundigen en strategische denkers nodig.

Zelfs als we ervan uitgaan dat het DCC i) de beste en intelligentste medewerkers heeft; ii) het een ongelooflijke 'lean' organisatie is (dat betekent dat er geen overtolligheid van menselijk kapitaal is); en iii) alle mensen binnen de organisatie op een uiterst gecoördineerde en efficiënte manier laat werken is het nog steeds moeilijk te bevatten hoe het DCC effectief kan opereren.

Specifieker, met dit budget en personeelsbestand, kan het DCC het deelnemen aan militaire cyberactiviteiten zeker continueren. Het kan zelfs af en toe een gerichte cyberoperatie uitvoeren 'to disrupt, deny, degrade, or destroy' — potentieel naast het toepassen van de gebruikelijke militaire krachten of andere nationale capaciteiten. Door zijn 'fysieke' cyberafdeling kan het de wereld ook tonen dat Nederland innovatief is en klaar voor moderne oorlogvoering. Desalniettemin kan, tenzij het publiekelijk bekende budget en personeelsbestand onjuist zijn, Nederland niet actief opereren tegen verschillende actoren in een gegeven tijdsinterval.

Bovendien kunnen budgetbeperkingen en het tekort aan personeel uitmonden in slechte methoden. Denk bijvoorbeeld aan het hergebruiken van code voor aanvallende cyberactiviteiten. Het opnieuw inzetten van code uit voorgaande operaties kan tijd en geld besparen. Zelfs de meest ontwikkelde entiteiten binnen de sector hebben dit in het verleden gedaan (zie bijvoorbeeld Kaspersky Lab's analyze van Equation Group). Hoewel het een efficiënte oplossing lijkt bij een tekort aan vaardigheden, kan het hergebruiken van code een slecht idee zijn voor eenheden die zorgvuldig en 'stealthy' te werk willen gaan.[8] Codestrings worden vaak voor opsporingsdoeleinden 'ondertekend' door geheime diensten of overheidsinstanties, wat betekent dat het ontdekken van de capaciteiten veel waarschijnlijker is als de code overlapt.

Conclusie

Zoals journalist David Sanger van *The New York Times* opmerkt in zijn recente boek *The Perfect Weapon*, wordt 'cyber' in tegenstelling tot de meeste recente militair gerelateerde technische ontwikkelingen — zoals drones — gewoonlijk niet beschouwd als een uitbreiding van andere wapens.[9] De unieke aard van 'cyber' maakt het onmogelijk om organisatorische sjablonen van andere

militaire eenheden naar het DCC te kopiëren en plakken. Het DCC — zelfs als het leert van andere nationale entiteiten — zal onmiskenbaar moeten leren via trial-and-error. We hebben een gedeelde verantwoordelijkheid — beleidsmakers, academici en de private sector — om ervoor te zorgen dat de leercurve van het DCC via kritische analyses en discussies zo steil mogelijk verloopt.

Dr. Max Smeets is onderzoeker en lecturer in cyberveiligheid aan de Universiteit van Stanford. Hij is tevens verbonden aan de Universiteit van Oxford en New America, een denktank in Washington, D.C. Hij is te volgen op Twitter: @SmeetsMWE.

Wilt u reageren?
Mail de redactie: redactie@atlcom.nl.

1. Max Smeets, 'Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks', *NATO CCD COE Publications*, 2017 9th International Conference on Cyber Conflict: https://ccdcoe.org; Max Smeets, 'Integrating offensive cyber capabilities: meaning, dilemmas, and assessment', *Defense Studies*, 18:4 (2018) 395-410.
2. Senior Military Cyber Commander, 'The Second International Cyber Symposium: Cyberspace and the Transformation of 21st Century Warfare', The Royal United Services Institute (RUSI) (Church House, Westminster: London), 19-20 Oktober 2016.
3. Josh Lospinso, 'Fish out of the Water: How the Military Is an Impossible Place For Hackers, And What To Do About it', *War on the Rocks*, (12 juli 2018): https://warontherocks.com.
4. Rob Joyce, 'Disrupting Nation State Hackers', USENIX Enigma 2016: https://www.usenix.org.
5. Martin C. Libicki, David Senty, Julia Pollak, 'H4cker5 Wanted: An Examination of the Cybersecurity Labor Market', (Rand Corporation: 2014): https://www.rand.org.
6. Minister van Defensie, 'Defensie Cyber Strategie', Kamerstuk 33 321:1, (27 juni 2012): https://zoek.officielebekendmakingen.nl/kst-33321-1.html.
7. Cyril Rosman, 'Nederlandse leger op zoek naar een cyberwapen', BN De Stem, (29 mei 2013): https://www.bndestem.nl.
8. Voor meer informatie: Max Smeets, 'A Matter of Time: On the transitory nature of cyberweapons', *Journal of Strategic Studies*, 41(2018)1-2.
9. David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, (New York: Penguin Random House: 2018).

COLOFON

Nummer: 6 / 2018 Jaargang 42
tijdschrift voor internationale betrekkingen en veiligheidspolitiek

Atlantisch Perspectief is een uitgave van de Stichting Atlantische Commissie ingeschreven bij de Kamer van Koophandel Haaglanden onder nummer 41149134. *Atlantisch Perspectief* verschijnt 6x per jaar

Bureau & Redactie
Emmapark 12
2595 ET Den Haag
telefoon: 070 363 94 95
fax: 070 364 63 09
e-mail: redactie@atlcom.nl
internet: www.atlcom.nl

Eindredacteur
Maarten Katsman

Begunstigerschappen
Begunstigers van de Atlantische Commissie ontvangen Atlantisch Perspectief. Kijk voor de tarieven van de verschillende begunstigerschappen op www.atlantischecommissie.nl

Opgave schriftelijk of elektronisch bij het bureau van de Atlantische Commissie.

Vormgeving
Arthur Meyer; M/vG ontwerpers

Opmaak & Druk
Quantes, Den Haag
ISSN-nr.: 0167-1847

Losse en voorgaande nummers van *Atlantisch Perspectief* zijn te verkrijgen bij de Atlantische Commissie.
Advertentietarieven zijn te bevragen bij de redactie.