Hackers, wiz kids, en offensieve cyberoperaties

Uitdagingen voor het Defensie Cyber Commando

Sergei Boeke

Wat heeft het Defensie Cyber Commando (DCC) de afgelopen jaren succesvol uitgevoerd, en waar liggen de uitdagingen?

In 2014 is het Defensie Cyber Commando (DCC) met veel fanfare door de minister van Defensie opgericht. Deze nieuwe eenheid kreeg als taak het uitvoeren van militaire operaties in cyberspace. Cyberspace wordt immers door veel krijgsmachten beschouwd als het vijfde domein voor oorlog voeren (naast land, zee, lucht en de ruimte), en niemand betwist dat toekomstig (militair) conflict een sterke cybercomponent zal bevatten. Het DCC bestaat inmiddels uit ongeveer tachtig man, waarvan meer dan twee dozijn hackers, opgeleid door FOX-IT. Afgelopen juni vond de eerste commando-overdracht van de eenheid plaats. Hierbij droeg eerste commandant generaal Hans Folmer het vaandel over aan commodore Elanor Boekholt-O'Sullivan, en werd het DCC anders opgehangen in de krijgsmachtorganisatie — nu direct onder de Commandant der Strijdkrachten (CDS).[1] Binnenkort wordt een nieuwe 'Defensie cyberstrategie' gepubliceerd, die een grotere nadruk op afschrikking legt. Afschrikking draait immers om attributie en een geloofwaardige capaciteit (en politieke wil) om terug te slaan, waardoor een agressor afziet van een bepaalde actie. Het is derhalve opportuun om nu het DCC onder het vergrootglas te leggen, en te kijken hoe ver Nederland is in het genereren van offensieve cybercapaciteit. Voor zover meetbaar, wat heeft het DCC afgelopen jaren succesvol uitgevoerd, en waar liggen de uitdagingen?

De opbrengsten van het DCC zijn op dit moment nog mager. Dit is deels te verklaren door de lange aanlooptijd die genomen is om te kunnen experimenteren; op zich een goede insteek. Cyber is een nieuw militair domein en de organisatie heeft tijd nodig om zich aan te passen. Er is wel degelijk capaciteit opgebouwd voor wat betreft kennis, trainingen en opleidingen, al loopt het traag. Zo zijn bijvoorbeeld amper 40 van de beoogde 150 cyberreservisten aangesteld. Wel is een belangrijke nevendoelstelling gerealiseerd: het 'normaliseren' van militaire cyberoperaties. Als militaire cyberoperaties, uitgevoerd in overeenstemming met het internationaal recht, doelwitten kunnen uitschakelen (of uitzetten) zonder het veroorzaken van doden of fysieke schade — wat is hierop tegen? Een vaak gebruikt voorbeeld is het potentieel uitzetten van de luchtafweersystemen van de tegenstander. Maar dit blijkt in de praktijk lastiger uit te voeren dan te beschrijven in doctrines of scenario-oefeningen. Het vermogen om hoogwaardige doelen uit te schakelen is derhalve nog niet aanwezig in het DCC. De oorzaak ligt bij een probleem op het gebied van *governance*.

Inlichtingenoperatie versus militaire actie

Een groot probleem ligt op het raakvlak tussen twee werelden: inlichtingenoperaties en militaire operaties. Beide hebben verschillende besluitvormingstrajecten voor inzet, andere organisatieculturen en afwijkende modus operandi. Voor militaire inzet is een besluit van de regering nodig. Er is ook een minder openbaar traject mogelijk, waarbij de Ministeriele Kerngroep Speciale Operaties een besluit tot inzet neemt.[2] Daarentegen wordt een inlichtingenoperatie gemandateerd door de Wet op de Inlichtingen en Veiligheidsdiensten (WIV 2017). Het inbreken in systemen of netwerken kan worden toegestaan als dit proportioneel en noodzakelijk is voor de nationale veiligheid. Dit wordt gedaan door de Joint Sigint Cyber Unit (JSCU) van de AIVD en MIVD. Het DCC mag dit tijdens vredestijd niet. Maar het aangrijpen van een doelwit — en dat vernietigen — is voorbehouden aan Defensie, en kan weer niet via de WIV. Naast deze twee verschillende wettelijke kaders zijn ook de modus operandi en organisatieculturen van belang. Militairen opereren in de regel 'overt'; dat wil zeggen zichtbaar. Zij dragen een uniform, en moeten volgens het internationaal recht herkenbaar zijn (als combattant van een bepaald land) tijdens gevechtssituaties. Er is een internationaal erkend juridisch kader (onder meer de Haagse & Geneefse Conventies) dat bepaalt wat niet geoorloofd is in gewapend conflict. De inlichtingenwereld opereert op een fundamenteel andere wijze. Het internationaal recht zegt weinig over spionage, en als landen klassiek militaire of politieke spionage uitvoeren in het buitenland, dan overtreden ze de wetten van de staat die slachtoffer is. Tegenwoordig blijken deze twee verschillende werelden, strikt gescheiden qua wettelijk kader (zie bijvoorbeeld de discussie in de VS over Title 10 versus Title 50 authority), steeds moeilijk uit elkaar te houden in de praktijk. Nergens geldt dit meer dan in cyberspace.

Een cyberaanval kan in een kwestie van seconden een organisatie platleggen, luidt het populaire gezegde. Men vergeet echter dat de voorbereiding maanden in beslag kan nemen, en dat de aanval op het laatste moment nog door een onvoorziene *software patch* of *systems-upgrade* verijdeld kan worden. Rob Joyce, het toenmalige hoofd van de Tailored Access Operations (TAO) van de Amerikaanse National Security Agency (NSA), legt in een mooi YouTube-filmpje uit hoe *nation state*-hackers te werk gaan.[3] Uiteindelijk moeten ze een gehard netwerk, vaak één dat niet verbonden is aan het internet (gescheiden door een

Brigadegeneraal Hans Folmer draagt het commando van het Defensie Cyber Commando over aan commodore Elanor Boekholt-O'Sullivan (foto: Wikimedia Commons)

air-gap), ongezien penetreren. De aanvaller wil het netwerk met al zijn zwaktes beter leren kennen dan de gebruiker. Volgens voormalig directeur NSA (en CIA) Michael Hayden zijn de mogelijkheden tot sabotage (*Cyber Network Attack; CNA*) per definitie inbegrepen in cyberspionage (*Cyber Network Exploitation, CNE*). Als je eenmaal ongezien een netwerk kan beheersen, kan je ook systemen aan- en uitzetten en schade aanrichten. Wil men op termijn de mogelijkheid bezitten om netwerken aan te vallen, dan moeten *implants* in het netwerk worden verstopt die ten tijde van conflict geactiveerd kunnen worden. Dit bleek de NSA te hebben gedaan in Iraanse netwerken onder de naam Operation Nitro Zeus (gelukkig nooit geactiveerd), en dat doen de Russen nu in westerse (inclusief Nederlandse) energienetwerken.[4] Maar inbreken in een netwerk, dat mag DCC niet. Dit is voorbehouden aan de JSCU.

Een aantal landen, waaronder bijvoorbeeld het VK, Canada, Australië en Denemarken, hebben ervoor gekozen al hun cybercapaciteit in de inlichtingensector te concentreren. De argumenten hiervoor komen uit de praktijk. Wederom volgens Hayden: "*in the cyber domain the technical and operational aspects of defence, espionage, and cyberattack are frankly indistinguishable – they are all the same thing*".[5] Het is logisch dat interactie tussen verdedigers en aanvallers beiden partijen kan sterken in hun werk, en het geldt ook voor het opzetten van databases: liever één centrale database dan verschillende versies beheerd door meerdere organisaties. Personeelsbeheer van IT-talent kan zo ook effectiever: de meest getalenteerde hackers (de zogenaamde *wiz kids*) willen niet monitoren en verdedigen, maar juist aan het werk diep in andermans netwerk. Als ze al bij de overheid werken (ze kunnen een veelvoud van een ambtelijk salaris verdienen in de privésector), dan is dat bij een eenheid waar het werk spannend is. Hiernaast is cyber een teamsport. Via *human intelligence* (HUMINT) kan bijvoorbeeld malware met een USB-stick in een netwerk worden gebracht, terwijl *signals intelligence* (SIGINT) nuttig is voor attributie. Daarom hebben landen zoals Denemarken bewust gekozen om ook de verdediging — hun National Cyber Security Center — in te bedden in de inlichtingengemeenschap. Er zijn natuurlijk ook nadelen. Zo moeten er oplossingen worden gevonden voor problemen zoals de omgang met geheimhoudingsvraagstukken en operaties die wellicht niet in de inlichtingenwereld thuis horen (bijvoorbeeld het bestrijden van cybercriminaliteit).

Governance-vraagstukken

Voor het inrichten van nationale *cyber security*-organisaties zijn er grofweg twee keuzes. Ten eerste de vraag of de nationale coördinatie van *cyber security* (en *cyber defense*) in de inlichtingengemeenschap wordt ingebed, of erbuiten.[6] Nederland heeft gekozen voor het tweede, en het Nationaal Cyber Security Centrum (NCSC) valt onder het ministerie van Justitie en Veiligheid. Duitsland en Frankrijk hebben eveneens gekozen voor een constructie buiten de inlichtingengemeenschap. Een tweede keus betreft het samenbrengen van alle capaciteit in één centrum of organisatie, of het meer gedistribueerd inrichten. Nederland heeft een gefragmenteerd cyberlandschap: naast het elders beleggen van *cyber defense*, zijn de JSCU en DCC ook apart. De JSCU combineert kroonjuwelen van zowel de MIVD als de AIVD, waarbij de eerste decennia van SIGINT-expertise bijdraagt, en de tweede een kleine groep bijzonder getalenteerde hackers. Weinig wapenfeiten zijn tot nu toe uitgelekt; wel dat deze eenheid succesvol de Russische groep APT 29 (Fancy Bear) heeft kunnen hacken, en dat zij letterlijk konden meekijken hoe de Russen westerse doelwitten zoals het Amerikaanse State Department aanvielen.[7] Deze eenheid binnen de JSCU heeft inmiddels veel ervaring in het heimelijk inbreken in verharde netwerken, en is aanwezig in belangrijke systemen van potentiele tegenstanders. Zij willen in ieder geval voorkomen dat DCC dwars door hun voorzichtige operaties heen loopt en zonder overleg gaat hacken.

De VS hebben ook *cyber defense* buiten de inlichtingenwereld ingebed. Zo coördineert het Department of Homeland Security (DHS) nationale *cyber security*, al gaat het gros van het miljardenbudget naar de National Security Agency (NSA), hun SIGINT/Cyberinlichtingenorganisatie. In 2009 werd U.S. Cyber Command (USCYBERCOM) opgericht, maar vanaf het begin werd erkend dat alle expertise op het gebied van cryptografie, netwerkanalyse en hacken bij de NSA lag. Daarom werd besloten USCYBERCOM en de NSA in hetzelfde gebouw te plaatsen in Fort Meade, onder één (*double hatted*) directeur. Zo kon het personeel van USCYBERCOM leren van de NSA en zouden, wanneer de tijd rijp was, beide organisaties hun eigen weg gaan. Op dit moment debatteert men nog steeds over het splitsen van de twee.[8] Voormalig defensieminister Ash Carter sprak zich uit over de wapenfeiten van USCYBERCOM in de strijd tegen Islamitische Staat (IS) in Irak en Syrië. Hij was teleurgesteld. Over het algemeen hadden cyberoperaties weinig effect op de vluchtige

DCC mag niet inbreken in een netwerk

terreurgroep, en telkens als USCYBERCOM een specifieke cyberaanval voorstelde, wilde de NSA die blokkeren.[9] Op het gebied van *governance* worstelt men nog met de inrichting, maar in de praktijk heeft de NSA dusdanig veel expertise opgebouwd in CNE en CNA (zie bijvoorbeeld ook Stuxnet), dat velen twijfelen of USCYBERCOM ooit volledig onafhankelijk kan zijn. Bijna tien jaar na zijn oprichting zit USCYBERCOM nog steeds vast aan de navelstreng van de NSA.

Cyberpolderen

Doordat de JSCU op afstand is gebleven heeft het Nederlandse DCC weinig zelfstandig op kunnen bouwen. Inmiddels heeft het DCC de hoop op een nieuw concept gezet: *cyber mission teams*. Deze teams zullen bestaan uit operators van zowel het DCC als JSCU, toegespitst op een specifieke missie. Maar ondanks missies in Mali en Irak heeft Defensie het concept nog niet via de artikel 100-procedure uitgeprobeerd. En zelfs al worden *cyber mission teams* ooit ingezet, zal deze weg alleen maar leiden tot een DCC dat beperkt capaciteit kan leveren voor kleine interventies; een soort mini-cyberuitzendbureau. Uiteindelijk ligt dan nog de meeste expertise bij de JSCU. Deze moet ook wel meewerken bij het opzetten van de gemengde teams, anders zou het DCC als alternatief expertise kunnen halen bij reservisten of inkopen bij een bedrijf. Maar zonder een wijziging in het *governance*-model zal het DCC nooit een volwaardige hub van cyber-expertise worden zoals de Britten of Denen hebben ingericht.

Het ligt voor de hand om in ieder geval het DCC te laten intrekken bij de JSCU, waarbij personeel onder de WIV werkt tijdens de inlichtingenfase van een operatie, en onder een 'CDS-mandaat' indien daadwerkelijk CNA-operaties uitgevoerd moeten worden. Aangezien de geplande gezamenlijke huisvesting van de MIVD en AIVD op de Frederikkazerne allerminst zeker lijkt, is een DCC/JSCU toenadering haalbaar. Ook hackers (tijdelijk) onder verschillende wettelijke kaders inzetten is niet zonder precedent: personeel van het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (JISTARC) kan eveneens in bijzondere omstandigheden onder de WIV worden gebracht. Tot nu toe heeft Defensie het *governance*-vraagstuk niet frontaal aangepakt, en is voorzichtig ingezet op een incrementele verbetering in de samenwerking tussen het DCC en de JSCU, met bijvoorbeeld meer detacheringen. *Cyber mission teams* zijn een stap vooruit, maar het blijft Nederlands polderen. In de zeventiende eeuw werd de marine geleid door vijf autonome admiraliteiten, die soms meer met elkaar in de clinch lagen dan met de Engelse of Franse vijand. De huidige cyberdreigingen zijn dermate ernstig dat een grondige herziening van het DCC *governance*-model gerechtvaardigd is.

Sergei Boeke is onderzoeker bij het Institute of Security and Global Affairs (ISGA), Universiteit Leiden, Campus Den Haag.

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

1. 'Bauer over cybercommando: militaire capaciteit die aan belang wint', 5 juli 2018, www.defensie.nl.
2. Paul Ducheine en Kraesten Arnold, 'Besluitvorming bij cyberoperaties', *Militaire Spectator*, 20 februari 2015, www.militairespectator.nl.
3. Rob Jocye, *USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers* - YouTube, 2016, www.youtube.com.
4. Nicole Perlroth en David E. Sanger, 'Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says', *The New York Times*, 15 maart 2018, www.nytimes.com.
5. Michael Sulmeyer, 'Much Ado About Nothing? Cyber Command and the NSA', *War on the Rocks*, 19 juli 2017, https://warontherocks.com.
6. Sergei Boeke, 'National Cyber Crisis Management: Different European Approaches', *Governance* 31, nr. 3 (1 July 2018): 449–64, https://doi.org/10.1111/gove.12309.
7. Huib Modderkolk, 'Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse verkiezingen', *de Volkskrant*, 26 januari 2018, www.volkskrant.nl.
8. Stew Magnuson, 'Roles, Responsibilities of Cyber Command Debated', *National Defense*, 8 februari 2017, www.nationaldefensemagazine.org.
9. Ash Carter, 'A Lasting Defeat: The Campaign to Destroy ISIS' (Belfer Center for Science and International Affairs, Harvard Kennedy School, October 2017), www.belfercenter.org/LastingDefeat.

In de praktijk blijken offensieve cyberoperaties moeilijker uit te voeren dan te beschrijven in doctrines of scenario-oefeningen (foto: Flickr/r. nial bradshaw)