Jaargang 191 nummer 9 - 2022

MILITAIRESPECTATOR

FOG OF WAR 2.0

THEMANUMMER MIVD

- Interview CDS en D-MIVD: 'Zonder inlichtingen geen veiligheid'
- De toekomst van de MIVD
- De militaire inlichtingendienst en zijn afnemers
- MIVD-cyberoperaties: all about access
- Geschiedenis Nederlandse militaire inlichtingen- en veiligheidsdienst(en), 1912-2022

FOTO MCD, SJOERD HILCKMANN

In *Militaire Spectator* 10-2022 verschijnt onder meer: 'Task Force Disaster Relief Bahamas. Zes inzichten voor toekomstige militaire noodhulpoperaties' van dr. J.P. Kalkman.

Nadat de orkaan Dorian in september 2019 een spoor van verwoesting over de Bahama's had getrokken stuurde Nederland hulp naar de eilanden. De Task Force Disaster Relief Bahamas aan boord van de Zr.Ms. Snellius en Zr.Ms. Johan de Witt bestond uit een operationele staf (NLMARFOR), een marinierseenheid, een Genie-eenheid, twee Cougar-helikopters, militairen van 1 CMI Commando en Franse en Duitse eenheden. Tijdens de noodhulpoperatie werden hulpgoederen geleverd, brandstof vervoerd, puin geruimd en een brug en gebouwen hersteld. Over een periode van tien dagen waren zo'n 650 militairen actief betrokken bij de inzet.

Een nadere bestudering van de noodhulpoperatie laat zien dat de Task Force enorm adaptief is geweest. De vooraf opgezette structuur en werkwijze bleken op een aantal punten niet te passen bij de lokale situatie. Plannen bleken namelijk al vrijwel direct niet meer houdbaar, protocollen waren te omslachtig en beveiligde communicatiemiddelen te langzaam. In korte tijd werden dan ook allerlei organisatorische en operationele aanpassingen gedaan om sneller en beter te kunnen optreden. Het is zinvol om te leren van deze ervaringen, zodat er bij toekomstige inzet vooraf rekening gehouden kan worden met de unieke vereisten van noodhulpoperaties. ■

KVBK BATTLEFIELD TOUR ZEELAND

De battlefield tour van de KVBK vindt op 8 oktober plaats in Zeeland. Bespreekpunten zijn in Westkapelle, Koudekerke, Vlissingen, het Liberation Museum en bij de Sloedam. Na afloop is het diner optioneel. KVBK-leden betalen 20 euro, niet-leden 30 euro.

Voor meer informatie en aanmelden zie www.kvbk.nl of scan de QR-code.

Turen in de mist

Afgevuurde wapens, inslagen en rookwolken, rumoer en chaos, met als gevolg het verlies van contact en een gebrek aan overzicht. Alle planning en voorbereiding ten spijt, het is de inherente 'frictie' van de *fog of war* die het verloop van de strijd dicteert.[1] Dit geldt ook in onze gedigitaliseerde wereld waar onzekerheid en onduidelijkheid door (digitale) ruis, perceptie en/of misleiding als instrument in de strijd enkel aan belang hebben gewonnen. De mogelijkheden van internet, sociale media en voortgaande technologische ontwikkelingen hebben de samenleving en het slagveld van de 21e eeuw veranderd.

Geheimen maken onderdeel uit van de hierboven geschetste frictie. Enerzijds beogen ze de mist te laten verdwijnen om de strijd in eigen voordeel te kunnen beslechten, anderzijds dragen ze er toe bij de tegenstander op het verkeerde been te zetten. Een paradox, die eveneens geldt voor de werkzaamheden van een organisatie als de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) in onze democratische samenleving, waar privacy (of persoonlijke geheimen) en transparantie hoog in het vaandel staan. Belangrijke verworvenheden die een geheime dienst dient te beschermen, waarbij uit de aard der zaak diezelfde privacy kan worden geschonden, terwijl niet altijd de verlangde mate van openheid kan worden gegeven.[2]

Het gebruik, belang en de noodzaak van inlichtingen ten behoeve van nationale en internationale veiligheid staat sinds het uitbreken van de oorlog in Oekraïne op ieders netvlies, geholpen door de ongekende openbaarmaking van geheime informatie in de maanden voorafgaand aan het neerkomen van de eerste Russische bommen. De inlichtingensluier is daarmee echter niet weggenomen. Zowel de militair op het fysieke en digitale strijdtoneel als de burger aan de zijlijn tuurt nog altijd in de mist. Correcte en betrouwbare informatie lijkt een steeds schaarser goed te worden. Meer dan ooit is (digitale) frictie onderdeel van het strijdtoneel, met als resultaat de *fog of war 2.0*.[3]

Met de voorliggende speciale editie van de *Militaire Spectator* wil de MIVD iets van de mist rondom zijn werkzaamheden wegnemen. Een bijdrage aan transparantie – ondanks alle beperkingen – waarin aspecten van militaire inlichtingen en veiligheid onder de loep worden genomen. Auteurs schrijven over de historische ontwikkeling van de dienst en zijn voorgangers, zijn toekomst, cyber en inlichtingen, en de relatie tussen militaire inlichtingenproducent en -afnemer. Daarnaast praten de CDS en de Directeur-MIVD in een uniek dubbelinterview uitvoerig over de (toekomstige) relatie tussen de dienst en de krijgsmacht. ■

1 'Friktion ist das einzige Begriff (...) was den wirklichen Krieg von dem auf dem Papier unterscheidet', Carl von Clausewitz, *Vom Kriege* (Berlin, 1832).

2 Dennis Broeders, *Het geheim in de informatiesamenleving* (Den Haag/Rotterdam, 2015); Paul Frissen, *Het geheim van de laatste staat. Kritiek van de transparantie* (Amsterdam, 2016).

3 Maarten Katsman, 'Fog of War 2.0. 20 jaar MIVD: Wat nieuwe ontwikkelingen vragen van inlichtingen- en veiligheidsdiensten', *zie: www.militairespectator.nl, 30 juni 2022.*

KVBK
KONINKLIJKE VERENIGING
TER BEOEFENING VAN
DE KRIJGSWETENSCHAP

UITGAVE
Koninklijke Vereniging ter Beoefening van de Krijgswetenschap
www.kvbk.nl
E info@kvbk.nl
facebook.com/KVBKsecretaris
twitter.com/kvbk1

Secretaris en ledenadministratie
Majoor R. Verheijen MA
E secretaris@kvbk.nl
Nederlandse Defensieacademie (NLDA)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
E ledenadministratie@kvbk.nl

De Militaire Spectator is aangesloten bij de European Military Press Association

LIDMAATSCHAP

binnenland	€ 30,00
studenten	€ 22,50
buitenlandtoeslag	€ 5,00

OPMAAK
Coco Bookmedia

DRUK
Wilco Meppel
ISSN 0026-3869

Coverfoto: Amerikaanse mariniers oefenen in een gebouw
Foto: Shutterstock

FOTO HERMAN ZONDERLAND

'Zonder inlichtingen geen veiligheid'

Alexander Claver, Peter Pijpers en Frans van Nijnatten

In een interview met de *Militaire Spectator* reflecteren Commandant der Strijdkrachten generaal Onno Eichelsheim en D-MIVD generaal-majoor Jan Swillens op het inlichtingenveld, het dreigingslandschap en een sterkere J2-constructie bij de krijgsmacht.

Voorbij de heilige huisjes

Saskia Pothoven

Aan de hand van drie heilige huisjes kan onderzocht worden of de gebruikelijke denkwijze over de inlichtingenproducent-klantrelatie ook standhoudt binnen het militaire inlichtingendomein.

476

MILITAIRESPECTATOR

JAARGANG 191 NUMMER 9 – 2022

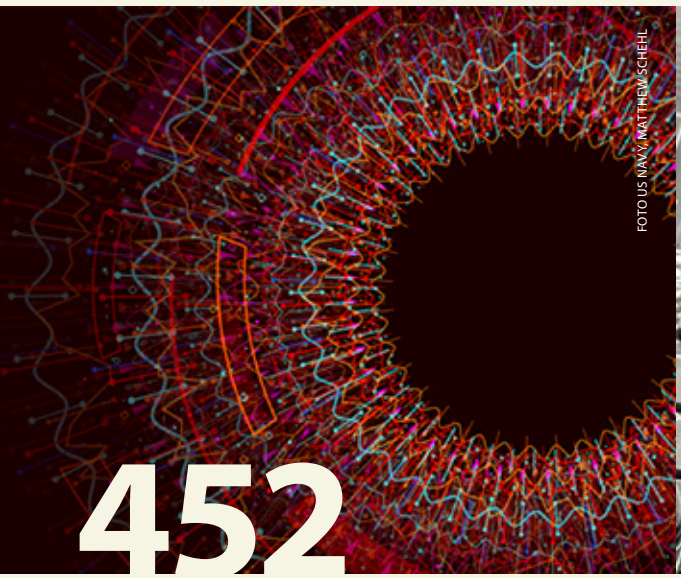


FOTO US NAVY, MATTHEW SCHEHL

FOTO MILITAIRE SPECTATOR

‘Zonder inlichtingen geen veiligheid’

Interview met CDS Onno Eichelsheim en D-MIVD Jan Swillens

De Militaire Inlichtingen en Veiligheidsdienst (MIVD) bestaat twintig jaar in zijn huidige constellatie. In een recent door de dienst georganiseerd seminar kwam naar voren dat de omgeving waarin de dienst opereert niet stil heeft gestaan.[1] Waar in het verleden bij wijze van spreken ‘mannen met gleufhoeden en opengeknipte kranten’ hun werk deden, heeft de opkomst van internet en cyberspace de manieren en mogelijkheden van opereren danig veranderd. In een interview met de *Militaire Spectator* reflecteren Commandant der Strijdkrachten generaal Onno Eichelsheim (tevens voormalig hoofd-MIVD) en de huidige directeur van de dienst, generaal-majoor Jan Swillens, op het inlichtingenveld, het dreigingslandschap en een sterkere J2-constructie bij de krijgsmacht die ook de MIVD beter moet laten aansluiten bij de behoeftes op het operationeel-tactische niveau.

Alexander Claver, Peter Pijpers en Frans van Nijnatten

MS: De militaire confrontatie in Oekraïne lijkt een reflectie van het veranderende karakter van oorlogvoering: een hybride conflict waarin informatie en *intelligence* een zeer prominente rol spelen, niet alleen om inzicht te krijgen waar de vijand is en hoe het slagveld eruit ziet, maar ook om in te zetten als wapen, zoals uit de narratieven op Russische media als RT en Sputnik blijkt. Wat is onze appreciatie van het veranderende karakter van oorlogvoering, of hebben we het hier over oude wijn in nieuwe zakken?

Generaal Eichelsheim: Het klopt dat het conflict in Oekraïne, zowel in de aanloop als in de uitvoering, 25 jaar geleden anders gevoerd zou zijn. Rusland zet weliswaar nog steeds conventionele middelen in, maar het is tevens

1 Maarten Katsman, ‘Fog of War 2.0 — 20 jaar MIVD: Wat nieuwe ontwikkelingen vragen van inlichtingen- en veiligheidsdiensten, *zie: www.militairespectator.nl, 30 juni 2022.*

Generaal Onno Eichelsheim
Generaal Onno Eichelsheim is sinds 15 april 2021 Commandant der Strijdkrachten. Eerder vervulde hij de functie van directeur van de Militaire Inlichtingen- en Veiligheidsdienst en vervolgens van Plaatsvervangend Commandant der Strijdkrachten (P-CDS). In de functie van P-CDS was hij ook lid van de Cyber Security Raad, het onafhankelijke en strategische adviesorgaan van het kabinet als het gaat om cybersecurity in Nederland. Eichelsheim is sinds 1986 werkzaam voor het ministerie van Defensie.

Generaal-majoor Jan Swillens
Generaal-majoor Jan Swillens is sinds juni 2019 directeur van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De MIVD richt zich op het verzamelen en analyseren van inlichtingen om de krijgsmacht en Nederland veilig te houden. De taken van de MIVD zijn vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wet veiligheidsonderzoeken (Wvo). Swillens is sinds 1985 werkzaam bij het ministerie van Defensie en vervulde eerder de functie van commandant van het Korps Commandotroepen.

FOTO HERMAN ZONDERLAND

CDS Onno Eichelsheim (rechts) en D-MIVD Jan Swillens

een proces om met retoriek de geesten in eigen land rijp te maken voor het voeren van de strijd. Een proces dat meer dan een jaar geleden startte. Voor mij is het een toonbeeld van de rol die informatie en de informatieoorlog in de aanloop speelden en hoe een hybride oorlog uiteindelijk gevoerd wordt.

Ook het Westen heeft voor het uitbreken van de oorlog intelligence-capaciteiten aangewend om daarmee informatie vrij te geven, die de desinformatie van Russische kant teniet moest doen en duidelijk maakte waartoe Rusland in staat was en welke plannen het had. Ondertussen vertellen de Russen dat de strijd om heel goede redenen gevoerd wordt en dat de middelen die zij daarvoor inzetten geoorloofd zijn. Dat is in zekere zin inderdaad oude wijn: het oude manoeuvreren op informatiegebied is hetzelfde, alleen zijn er nu veel meer kanalen ter beschikking.

Het is in de huidige fase voor de Oekraïense president Zelensky belangrijk dat hij zijn boodschap via sociale media en andere communicatiemiddelen, nationaal en internationaal, kan blijven pluggen. Communicatie en informatie spelen een heel belangrijke rol bij het verkrijgen van internationale steun.

Cyberactiviteiten spelen uiteraard ook een rol in deze hybride context, maar tegelijkertijd moeten we constateren dat de Russische acties in de aanloop naar de oorlog niet erg succesvol zijn geweest.

De confrontatie in Oekraïne laat zien hoe een oorlog in de verschillende domeinen wordt gevoerd, zoals in het informatiedomein. Onze kracht ligt onder meer in het aan de voorkant vrijgeven van inlichtingen om de boodschap van de opponent enigszins te ontkrachten. Rusland zal overigens van dit conflict leren dat de geïntegreerde inzet van de verschillende domeinen veel beter zal moeten. Ook de tijdfasering die daarbij hoort zullen ze beter moeten gebruiken.

MS: Heeft het Westen er ook van geleerd? In Afrika en Azië lijkt de Russische boodschap intussen aan te slaan.

Generaal Eichelsheim: Daar valt nog een wereld te winnen. Het Westen redeneert vanaf de *moral highground* en doet niet aan manipulatie. We moeten proberen de desinformatie teniet te doen, maar dat is ingewikkeld als we het, zoals Rusland en China, niet combineren met de inzet van andere instrumenten van macht, zoals het economisch of diplomatiek ondersteunen van bijvoorbeeld een Afrikaans land, zodat zij achter je staan bij je volgende *quest*. Dat fenomeen hebben we wel in de gaten, maar we handelen er nog onvoldoende naar. Dat kan ons op termijn schaden. Westerse landen moeten daarom ook al hun middelen inzetten – niet als overheerser of 'kolonist' en op een andere manier dan de autocratieën – om bepaalde boodschappen te counteren; anders gaan we op een gegeven moment de strijd verliezen.

MS: Er zijn door de 21e-eeuwse informatierevolutie (internet, social media, *low-cost accessibility* van data in bulk) andere soorten middelen beschikbaar. Er komen dreigingen in cyberspace op ons af. Is het werk en de wijze van opereren van de MIVD daardoor de laatste tijd veranderd?

Generaal-majoor Swillens: De MIVD is altijd een *allsource*-dienst geweest: er zijn veel verschillende manieren om informatie binnen te halen en het is een grote kracht om dat onder één dak te hebben. We hebben bijvoorbeeld nog steeds *high frequency*-interceptie, een belangrijk *old school*-middel. Anderzijds zijn er de afgelopen jaren elementen bijgekomen die een enorme aanjager voor de ontwikkeling van de MIVD vormen, zoals cyber, kabelinterceptie, open source intelligence (OSINT) en internationale samenwerking. Wat betreft het laatste aspect: digitale dreigingen zijn grenzeloos en dusdanig dat geen enkel land die zelfstandig kan beantwoorden. Vaak spreekt men over QPQ, maar mijn ervaring is dat echte internationale samenwerking, bijvoorbeeld waar het digitale dreiging betreft, gebaseerd is op vertrouwen.

Het inzetten op kwaliteit is van belang, immers er zijn met de opkomst van het digitale domein dreigingen bijgekomen die inhaken op de kwetsbaarheden van de Nederlandse kennis- en

digitale infrastructuur. Gezien het hoge tempo van de ontwikkelingen is snel kunnen handelen meer dan ooit van belang.

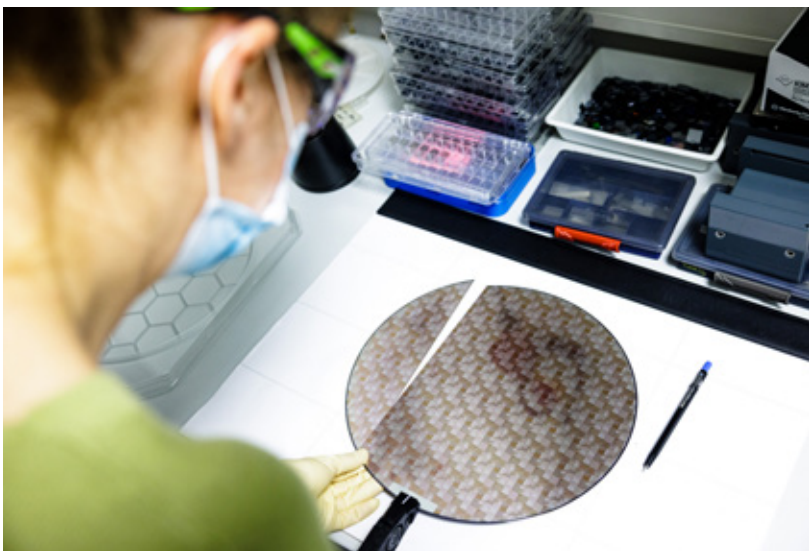
In de *grey zone* tussen oorlog en vrede kunnen aanvallers opereren onder de drempel van fysiek gewapend conflict, terwijl de effecten een ander land wel pijn kunnen doen. Het digitale domein onderstreept het belang dat de MIVD een inlichtingen- *en* veiligheidsdienst is: zonder inlichtingen geen veiligheid.

Generaal Eichelsheim: De samenwerking tussen het Defensie Cyber Commando (DCC) en de MIVD zou beter kunnen. Daar is zeker nog meer synergie te vinden, vooral om snel en effectief op te kunnen treden in het cyberdomein, waar geen onderscheid bestaat tussen strategisch, operationeel en tactisch niveau. Offensief optreden in cyberspace zal hand in hand moeten gaan met de focus die de MIVD weet te leggen. Maar de inzet van de cybercapaciteit is wel aan de CDS.

Generaal-majoor Swillens: In de digitale wereld hebben DCC en MIVD elk een rol, taken en verantwoordelijkheden. Daarbij horen ook juridische kaders en de vraag wat we willen bereiken. Zo moet het DCC in opdracht van de CDS militaire cybereffecten creëren en formuleert het tevens de effecten die we aan eigen zijde willen voorkomen. Dat is een andere benadering dan het kijken naar cyber vanuit een inlichtingen- en veiligheidsperspectief.

Generaal Eichelsheim: We zijn het als Nederland niet gewend, maar we zijn in een *24/7* strategische competitie terecht gekomen die voornamelijk onder het niveau van gewapend conflict plaatsvindt. Ook in het cyberdomein is de vraag hoe we daar actie op ondernemen en welke effecten we willen bereiken. We willen per definitie niet altijd een militair effect bereiken en moeten kijken wiens verantwoordelijkheid het is om iets met de effecten te doen. De indeling, dat het DCC er alleen voor oorlog en gewapend conflict is, past niet meer: we kijken nu hoe we de competitie beter in kunnen gaan, zodat we de 'wedstrijd' ook desgewenst kunnen winnen.

FOTO EUROPESE UNIE



Op het gebied van chiptechnologie heeft Nederland te maken met landen die met een offensief programma proberen die kennis weg te halen

MS: Economische veiligheid was een aantal jaren geleden geen aandachtsgebied voor Defensie, nu duidelijk wel. Is dat een voorbeeld van die veranderende dreiging, met kernwoorden als China en kennispositie?

Generaal-majoor Swillens: Zeker! Economische veiligheid is direct gelinkt aan de nationale veiligheid, denk daarbij aan het gebruik van microchips die in wapensystemen zitten waardoor zij sneller en beter functioneren dan die van de tegenstander. Chiptechnologie is natuurlijk het meest in het oog springend, daar heeft Nederland een toppositie met bedrijven en kennisinstituten. Die moeten we goed beschermen, want we hebben te maken met landen die een offensief programma hebben om die kennis weg te halen; door te hacken, maar ook door mensen die kennis hebben te 'kopen'. De MIVD kan ook voor andere technologieën vanuit de overheid vragen krijgen over exportcontrole, bijvoorbeeld hoe groot de kans is dat Nederlandse technologie in een ander land in de defensie-industrie terecht kan komen.

MS: In Nederland kennen we naast de dienst(en) ook andere entiteiten die actief zijn in het beschermen tegen beïnvloeding via de informatieomgeving, zoals de AIVD, NCTV,

‘Real-time antwoorden kan niet, maar we moeten de antwoorden wel steeds sneller genereren’

NCSC, of het DCC. Op welke wijze is er samenwerking met deze entiteiten, en is er een soort rolverdeling afgesproken?

Generaal-majoor Swillens: Het uitgangspunt is de driehoek belangen-dreigingen-weerbaarheid. Het begint met de regering die definieert wat we willen beschermen. Vervolgens maken de MIVD en AIVD de dreigingsappreciaties en -analyses. De NCTV moet de antwoorden op die dreigingsappreciaties coördineren en de weerbaarheidsmaatregelen formuleren. Dat we elkaar daarbij goed kunnen vinden blijkt bijvoorbeeld uit het rapport *Dreigingsbeeld statelijke actoren*,[2] een coproductie van de diensten en de NCTV.

MS: Zou de NCTV de bevoegdheden van AIVD of MIVD moeten krijgen?

Generaal-majoor Swillens: De NCTV is vooral de centrale coördinator van handelingsopties tussen bepaalde departementen. Ik denk dat de samenwerking nu goed en overzichtelijk geregeld is. Van groot belang is dat de juiste informatie tijdig met de juiste analyse op de juiste plek terecht komt. Deze informatiedeling hebben we in Nederland goed geregeld.

Inlichtingen en Veiligheid is allang niet meer het solitaire terrein van BZK, J&V, BZ en Defensie. Ook bijvoorbeeld EZK, OCW en I&W zijn steeds meer betrokken.

Generaal Eichelsheim: De fenomeenanalyses van de NCTV[3] roepen soms wel de vraag op of de NCTV niet toch een inlichtingendienst is. Het idee achter een fenomeenanalyse is het duiden van trends in de samenleving die een impact hebben op de nationale veiligheid. De NCTV maakt deze duiding op basis van analyses van de AIVD of de MIVD. Indien de NCTV zelf inlichtingenvergaring en -verwerking doet zou het inderdaad een derde dienst zijn wat, gegeven het huidige juridische bestel, onwenselijk is.

MS: In het inlichtingenveld wordt steeds meer verwacht dat je *real-time* antwoorden geeft. Kunnen we dat? Zijn de afnemers van de inlichtingen zich daar van bewust?

Generaal Eichelsheim: Als voormalig directeur van de MIVD weet ik hoeveel tijd het kost om een goede analyse te maken. Het is belangrijk om data snel te verwerken en te analyseren. Real-time antwoorden kan niet, maar we kunnen en moeten de antwoorden wel steeds sneller genereren.

Generaal-majoor Swillens: Een inlichtingen- en veiligheidsdienst moet nooit speculeren, maar ook geen voorspellingen doen. We schetsen of een scenario meer of minder waarschijnlijk is en dat vergt zorgvuldige analyses en regelmatige bijstelling. Tegelijkertijd is de behoefte aan snelle duiding in de informatiemaatschappij waarin we leven gigantisch. Bij de beschieting van het winkelcentrum van Krementsjoek [Oekraïne, 27 juni – red.] wordt verwacht dat de MIVD binnen het uur aangeeft of dat een Russische aanval was, of het ging om het bewust *targeten* van burgers, et cetera. Het risico van een overhaaste duiding is dat indien een attributie later niet blijkt te kloppen dit ten koste gaat van de betrouwbaarheid van de dienst. Als er om politieke of andere redenen toch besloten wordt om snel naar buiten te treden, dan blijft de MIVD glashelder over zijn (informatie)positie en de mate van waarschijnlijkheid van zijn duiding

2 AIVD, MIVD, NCTV, ‘Dreigingsbeeld Statelijke Actoren’, 2021. Zie: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren.

3 Zie bijvoorbeeld: Fenomeenanalyse ‘De verschillende gezichten van de coronaprotesten’: https://www.nctv.nl/documenten/publicaties/2021/04/14/fenomeenanalyse-de-verschillende-gezichten-van-de-coronaprotesten.

en/of oordeel. In de praktijk is de dienst vanwege de goede beeldopbouw tegenwoordig ook bij het overleg over handelingsopties betrokken.

Generaal Eichelsheim: Het scenariowerk dat de dienst doet maakt duidelijk op welke indicatoren kan worden ingegrepen en op welke niet. Die inschattingen zijn nuttig bij het bekijken van de handelingsopties.

MS: Om beter te kunnen voorzien in de behoefte aan operationele en tactische inlichtingen van de krijgsmacht worden sinds kort operationele eenheden deels en tijdelijk onder de MIVD geplaatst. Daarnaast zal ten behoeve van de CDS de J2-cel worden versterkt en uitgebreid om meer sturing te geven aan de operationele en tactische inlichtingenvraag vanuit de krijgsmachtdelen. Hoe kijkt u daar precies naar?

Generaal Eichelsheim: Zoals het nu geregeld is kan de krijgsmacht zonder expliciet mandaat geen inlichtingen vergaren. Echter, op het moment dat de krijgsmacht is ingezet of zich voorbereidt op een specifieke inzet dan mag er meer, mits hier een duidelijk mandaat van de VN en/of het NAVO-verdrag, ondersteund door een Artikel 100-brief, aan ten grondslag ligt. Het is dan verstandig om de voorbereiding onder de Wiv uit te voeren met opdrachten die ik in samenspraak met de D-MIVD verstrek. Op die manier vinden de benodigde activiteiten plaats binnen de wettelijke kaders met het toezicht dat er bij hoort en in het analyseregime van de dienst.

Dat kan binnen de krijgsmacht uitgelegd worden als het aan de leiband lopen van de dienst, maar dat is niet het geval. Ik weet dat er in het verleden veel onderlinge strijd is geweest, mede doordat veel inlichtingencapaciteiten van de defensieonderdelen samengevoegd zijn onder de MIVD, met de gedachte dat die de onderdelen strategisch, operationeel en tactisch zou gaan bedienen. Dat is niet helemaal fair, want de behoeftes zijn veel groter dan de capaciteit van de dienst, terwijl het voor de onderdelen ingewikkeld is om op de juiste manier vragen te stellen; waar moeten ze die kwijt? Tactisch en operationeel gaat het in deze wereld echt zo snel dat daar een andere constructie voor nodig is. De MIVD en de I&V-capaciteiten van de krijgsmacht moeten binnen de wet hun werk kunnen doen. De defensieonderdelen en de CDS moeten regie kunnen voeren over de I&V-capaciteiten en het zou zonde zijn om die capaciteiten niet gericht in te zetten. Daar is de J2-organisatie voor, die aangesloten moet zijn aan de dienst. Dat is het pad dat de CDS en de MIVD moeten vinden, en het voorkomt het ontstaan van een derde inlichtingencapaciteit met eigen analyses.

MS: De J2-cel, eventueel binnen een CDS-huis, eventueel binnen een Permanent Joint Headquarters (PJHQ), die vervult dan die liaisonrol?

Generaal Eichelsheim: Ja, want door de hele lijn bestaat er operationele en tactische I&V-capaciteit en de vraag in de 24/7 strategische competitie is hoe die slim ingezet kan worden. Generaal-majoor Swillens en ik denken met een sterkere J2-constructie de MIVD beter te kunnen laten aansluiten bij de behoeftes op het operationeel-tactische niveau van de krijgsmachtonderdelen in alle domeinen. Daar moet de J2-capaciteit bij het PJHQ, of de Defensiestaf, of waar die ook komt te zitten, invulling aan gaan geven. Het zal de coördinatie en structuur ten goede komen, maar het kan nooit losstaan van de MIVD. Het is nu bijvoorbeeld goed dat de MIVD inlichtingencapaciteit van JISTARC inzet in relatie tot Rusland. Het zou vreemd zijn als dat niet gebeurde; we moeten zulke dingen juist veel meer aan elkaar koppelen. Er zit nog oud zeer bij de opvatting overgeleverd te zijn aan de MIVD die alleen maar strategische inlichtingen verstrekt, maar de dienst verschaft natuurlijk ook operationele inlichtingen. Het hele I&V-netwerk moet veel beter ontsloten worden en de J2 gaat daar een belangrijke rol in spelen.

Generaal-majoor Swillens: Binnen het Informatiegestuurd Optreden (IGO) vormt informatie de kern van inzet. Het begrijpen van de situatie door inlichtingen is belangrijk op elk niveau. Als dat goed geregeld is, kunnen er besluiten worden genomen: dat is de G van IGO, het sturen, de *core business* van de CDS. Vervolgens moet er worden nagedacht over de

effecten die de krijgsmacht wil bereiken en ook dat is een keuze die de CDS binnen de eigen middelen kan maken. Het gevecht in Oekraïne maakt duidelijk dat data een steeds crucialer element wordt. De kwaliteit van informatie, de snelheid waarmee deze kan worden verwerkt en de snelheid waarmee de krijgsmacht dan de juiste effecten kan brengen: dat is IGO, en daarmee is zo'n J2-organisatie alleen maar heel logisch.

Generaal Eichelsheim: Het opbouwen van een informatiepositie kan er bijvoorbeeld toe leiden dat we weten wat het effect zal zijn van de inzet van Zr.Ms. Evertsen [in de Zwarte Zee – red.].[4] Dat ondersteunt het pleidooi voor een PJHQ en een J2-cel die continu met de MIVD interacteert in het hele palet waarin de krijgsmacht wordt ingezet, of dat nu gereedstellingsactiviteiten zijn of inzet op alle domeinen.

Generaal-majoor Swillens: In het geval van Oekraïne is bijvoorbeeld nog niet bekend of en waar Nederland gaat mijnenjagen, maar er moet van tevoren over nagedacht worden en er moet een analyse worden opgesteld voor het geval er een besluit komt. De MIVD wil continu voor op de *power curve* zitten, maar dat wil een militair commandant eigenlijk altijd: nooit verrast worden en het gevoel hebben voorop te lopen. Dat begint uiteraard met een goede inlichtingenpositie en de analyses die daaronder liggen en het op een verstandige manier delen van die informatie met andere *key players*.

MS: Bent u tevreden met de huidige, net aangepaste Wet op de Inlichtingen- en veiligheidsdiensten (Wiv) en de toezichtstructuur op de MIVD?

Generaal-majoor Swillens: Om zijn werk te kunnen doen heeft de MIVD mensen, middelen en een mandaat nodig. De juridische kaders zijn ongelofelijk belangrijk. Het heeft mij en de evaluatiecommissie verrast hoeveel discussie er over de interpretatie van de letter en de geest van wetsteksten gevoerd kan worden. Het lastige aan de discussie is dat het vaak als een soort balans gezien wordt: meer veiligheid betekent minder privacy en vice versa, terwijl dat in mijn beleving helemaal niet aan de orde is. Daarom moeten we het publiek zoveel mogelijk inzicht geven in hoe de MIVD en de AIVD hun werk doen, bijvoorbeeld op het gebied van cyber, om begrip en vertrouwen te creëren. Zo gaat het 'slepen' van hele woonwijken niet gebeuren,[5] omdat er in Nederland andere, veel simpelere middelen zijn om een inlichtingenvraag te beantwoorden. Ook kabelinterceptie vergt een nog betere uitleg aan het publiek: hoe werkt het en waarom is het zo belangrijk? Maar willen we Nederland veilig houden, dan is kabelinterceptie absoluut noodzakelijk, want tegenstanders houden zich aan geen enkele regel en maken gebruik en misbruik van de kabel. Ik vind het een gotspe dat dat nog steeds niet geregeld is.

De frames gekoppeld aan de inbreuk op de privacy en de 'sleepwet' zijn zeer hardnekkig, maar ik zou er wakker van liggen als er iets met de krijgsmacht of met Nederland zou gebeuren en achteraf blijkt dat als de lijntjes aan elkaar waren gebonden, dit bekend had kunnen zijn. Daarom is het goed dat er nu wordt gewerkt aan een tijdelijke wet die ons de mogelijkheid biedt te doen wat nodig is. Landen zoals Rusland en China hebben een offensief cyberprogramma tegen Nederland. Onder de huidige wet kunnen wij niet op alle fronten zien waar de tegenstander is en kunnen we niet op alle fronten snel en flexibel handelen. Dat is een risico voor de nationale veiligheid. Als onze veiligheid niet is gewaarborgd omdat de wet daarvoor in de weg heeft gestaan, dan is het niet goed geregeld. Goed toezicht draagt bij aan het vertrouwen in de diensten, zo blijkt uit een onderzoek van de AIVD.

Dus: *be my guest*, controleer me elk moment. Ik denk dat onze toezichthouders de diensten waarderen met een dikke voldoende, maar dat is niet altijd het beeld dat opgeroepen wordt. Dat moet de MIVD dan ontkrachten door meer naar

4 Zie ook: KTZ Henk Warnar, 'Marinediplomatie: instrument in het Nederlandse evenwichtsbeleid', 9 juli 2021. Zie: https://www.militairespectator.nl/thema/essay/artikel/marinediplomatie-instrument-het-nederlandse-evenwichtsbeleid.

5 'Slepen' staat voor het binnenhalen of aftappen van dataverkeer via een interceptie op bijvoorbeeld een internetkabel.

buiten te treden, uiteraard zonder daarbij onze modus operandi en de bronnenpositie prijs te geven.

MS: Bob de Graaff gaf tijdens het recente MIVD-seminar interessante inzichten in de geschiedenis en transities van de dienst en zijn voorlopers en concludeerde dat die behoorlijk veel tijd nodig hadden om de werkwijze aan te passen.[6] Is dat verandervermogen nu *up to speed*? Of is er misschien een voortdurende transitie, en kunnen we die bijbenen?

Generaal-majoor Swillens: Werken in een context van continue verandering is onze core business. De ontwikkelingen volgen elkaar in hoog tempo op. Voortdurend innoveren en verbeteren is onze realiteit. Stilstand is achteruitgang. Maar je bent er nooit. De grootste uitdaging voor mij als D-MIVD is de schuivende geopolitieke ontwikkeling, toenemende datahoeveelheden, technologie die zich met de snelheid van het licht ontwikkelt en schaarste op de arbeidsmarkt en *compliance* en daarmee onze *performance* op orde brengen. Hoe zorgen we dat we tegelijkertijd de lopende zaken behappen en daarnaast voldoende tijd en energie vrijmaken om de noodzakelijke veranderingen te incorporeren? Ik stel vast dat we in het regeerakkoord financiële middelen hebben gekregen om daar invulling aan te geven.

We leren ook van anderen. Momenteel kijken we bijvoorbeeld goed naar de *lessons learned* van de oorlog in Oekraïne: de *resilience* in de communicatie, de cyberveiligheid, en dat terwijl het land iedere dag maximaal onder vuur ligt. De Oekraïners laten zien dat ze de lessen van 2014 heel goed hebben geleerd. Dat is wat wij nu ook proberen: dezelfde lessen leren zonder dat we dezelfde ervaring hebben.

MS: Hoe gebruikt u beiden uw ervaringen uit uw vorige functies?

Generaal Eichelsheim: Omdat ik directeur van de MIVD ben geweest heb ik een goede kijk op de informatiepositie en de risico's die er in de wereld zijn, dus het is zeker een verrijking. De D-MIVD leert alle domeinen beter kennen, zoals

FOTO TEUN VOETEN

Een Oekraïnse stelling in de buurt van Mykolaiv: 'Het gevecht in Oekraïne maakt duidelijk dat data een steeds crucialer element wordt'

cyber en informatie, en leert hoeveel tijd de dienst soms nodig heeft om informatie op een juiste manier te kunnen duiden. Als CDS weet ik daardoor hoe ik de dienst beter kan gebruiken en dat het goed is de MIVD te betrekken bij planning en besluitvorming. D-MIVD zit bij veel meer fora aan dan vroeger: de inlichtingen zijn immers nodig bij de besluitvormingsprocessen en bij de ontwikkelprocessen van de krijgsmacht. Een praktisch element voor mij als CDS is dat ik als voormalig D-MIVD al goed bekend was in de politieke omgeving en daardoor wist hoe het werkt om een advies te moeten geven.

Generaal-majoor Swillens: Uit mijn vorige functie als commandant van het Korps Commando Troepen heb ik de creatieve *mindset* meegenomen naar de MIVD: durf jezelf continu de vraag te blijven stellen of je de dingen wel goed ziet. Omdat de CDS en ik allebei uitvoerende ervaring binnen de krijgsmacht hebben, weten we hoe belangrijk details kunnen zijn en hoe belangrijk opmerkingen van soldaten en het horizontaal leren zijn. Dat herken ik ten volle uit de SF-wereld: bij evaluaties is het daar nooit een 10, hoogstens een 9,5, want het kan altijd beter. ■

6 Zie ook: Bob de Graaff, *Ongekend en onderscheidend. De geheime geschiedenis van de MIVD* (Amsterdam, Uitgeverij Boom, 2022).

De toekomst van de MIVD

Een complex perspectief

Prof. dr. ir. Bas Rietjens*

Inlichtingen- en veiligheidsdiensten opereren in een complexe omgeving, waarin de ontwikkelingen snel gaan en de fog of war het totale overzicht belemmert. Het is essentieel dat de diensten zich blijven aanpassen, zo ook de MIVD. Complexiteitstheorie is een voor de hand liggend en interessant perspectief om aanpassingen in kaart te brengen. Dit artikel focust op drie organisatie-eigenschappen die hierbij centraal staan: noodzakelijke variëteit, minimale specificaties en lerend vermogen. De analyse identificeert verschillende uitdagingen waar de MIVD mee wordt geconfronteerd. De belangrijkste hiervan zijn de implementatie van het datagedreven werken, het gebruik maken van open bronnen en het inrichten van samenwerkingsrelaties.

Evacuatieoperatie op Hamid Karzai International Airport in Kabul, augustus 2021: verschillende inlichtingendiensten waarschuwden voor de val van de Afghaanse overheid, maar slechts weinige voorzagen het exacte verloop

FOTO US MARINE CORPS, SAMUEL RUIZ

De tragische gebeurtenissen in Afghanistan in de zomer van 2021 en de recente Russische inval in Oekraïne tonen eens te meer aan dat we leven in een onvoorspelbare en complexe wereld. Hoewel verschillende inlichtingendiensten waarschuwden voor de val van de Afghaanse overheid in de maanden daaraan voorafgaand, waren er maar zeer weinigen die de exacte loop van omstandigheden voorzagen. De hoogste Britse officier, generaal Nick Carter, vatte het als volgt samen: 'It was the pace of it that surprised us and I don't think we realised quite what the Taliban were up to. They weren't really fighting for the cities they eventually captured, they were negotiating for them, and I think you'll find a lot of money changed hands as they managed to buy off those who might have fought for them'.[1]

En waar met name Amerikaanse en Britse inlichtingendiensten de Russische inval in Oekraïne erg nauwkeurig voorspelden, zijn velen verrast door de weerstand die de Oekraïense strijdkrachten bieden. Deze voorbeelden laten zien dat het genereren van inlichtingen die accuraat, specifiek en op tijd zijn en ook nog handelingsperspectief bevatten, zeer uitdagend is. Deze uitdaging wordt voor een groot deel bepaald door de complexiteit van de omgeving waarin inlichtingen- en veiligheidsdiensten (I&V-diensten) opereren. In dit artikel ga ik eerst in op deze omgeving en schets ik enkele grote ontwikkelingen die de complexiteit ervan bepalen. Vervolgens wend ik me tot de complexiteitsliteratuur en behandel ik drie karaktereigenschappen die een I&V-dienst in het algemeen, en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) in het bijzonder, nodig heeft om goed te kunnen opereren in zo'n complexe omgeving. Ik besluit dit artikel met een conclusie.

Ontwikkelingen

De ontwikkelingen waarmee I&V-diensten zoals de MIVD worden geconfronteerd zijn talrijk. Hieronder schets ik de belangrijkste: het veranderende karakter van oorlog en conflict, privatisering, globalisering en technologie en informatierevolutie.

Het veranderende karakter van oorlog en conflict

I&V-diensten worden geconfronteerd met een breed palet aan dreigingen. Waar deze dreigingen tijdens de Koude Oorlog nog redelijk overzichtelijk en inzichtelijk waren, is dit nu allang niet meer het geval. Er worden veel verschillende termen gebruikt om de huidige conflicten en dreigingen te benoemen. Denk aan asymmetrische oorlogvoering, hybride oorlogvoering, *grey-zone warfare* of *non-linear warfare*.

* Bas Rietjens is hoogleraar Intelligence & Security aan de Nederlandse Defensie Academie.

1 Jessica Elgot, ''Everybody got it wrong'' on Taliban strategy, says UK defence chief', *The Guardian*, 5 september 2021.

En dan is er natuurlijk ook nog het huidige conflict in Oekraïne dat veel gelijkenissen vertoont met conventionele oorlogvoering. Maar het zou weer te kort door de bocht zijn dit volledig als zodanig te bestempelen. Wat al deze conflicten gemeen hebben is dat ze worden gekenmerkt door geweld en de dreiging daarvan tussen verschillende combinaties van statelijke en niet-statelijke actoren. Er zijn sterk vervagende scheidslijnen tussen oorlog en georganiseerde criminaliteit, een grootschalige schending van mensenrechten en het inzetten van allerlei niet-traditionele wapens. Of, zoals Mark Galeotti dit in zijn meest recente boek omschreef, de 'weaponization of everything'.[2] Concrete voorbeelden hiervan zijn de vluchtelingen die door president Loekasjenko van Belarus worden opgehaald in Syrië en vervolgens de grens over worden gezet naar Polen. Of Zweedse kinderen die tussen TikTok-filmpjes door worden geattendeerd op de naderende Russische dreiging. Het duiden van deze ontwikkelingen en het beschermen tegen de veelheid aan dreigingen leidt tot een immense uitdaging voor I&V-diensten.

Privatisering

Een tweede ontwikkeling is de toenemende rol van private organisaties in het I&V-domein. Dit zijn allereerst de civiele *contractors*. Deze contractors leveren veel verschillende goederen en diensten, variërend van *cloud services*, beveiliging en personeel dat zogeheten missiekritieke taken uitvoert. Privatisering in het I&V-domein heeft een grote vlucht genomen in landen als Australië, Frankrijk en Groot-Brittannië. Maar nergens in de westerse wereld is het zo'n belangrijk thema als in de Verenigde Staten, waar de inlichtingengemeenschap ongeveer 80 procent van haar totale budget van 80 miljard dollar besteedt aan private contractors. Dit bracht Simon Chesterman tot zijn uitspraak 'We can't spy… if we can't buy'.[3] Naast het afnemen van goederen en diensten door contractors is er de laatste jaren een enorme opmars van non-profit collectieven. Deze collectieven bestaan uit een netwerk van vrijwilligers en maken gebruik van de grote hoeveelheid beschikbare openbare bronnen. Bellingcat is het bekendste voorbeeld.[4] Maar ook een organisatie als Amnesty International heeft met behulp van 28.000 vrijwilligers en door gebruik te maken van publiek toegankelijke satellietbeelden bewijsmateriaal verzameld van oorlogsmisdaden in Soedan.

Globalisering

Een derde ontwikkeling is globalisering. In haar baanbrekende studie omschrijft Mary Kaldor globalisering als de intensivering van globale connectiviteit, zowel op politiek, economisch, militair als cultureel vlak.[5] Door globalisering vervaagt het onderscheid tussen lokaal, nationaal, Europees en mondiaal niveau meer en meer. Dit heeft veel invloed op de veiligheidssituatie. Zo heeft globalisering geleid tot een flinke toename van transnationale criminaliteit, waaronder de handel in verdovende middelen, mensensmokkel en diefstal van technologie. Ook vervaagt de scheidslijn tussen interne en externe veiligheid en zijn geografisch afgebakende landsgrenzen steeds minder relevant voor het categoriseren van dreigingen.
Globalisering heeft er verder toe geleid dat inlichtingen niet langer exclusief toebehoren aan overheidsorganisaties. Meer dan voorheen zijn individuele burgers en private organisaties in staat inlichtingen te genereren en daarmee te concurreren met I&V-diensten. In haar recente boek *Spies, Lies, and Algorithms* schrijft Amy Zegart dit toe aan de toegankelijkheid van satellietdata, de toegenomen connectiviteit en beschikbaarheid van informatie en de beschikbare rekenkracht van computers.[6]

Technologie en informatierevolutie

Het staat buiten kijf dat technologie en technologische ontwikkelingen van cruciaal belang zijn voor inlichtingen- en veiligheidsorganisaties. Biotechnologie, *quantum computing*, radar-

2 M. Galeotti, *The Weaponization of Everything. A Field Guide to the New Way of War* (New Haven, Yale University Press, 2022).
3 S. Chesterman, ''We Can't Spy… If We Can't Buy!'. The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'', *European Journal of International Law*, Vol. 19, No. 5 (2008) 1055-1074.
4 Zie onder andere E. Higgins, *Wij zijn Bellingcat* (Amsterdam, Spectrum, 2021).
5 M. Kaldor, *New and Old Wars. Organized Violence in a Global Era* (Cambridge, Polity Press, 1999) 71.
6 A. Zegart, *Spies, Lies, and Algorithms. The History and Future of American Intelligence* (Princeton, Princeton University Press, 2022).

Tegenstrijdige berichten over het conflict in Oekraïne bemoeilijken het duiden van de grote hoeveelheden data die in omloop zijn

FOTO TEUN VOETEN

technologie en kunstmatige intelligentie zijn slechts een paar voorbeelden. Maar waar militaire organisaties in het verleden leidend waren in de ontwikkeling van nieuwe technologie, is dat allang niet meer het geval. Nu zijn het vooral universiteiten en technologiebedrijven die het voortouw nemen op innovatiegebied.
Veel technologische ontwikkelingen spelen zich af in het informatiedomein. Zo hebben ontwikkelingen op ICT-gebied ervoor gezorgd dat de hoeveelheid data die wordt gegenereerd en gedeeld door onder meer bedrijven, overheidsinstanties, wetenschappelijke onderzoekers en burgers de afgelopen jaren zeer sterk is gestegen. In de literatuur wordt deze dataontwikkeling vaak gekarakteriseerd door de zogeheten V's.[7] In grote lijnen komt het erop neer dat data voorkomt in grote hoeveelheden, zowel gestructureerd als ongestructureerd, in verschillende formats (tekst, video, beeldmateriaal en geluidsopnames), sterk verschilt in betrouwbaarheid, en onder hoge snelheid wordt aangevoerd. Wat betreft de betrouwbaarheid zijn de tegenstrijdige berichten over het conflict in Oekraïne een zeer goed voorbeeld. Data zijn in veel gevallen incompleet, ambigu, tegenstrijdig of gewoonweg onwaar. Dit maakt duiding van deze gegevens erg moeilijk.

De hierboven in vogelvlucht geschetste ontwikkelingen zijn bepalend voor de complexiteit waarmee I&V-diensten in het algemeen, en de MIVD in het bijzonder, worden geconfronteerd. Deze situatie vertoont grote gelijkenissen met

7 Afhankelijk van de bron identificeert men 3, 4 of zelfs 7 V's die de karakteristieken van data weergeven: *Volume* (zoals grote datasets bestaande uit terabytes, petabytes, zetabytes aan data – of zelfs meer); *Variety* (zoals meervoudige dataformats met gestructureerde en ongestructureerde tekst, afbeeldingen, audiofiles, video's, geluidsfragmenten of sensordata); *Veracity* (zoals toenemende complexe datastructuren, inconsistenties en onvolledigheden in de datasets); *Velocity* (zoals veel binnenkomende data zonder homogene structuur); *Variability* (zoals data waarvan de betekenis constant verandert); *Visualization* (zoals het presenteren van de data op een inzichtelijke manier); *Value* (zoals het ontsluiten van kennis van grote hoeveelheden gestructureerde en ongestructureerde data zonder verlies voor de eindgebruikers).

zogeheten *wicked problems*.[8] Dit soort problemen zijn ambigu en *fuzzy* en er is een gebrek aan bestaande kennis en standaarden om de gewenste doelstelling te bereiken. En als er al iets is dat in de buurt komt van een oplossing, dan is dit geen *one-size-fits-all,* maar verschilt deze van situatie tot situatie.
Vanuit de complexiteitsliteratuur is bekend dat er verschillende eigenschappen zijn die organisaties moeten hebben om adequaat om te gaan met deze wicked problems.[9] In het vervolg van dit artikel behandel ik drie van deze eigenschappen – noodzakelijke variëteit, minimale specificaties en lerend vermogen – en zal ik reflecteren op het belang ervan voor de MIVD.[10]

Noodzakelijke variëteit

De eerste eigenschap, noodzakelijke variëteit, is gebaseerd op Ashby's wet van *requisite variety.*[11] Deze wet geeft aan dat, wil een systeem levensvatbaar zijn, zijn interne variëteit moet aansluiten bij de variëteit van de omgeving. Alleen in dat geval zal het systeem in staat zijn de uitdagingen te onderkennen en aan te gaan.[12] Kijkend naar de MIVD geldt dat de dienst in veel en uiteenlopende informatiebehoeften moet voorzien. Deze behoeften variëren van het duiden van cyberdreigingen door hackersgroepen gelieerd aan China of Rusland tot aan activiteiten van terroristische groeperingen zoals IS. Dit betekent dat er kennis en expertise nodig is op sterk uiteenlopende gebieden.
Een organisatie die probeert aan al deze informatiebehoeften te voldoen wordt al snel te complex.[13] Om dit te voorkomen is samenwerking met verschillende stakeholders van cruciaal belang en die zijn bij de MIVD zeer uiteenlopend.[14] Deze stakeholders bevinden zich binnen het Nederlandse ministerie van Defensie[15] en andere departementen,[16] maar daarnaast zijn het ook de inlichtingendiensten van partnerlanden, het bedrijfsleven,[17] de wetenschap en non-profitorganisaties. Het managen van al deze verschillende samenwerkingsrelaties is een grote uitdaging, zeker voor een organisatie die van nature erg gesloten is. En waar de focus vaak ligt op formele samenwerkingsstructuren, blijkt uit onderzoek van Pepijn Tuinier dat onderling vertrouwen en sociale relaties minstens zo belangrijk zijn.[18] Reputatie, het herkennen van professionaliteit en gedeelde eigenschappen verbinden inlichtingenprofessionals. Dit helpt hen om verschillen te overbruggen die ontstaan door nationaliteit, organisatie of zelfs conflicterende belangen.

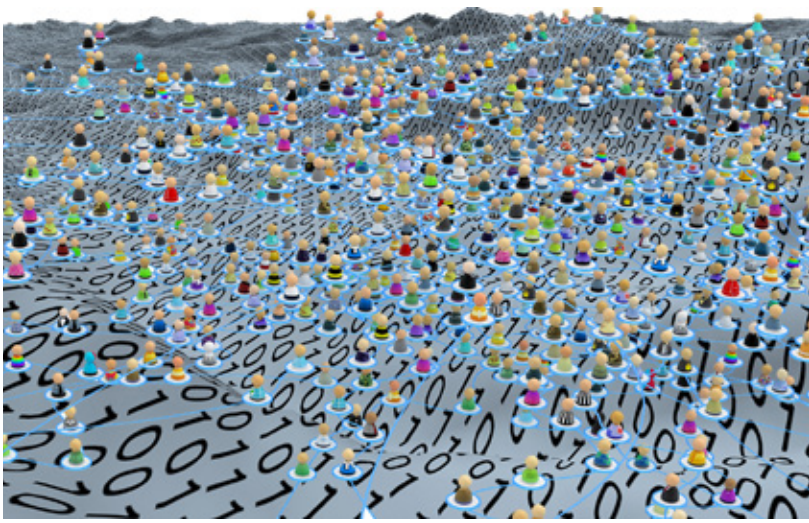
Naast samenwerking is diversiteit een tweede aspect dat van belang is om de noodzakelijke variëteit te bewerkstelligen.[19] De eerste gedachte is dan vaak culturele diversiteit, gebaseerd op ras, huidskleur, religie, gender, seksuele oriëntatie, afkomst, en leeftijd.[20] Daarnaast is cognitieve diversiteit echter ook belangrijk: verschillende perspectieven, verschillende ervaringen en verschillende manieren van denken. In zijn boek *Rebel Ideas* laat Matthew Syed zien dat er voor het beschouwen van complexe problemen verschillende standpunten nodig zijn, om te voorkomen dat een groep of

8 H. Rittel en M. Webber, 'Dilemmas in a General Theory of Planning', *Policy Sciences,* Vol. 4, No. 2 (1973) 155-169.
9 Zie onder meer S. Brown en K. Eisenhardt, 'The art of continuous change. Linking complexity theory and time-paced evolution in relentlessly shifting organizations', *Administrative Science Quarterly*, Vol. 42, No. 1 (1997) 1-34.
10 Deze analyses zijn gebaseerd op beschikbare literatuur en documenten alsook op informele gesprekken met medewerkers van de MIVD. Een conceptversie is voorgelegd aan drie tegenlezers om de validiteit en betrouwbaarheid te versterken.
11 W. Ashby, *An Introduction to Cybernetics* (Londen, Chapman & Hall, 1956).
12 Zie onder meer G. Morgan, *Images of Organization. The Executive Edition* (Thousand Oaks, Sage, 2006).
13 K. Desouza, 'Information and Knowledge Management in Public Sector Networks. The Case of the US Intelligence Community', *International Journal of Public Administration,* Vol. 32, No. 14 (2009) 1219-1267.
14 Zie onder meer H. de Bruijn, *Managing Performance in the Public Sector* (Londen, Routledge, 2007).
15 Onder meer Directoraat-Generaal Beleid (DGB), de operationele commando's, het Special Operations Command (SOCOM) en het Joint ISTAR Commando (JISTARC).
16 Onder meer Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Nationaal Cyber Security Centrum (NCIS), Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de verschillende directies van Buitenlandse Zaken.
17 Onder meer cyber security-bedrijven zoals Fox-IT.
18 P. Tuinier, T. Brocades Zaalberg & S.J.H. Rietjens, 'The Social Ties that Bind: Unraveling the Role of Trust in International Intelligence Cooperation', *International Journal of Intelligence and CounterIntelligence* (2022) DOI: 10.1080/08850607.2022.2079161.
19 Zie onder meer J. Gentry, 'Demographic Diversity in U.S. Intelligence Personnel: Is it Functionally Useful?', *International Journal of Intelligence and CounterIntelligence* (2021).
20 R. Callum, 'The Case for Cultural Diversity in the Intelligence Community', *International Journal of Intelligence and CounterIntelligence*, Vol. 14, No. 1 (2010) 25-48.

organisatie in dezelfde referentiekaders blijft zitten en dezelfde denkfouten maakt.[21] Het klassieke voorbeeld van het belang van diversiteit is dat van de CIA in de aanloop naar *9/11*. Met een personeelbestand van vooral hoogopgeleide blanke mannen sloeg de dienst niet voldoende aan op de diverse signalen die aan de aanslagen voorafgingen.

Bij de MIVD valt allereerst de mix tussen militaire en civiele medewerkers op. De burgermedewerkers van de MIVD zijn in de meerderheid en hebben verschillende achtergronden, referentiekaders en ervaringen. Denk hierbij aan landenspecifieke kennis, beheersing van een bepaalde taal, ervaring op het gebied van hacken of het omgaan met grote datasets. Maar het is de militaire expertise en kennis die de MIVD onderscheidt van andere organisaties en die essentieel is om zijn taakstelling te kunnen vervullen.[22] Het is daarom zorgelijk dat de MIVD steeds slechter in staat is om voldoende militair personeel aan zich te binden.
Ten tweede en hieraan gerelateerd hebben medewerkers van de MIVD allerlei verschillende opleidingen genoten. Kijkend naar het klassieke onderscheid tussen alfa's (geschiedenis, taalkunde), bèta's (natuurkunde, informatica) en gamma's (psychologie, sociologie, economie), dan is vooral personeel met een bèta-achtergrond schaars. Zeker gezien de grote ontwikkelingen in het informatiedomein is het voor de MIVD, net zoals voor veel andere kennisintensieve organisaties, van groot belang bèta's te werven en te behouden. De *summerschool* die de Joint Sigint Cyber Unit jaarlijks organiseert is een mooi voorbeeld hoe de MIVD creatief mensen met een bèta-profiel werft.[23]
Het managen van diversiteit heeft echter meer om het lijf dan een gevarieerd personeelsbestand. Zo heeft de MIVD in 2008 de Devil's Advocate in het leven geroepen.[24] Dit bureau heeft als taak de dominante denkwijze binnen de MIVD ter discussie te stellen en alternatieve perspectieven aan te dragen om het risico op groepsdenken te verminderen.[25] Andere uitdagingen voor de MIVD bij het managen van diversiteit zijn het creëren van een gezamenlijke identiteit, het combineren van verschillende leiderschapsstijlen, een optimaal gebruik van de

FOTO DARPA



De MIVD heeft een mix van militaire en burgermedewerkers die ook vanuit hun opleiding – alfa, bèta en gamma – verschillende perspectieven, ervaringen en manieren van denken meebrengen

uiteenlopende achtergronden en expertisegebieden en verschillende carrière- en trainingsmogelijkheden.[26]

Minimale specificaties

De tweede eigenschap die organisaties in staat stelt goed om te kunnen gaan met complexiteit is die van minimale specificaties. In dit kader moet alleen het hoognodige worden vastgelegd en moeten de mensen die daadwerkelijk het werk uitvoeren genoeg vrijheid krijgen. Dit moet hen in staat stellen meer te experimenteren en bestaande procedures, normen en prestatiecriteria in twijfel te trekken. Karl Weick gebruikt hiervoor de term 'the charm of the

21 M. Syed, *Rebel Ideas. The Power of Diverse Thinking* (Londen, John Murray Publishers, 2020).
22 Zie artikel 10 van de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv) van 2017.
23 Zie: https://jscu.summerschool.sh.
24 A. Claver en H. van de Meeberg, 'Devil's Advocacy within Dutch military intelligence (2008-2020). An effective instrument for quality assurance?', *Intelligence and National Security*, Vol. 36, No. 6 (2021) 849-862.
25 Claver en Van de Meeberg (2021).
26 NATO STO HFM-226 Task Group, *Civilian and Military Personnel Integration and Collaboration in Defence Organisations* (Brussel, NAVO, 2018); I. Goldenberg e.a., 'Integrated defence workforces. challenges and enablers of military–civilian personnel collaboration', *Journal of Military Studies*, Vol. 8 (2019) 28-45.

Statement van een aanwezige bij de bekendmaking van het raadgevend referendum over de Wiv in 2018: het maatschappelijk draagvlak vormt een begrenzing voor het werk van de MIVD

FOTO ANP, REMKO DE WAAL

skeleton'.[27] Hij benadrukt hierbij het vinden van een balans tussen aan de ene kant het strak in de hand houden van een organisatie en aan de andere kant het loslaten van de regelgeving. In het inlichtingendomein leiden deze minimale specificaties tot een paradoxale situatie. Om de complexe inlichtingenvraagstukken te adresseren heeft een I&V-dienst manoeuvreerruimte nodig. Inlichtingenteams worden immers steeds vaker geconfronteerd met zogeheten *unknown unknowns*, ofwel ongekende dreigingen. Een belangrijke strategie bij het onderkennen van deze ongekende dreigingen is het concept van *enactment* of, zoals Dan Isenberg het noemt, 'fighting empirically'.[28] Enactment gaat uit van de symbiotische relatie tussen een organisatie en haar omgeving en stelt dat alleen organisaties die daadwerkelijk actie ondernemen grip kunnen krijgen op hun omgeving en zich kunnen aanpassen. Hierbij moeten de betrokken personen veel energie stoppen in het constant reflecteren op wat ze doen in plaats van de omgeving als een statisch gegeven te zien. Offensieve contra-inlichtingenoperaties, zoals het inbreken in computernetwerken van een concurrerende dienst, zijn een goed voorbeeld hoe I&V-diensten enactment invullen. Deze operaties zijn er in beginsel niet op gericht om vijandelijke inlichtingenoperaties af te stoppen, maar juist om 'zoveel mogelijk informatie over de tegenstander, diens operaties en de ontwikkeling van diens heimelijke activiteiten op te doen'.[29]

Een tweede strategie om ongekende dreigingen te onderkennen is het achterhalen van correlaties in grote hoeveelheden data, zoals bulkdatasets. Dit wordt vaak aangeduid met de term 'datagedreven werken' en is erop gericht om algemene trends en afwijkingen te onderkennen en daarmee de invloed van cognitieve vooroordelen te ondervangen.

De eigenschap 'minimale specificaties' wil niet zeggen dat er helemaal geen beperkingen moeten worden gesteld aan het optreden van een I&V-dienst. Er zijn verschillende mecha-

27 K. Weick, 'Rethinking Organizational Design', in: R. Boland en F. Collopy (red.), *Managing as Designing* (Stanford, Stanford University Press, 2004) 36-53.

28 D. Isenberg, 'Some Hows and Whats of Managerial Thinking', in: J. Hunt en J. Blair (red.), *Leadership of the Future Battlefield* (New York, Pergamon, 1985).

29 B. de Jong en P. Keller, 'Contra-inlichtingen en contraspionage', in: B. de Graaf, E. Muller en J. van Reijn (red.), *Inlichtingen- en Veiligheidsdiensten* (Alphen aan den Rijn, Kluwer, 2010) 280.

nismen die zijn manoeuvreerruimte begrenzen. De Evaluatiecommissie Wiv 2017[30] en de Algemene Rekenkamer[31] hebben de spanning tussen de operationele slagkracht van de I&V-diensten en de implementatie van de Wiv 2017, inclusief het bijbehorende toezichtsregime, helder in kaart gebracht. De grootste spanningen treden op bij de verwerving en verwerking van bulkdata, de geautomatiseerde data-analyse (GDA), de samenwerking met buitenlandse diensten en het stelsel van toezicht. Zo stelt artikel 26 van de Wiv dat de diensten bij het verwerven van bulkdatasets moeten voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Daarnaast is ook het gerichtheidsvereiste van belang. Een dienst moet hierbij 'doen wat redelijkerwijze in haar vermogen ligt om reeds bij verwerving van gegevens de niet voor onderzoek noodzakelijke gegevens tot een minimum te beperken en motiveren dit in hun aanvraag tot de inzet van een bevoegdheid'.[32] De dienst moet hierbij zoveel mogelijk afbakenen naar locatie, tijdstip, soort data, object of naar gedraging. Deze afbakening staat echter op gespannen voet met het onderkennen van ongekende dreigingen.

Naast het juridisch regime worden de activiteiten van de diensten begrensd door de Geïntegreerde Aanwijzing (GA). Dit document, dat in goed overleg tussen de behoeftestellers en de diensten tot stand dient te komen, beschrijft waar een dienst onderzoek naar moet doen, de te bereiken doelen en de prioriteiten. Per thema wordt daarbij aangegeven welke diepgang een onderzoek moet hebben.[33] De GA functioneert relatief goed als het gaat om known unknowns, zaken waarvan je weet dat je ze niet weet. Ook is de GA een goed instrument om middelen aan een dienst toe te wijzen en om hun resultaten te kunnen beoordelen. Maar bij ongekende dreigingen voelt de GA vaak aan als een te strak keurslijf. De GA heeft een looptijd van vier jaar, maar kan jaarlijks worden bijgesteld. Toch lijkt zo'n jaarcyclus te lang om adequaat op nieuwe en onvoorziene bedreigingen van de nationale veiligheid te reageren.[34] Met de toekenning van beperkte discretionaire ruimte aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie om aanvullende onderzoeksopdrachten te verstrekken heeft de wetgever getracht dit te ondervangen. Ook stelt de Wiv 2017 expliciet dat de diensten capaciteit kunnen blijven inzetten om ongekende dreigingen te onderkennen. Maar een I&V-dienst zal in de eerste plaats geneigd zijn om zijn middelen in te zetten op de onderzoeksthema's waarop hij wordt afgerekend. Dit gedrag is goed te verklaren, maar draagt ertoe bij dat ongekende dreigingen minder aandacht krijgen dan ze verdienen.

Een laatste begrenzing is die van het maatschappelijk draagvlak en de daaruit volgende balans tussen transparantie en geheimhouding. Er zijn veel bedrijven en overheidsorganisaties die persoonlijke gegevens van burgers verzamelen en gebruiken. Vaak is het niet helder waarom en waarvoor deze gegevens verzameld worden en in hoeverre dit in het belang van de burger is. Dit leidt tot veel zorgen in de samenleving, met name op het gebied van privacy. Deze gegevens kunnen immers gebruikt worden voor *profiling*, sturing en zelfs manipulatie van burgers.[35] Aangezien de maatschappij, door toedoen van de wetgever, bijzondere bevoegdheden heeft toegekend aan I&V-diensten, is het van groot belang dat zij het maatschappelijk draagvlak behouden en zo transparant mogelijk zijn over hun werkzaamheden. De grootschalige onthullingen over de interceptie-activiteiten van de Amerikaanse National Security Agency (NSA), maar ook de recente berichtgeving rondom de activiteiten van het Land Information Manoeuvre Centre van de landmacht (LIMC)[36] en de analyse-afdeling van de NCTV,[37] hebben een negatief effect op de beeldvorming van de MIVD.

30 Evaluatiecommissie Wiv 2017, *Evaluatie 2020: Wet op de Inlichtingen- en veiligheidsdiensten 2017* (2021).
31 *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt* (Den Haag, Algemene Rekenkamer, 2021).
32 Kamerstukken II 2018/2019, 35 242, nr. 3, p. 5 (MvT wijziging Wiv 2017).
33 P. Abels, *PER UNDAS ADVERSAS? Geheime diensten in de maalstroom van politiek en beleid* (Leiden, Universiteit Leiden, 2018).
34 Abels (2018).
35 Evaluatiecommissie Wiv 2017 (2021) 22.
36 E. Rosenberg en K. Berkhout, 'Militairen zouden dit zelf heel netjes moeten willen regelen', *NRC,* 16 november 2020.
37 A. Kouwenhoven, E. Rosenberg en R. van der Poel, 'Onmin en uitglijders bij de club die het land moet beschermen', *NRC*, 9 april, 2021.

Het dilemma van minimale specificaties vraagt om een zorgvuldige balans tussen taakstelling, manoeuvreerruimte en begrenzingen

Samenvattend vraagt het dilemma van minimale specificaties om een zorgvuldige balans tussen taakstelling, manoeuvreerruimte en begrenzingen. Om zijn taken goed uit te voeren heeft de MIVD manoeuvreerruimte nodig (zoals het hiervoor benoemde concept van enactment), maar wordt de dienst begrensd door met name het juridische regime, de GA en het draagvlak in de maatschappij.

Lerend vermogen

De derde eigenschap richt zich op het lerend vermogen van een organisatie. De organisatieliteratuur onderscheidt verschillende typen van leren: *single loop learning*, dat refereert aan het doen van relatief simpele aanpassingen en het doorvoeren van correcties; *double loop learning*, dit impliceert het reframen en zien van onderwerpen op een nieuwe wijze; en *triple loop learning*, wat inhoudt dat actoren nieuwe processen of methoden ontwikkelen om te komen tot dit soort reframings en zienswijzen.[38]

Op het niveau van single loop learning zijn er duidelijke voorbeelden binnen de MIVD. Op individueel en teamniveau vindt het leren doorlopend plaats. Zo maken medewerkers steeds vaker gebruik van open bronnen en experimenteren data-analisten met beschikbare softwareapplicaties en modellen. Op organisatieniveau zijn er echter weinig formele procedures om ervaringen en geleerde lessen te codificeren. Terwijl sommige medewerkers hun ervaringen en lessen vastleggen (vaak in zelfontwikkelde formats), besteden anderen hier nauwelijks aandacht aan. Dit leidt tot fragmentatie en belemmert een structurele vergelijking en analyse van de geleerde lessen.
Dit probleem wordt aangewakkerd door de beperkte functieduur van vooral militaire werknemers. Veelvuldige functiewisselingen leiden ertoe dat kennis verloren gaat en dat relaties opnieuw moeten worden opgebouwd. Daarnaast geven leidinggevenden vaak de voorkeur aan operationeel inzetbaar personeel boven personeel dat belast is met het vastleggen en codificeren van opgedane kennis. Dit is wellicht begrijpelijk vanuit een operationeel perspectief, maar komt het lerend vermogen van een organisatie niet ten goede. Tot slot speelt psychologische veiligheid een belangrijke rol bij het lerend vermogen. Dit betreft de mate waarin medewerkers kritisch naar zichzelf, hun team en de gehele organisatie kunnen zijn op basis van de verwachting dat collega's en leidinggevenden hier constructief op reageren. Pas als dit het geval is zal een organisatie daadwerkelijk leren.

Op het niveau van double loop learning is er een langzame verandering van de wijze waarop inlichtingenvraagstukken worden benaderd. In de inlichtingenliteratuur zijn er grofweg twee stromingen die dit beschrijven.[39] De eerste stroming is terug te voeren op Jomini en probeert de omgeving systematisch uiteen te rafelen. Het bekende spaghettidiagram dat generaal Stanley McChrystal en zijn staf maakten van de situatie in Afghanistan is hier een goed voorbeeld van.[40] Critici van deze aanpak wijzen er op dat het simpelweg onmogelijk is om alle relevante elementen in een analyse op te nemen.[41] En als ze daar al toe in

38 Zie onder meer A. Romme en A. van Witteloostuijn, 'Circular organizing and triple loop learning', *Journal of Organizational Change Management*, Vol. 12, No. 5 (1999) 439-453.

39 Zie onder meer W. Agrell en G. Treverton, *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy* (Oxford, Oxford University Press, 2015).

40 Zie: https://www.theguardian.com/news/datablog/2010/apr/29/mcchrystal-afghanistan-powerpoint-slide.

41 K. Galster, *The Face of the Foe. Pitfalls and Perspectives of Military Intelligence* (Kingston, Legacy Books Press, 2015).

staat zijn, leidt deze benadering vaak tot een sterke versimpeling van de werkelijkheid, waardoor de oplossing voor het probleem vaak niet voldoet.
De tweede stroming erkent deze problematiek. Zij legt dan ook de nadruk op de complexiteit en de daarmee gepaard gaande onzekerheid en verwarrende omstandigheden. Vaak wordt hier de vergelijking gemaakt met de zogeheten *fog of war*, ofwel de mist van de oorlog. Deze vergelijking wordt toegeschreven aan de Pruisische generaal Carl von Clausewitz, die stelde dat tijdens oorlog 75 procent van de factoren waarop een actie is gebaseerd min of meer in mist gehuld is.[42] Deze stroming stelt dat het hoogst haalbare is om te komen tot een scherp en weloverwogen oordeel dat de waarheid of waarheden benadert.[43]

In de Nederlandse inlichtingengemeenschap zien we nog steeds veel aanhangers van de Jominiaanse benadering. Vaak hebben zij een grote behoefte om een omgeving systematisch uiteen te rafelen door middel van raamwerken zoals PMESII (Politiek, Militair, Economisch, Sociaal, Informatie en Infrastructuur). Ook wordt de uitspraak *speaking truth to power* nog veelvuldig gebruikt. Dit impliceert dat er één waarheid is en dat die waarheid tevens onderkend kan worden. Deze gedachte staat vanzelfsprekend op gespannen voet met het complexiteitsdenken. Toch is er langzaam maar zeker een verschuiving richting de Clausewitziaanse benadering. Veel betrokkenen beseffen dat het simpelweg niet mogelijk is de mist volledig te laten optrekken. Het omgaan met complexiteit en onzekerheid wordt daarmee steeds meer geaccepteerd. Dit werd benadrukt tijdens het recente seminar bij het 20-jarig bestaan van de MIVD.[44] Tijdens dit seminar met de veelzeggende titel Fog of War 2.0 benoemden nagenoeg alle sprekers de verwarrende omstandigheden en de onmogelijkheid om volledig zicht te krijgen op de omgeving.

Nu het besef van deze paradigmaverandering langzaam maar zeker indaalt is het voor de MIVD van belang nieuwe processen of methoden te ontwikkelen om hier invulling aan te geven. Dit is het derde niveau van triple loop learning.

Een van de grote uitdagingen hierbij is het gebruik maken van open bronnen. Als het belang van open bronnen nog niet duidelijk was, dan heeft het conflict in Oekraïne hier wel voor gezorgd. De voorbeelden zijn legio: van het bedrijf Maxar Technologies dat satellietdata verspreidt tot aan de Liveuamap, die nagenoeg live verslag doet van de ontwikkelingen op het slagveld en deze weergeeft op een kaart.[45] Open bronnen hebben meerdere voordelen, waaronder: het kunnen schetsen van een bredere context van reeds vergaarde inlichtingen; ze zijn veelal goedkoper dan andere inlichtingenmiddelen; ze kunnen worden gebruikt om inlichtingenproducten van diensten mee te vergelijken; ze zijn gemakkelijk op te schalen; ze zijn eenvoudig te verspreiden onder afnemers.[46] John Gannon, voormalig plaatsvervangend directeur van de CIA, zag open source in 2001 al als ‘‘frosting on the cake’ of intelligence material dominated by signals, imagery, and human-source collection. Today, open source… comprises a large part of the cake itself’.[47]

Ondanks het geweldige potentieel van open bronnen en het subsidiariteitsbeginsel dat bepaalt dat I&V-diensten het lichtste middel in moeten zetten waarmee een doel bereikt kan worden, lijkt open source intelligence (OSINT) nog onvoldoende te worden benut. Dit geldt in zijn algemeenheid voor I&V-diensten, maar zeker ook voor de MIVD. De oorzaak is deels te vinden in de cultuur van I&V-diensten, waarin bijzondere inlichtingenmiddelen vaak hoger in aanzien staan dan open bronnen. Tevens is er de zorg dat intensivering van OSINT kan leiden tot een afname van het exclusieve karakter van I&V-diensten ten opzichte van denktanks, onderzoeksinstituten en collectieven zoals

42 C. von Clausewitz, *Vom Kriege* (1832). Translated by M. Howard en P. Paret, *On War* (New Jersey, Princeton University Press, 1984).
43 Galster, *The Face of the Foe.*
44 Seminar *The Fog of War 2.0* (Den Haag, 23 juni 2022). Zie: https://www.youtube.com/watch?v=_C0jgTqQQjw.
45 Zie: https://liveuamap.com.
46 Zie onder meer S. Gibson, ‘Open Source Intelligence’, R. Dover, M. Goodman en C. Hillebrand (red.). *Routledge Companion to Intelligence Studies* (Londen, Routledge, 2014) 123-131.
47 John Gannon, ‘The Strategic Use of Open-Source Information’, *Studies in Intelligence*, Vol. 45, No. 3 (2001) 67.

Bellingcat. En aangezien open bronnen niet afgeschermd of heimelijk vergaard zijn, is het vaak onduidelijk wat nu precies informatie is en wanneer het om inlichtingen gaat. Hierdoor kan het begrip inlichtingen zijn waarde gaan verliezen of zoals Wilhelm Agrell het twee decennia geleden al verwoordde: 'When everything is intelligence, nothing is intelligence'.[48] I&V-diensten zullen hun visie op en inbedding van OSINT daarom snel moeten gaan herijken.

Een tweede uitdaging bij de ontwikkeling van nieuwe processen en methoden is de implementatie van het datagedreven werken. Waar veel inlichtingenteams met name gebruik maken van traditionele en kwalitatieve analyses worden zij nu geconfronteerd met de grote ontwikkelingen in het technologie- en informatiedomein (zie paragraaf 2). Zo hebben I&V-diensten in potentie de beschikking over een exponentieel groeiende hoeveelheid (open source) data, snel toenemende rekenkracht van computers en de beschikbaarheid van modellen voor data-analyse. Dit maakt de implementatie van datagedreven werken van essentieel belang. De MIVD ondervindt hierbij echter grote uitdagingen. Veel betrokkenen wijzen direct op het geringe aantal medewerkers met een bèta-profiel. Hoewel dit zeker het geval is, zijn er veel andere uitdagingen, zoals de beschikbare infrastructuur (onder meer hardware, software en applicaties), het data-analfabetisme van veel analisten en een groot deel van het management, de integratie tussen kwalitatieve en kwantitatieve analyses, en niet in de laatste plaats de informatiehuishouding.

FOTO US MARINE CORPS, NICHOLAS GUEVARA

Conclusie

'Het is niet de sterkste soort die overleeft, noch de meest intelligente. Het is degene die zich het beste kan aanpassen.' Hoewel niet letterlijk te herleiden, wordt deze opmerking vaak toegeschreven aan Charles Darwin, de grondlegger van de evolutietheorie. Ook voor I&V-diensten is het essentieel dat zij zich blijven aanpassen. Zij worden immers geconfronteerd met verschillende grote ontwikkelingen, zoals het veranderende karakter van oorlog en conflict, privatisering, globalisering en technologie. Gezien de complexiteit van deze ontwikkelingen, is complexiteitstheorie een voor de hand liggend en interessant perspectief om deze aanpassingen in kaart te brengen. Dit perspectief is vormgegeven door te focussen op drie organisatie-eigenschappen. Noodzakelijke variëteit, de eerste eigenschap, benadrukt het belang van zowel cognitieve als culturele diversiteit en samen-

48 Zie: https://www.hsdl.org/?view&did=442465.

49 P. Drucker, *Management. Task, Responsibilities, Practices* (New York, Harper & Row, 1973).

De rookmachine heeft niet langer alleen een letterlijk effect: de inlichtingengemeenschap verschuift langzaam naar de Clausewitziaanse benadering dat de huidige omstandigheden zo complex zijn dat de fog of war nooit helemaal kan optrekken

werking met een breed palet aan actoren. De tweede eigenschap, minimale specificaties, vraagt om een zorgvuldige balans tussen taakstelling, begrenzingen die voortkomen uit regels en principes en manoeuvreerruimte en operationele slagkracht die een I&V-dienst nodig heeft om effectief te zijn.
De derde en laatste eigenschap is het lerend vermogen. Hier kan een onderscheid gemaakt worden tussen het doen van relatief simpele aanpassingen (single loop learning), het reframen en zien van onderwerpen op een nieuwe wijze (double loop learning) en het ontwikkelen van nieuwe processen of methoden (triple loop learning). Het omarmen van complexiteit, het beter benutten van open bronnen en het datagedreven werken zijn aandachtspunten die hier naar voren komen.

Het was managementgoeroe Peter Drucker die stelde: 'Het enige dat we over de toekomst weten, is dat het anders zal zijn'.[49] Dit wetende kunnen I&V-diensten zich maar beter zo goed mogelijk voorbereiden op deze onzekerheid. ■

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]

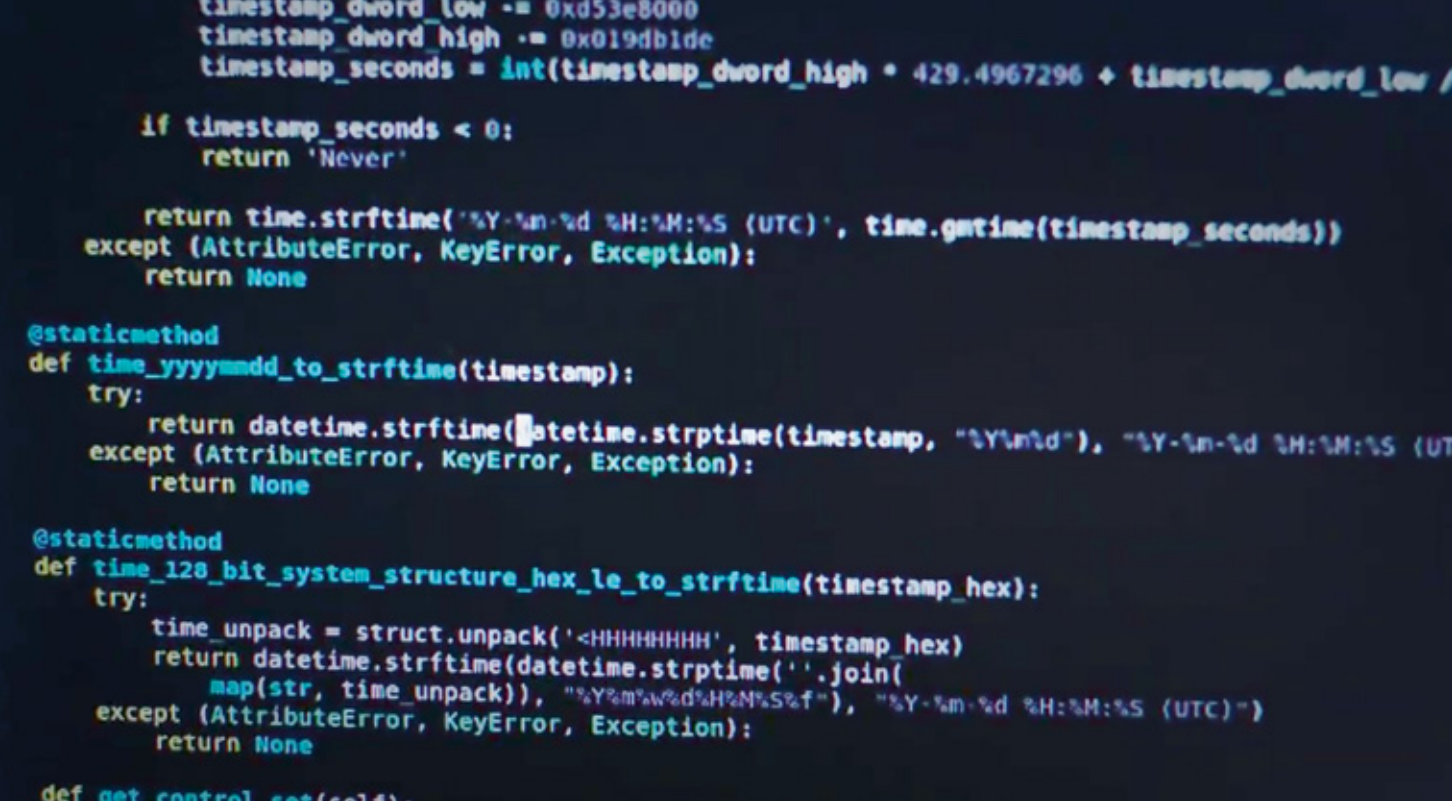
'Also never give them any excuse to hack you. Just don't f-ck with the Dutch in general.'[2]

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-.

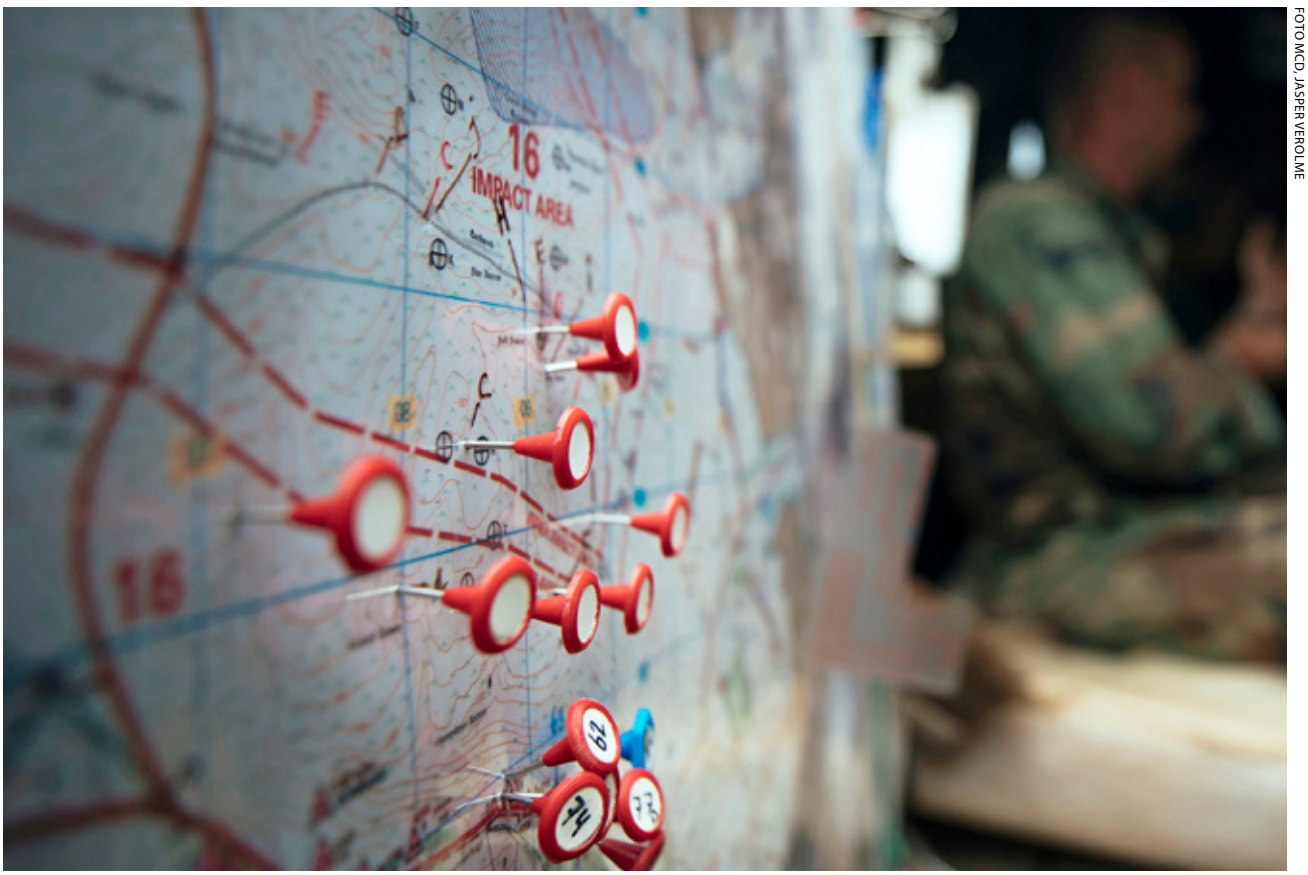


FOTO MCD, JASPER VEROLME

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.

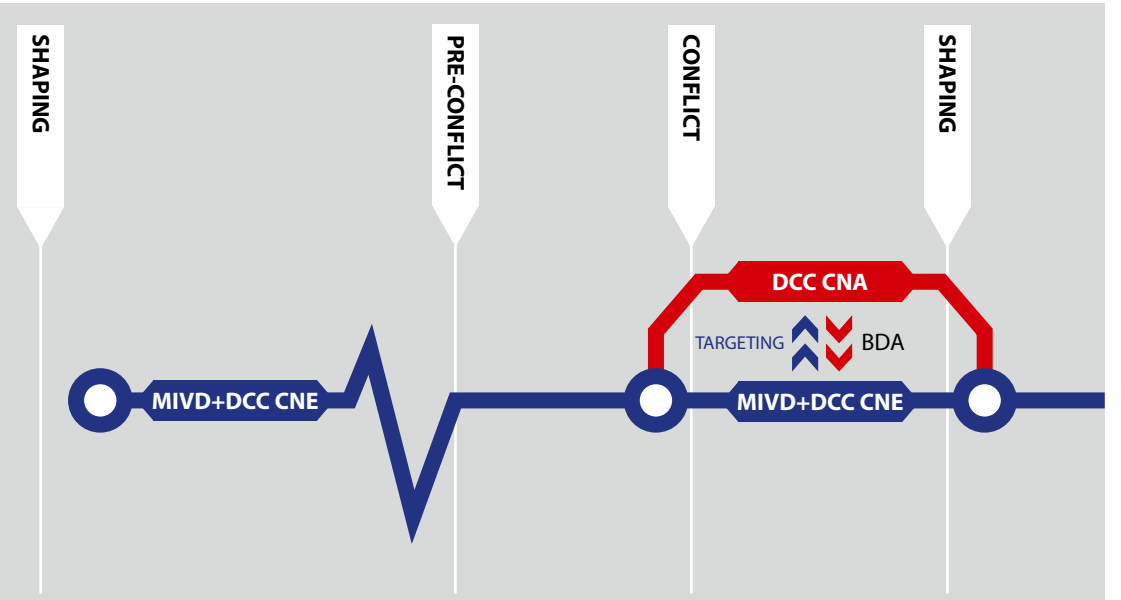
4. Versterking offensieve digitale slagkracht
Ten vierde leidt de intensivering van de samenwerking tussen het DCC en de MIVD tot een toename van de beschikbare cybercapaciteit binnen zowel het DCC als de MIVD. Het resultaat van een dergelijke integratie zal meer zijn dan de som der delen. Bovenal kan 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*.

Voorbij de heilige huisjes

Militair perspectief op de inlichtingenproducent-klantrelatie

Saskia Pothoven MA*

De relatie tussen inlichtingenproducenten en hun klanten is al decennialang onderwerp van debat, zowel in academische als in professionele kringen. Het militaire inlichtingendomein onderscheidt zich in een aantal belangrijke zaken van het civiele domein, en behoeft daarom speciale aandacht. Het is dus relevant om te toetsen in hoeverre heersende opvattingen over de inlichtingenproducent-klantrelatie, de 'heilige huisjes', die doorgaans zijn gebaseerd op het civiele inlichtingendomein, standhouden binnen het militaire inlichtingendomein. Dit artikel biedt aan de hand van drie onderscheidende eigenschappen en drie heilige huisjes, voortkomend uit literatuuronderzoek, een militair perspectief op de inlichtingenproducent-klantrelatie. De focus ligt hierbij op het strategische niveau.

Door institutionele inbedding zou op een militaire inlichtingenproducent druk kunnen ontstaan om analyses te leveren die niet nadelig zijn voor de eigen organisatie

FOTO MCD, KEESNAN DOGGER

Om de vraag te kunnen onderzoeken hoe de heersende opvattingen, gebaseerd op het civiele inlichtingendomein, standhouden binnen het militaire inlichtingendomein, moet eerst gekeken worden naar de eigenschappen van militaire inlichtingendiensten. Deze diensten zijn vaak het resultaat van een samensmelting of centralisering van inlichtingendiensten van verschillende krijgsmachtonderdelen en dienen hoofdzakelijk het politieke en militair-strategische niveau.[1] Zo zien we in Nederland dat de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) voortkomt uit de Militaire Inlichtingendienst (MID), die in 1988 ontstond uit een samensmelting van de Marine Inlichtingendienst (MARID), de Landmacht Inlichtingendienst (LAMID) en de Luchtmacht Inlichtingendienst (LUID). Met de introductie van de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv) in 2002 is de MID omgedoopt tot de MIVD.[2]

Militaire inlichtingendiensten hebben een aantal eigenschappen waarmee ze zich onderscheiden van civiele inlichtingendiensten. Ten eerste zien we een hoge gradatie van 'institutionele inbedding', wat betekent dat dit soort inlichtingendiensten onderdeel is van de organisatie die tegelijkertijd ook hun voornaamste afnemer is: het ministerie van Defensie. Hieronder valt ook de relatie met de inlichtingenfunctionaliteiten binnen de krijgsmacht, die verantwoordelijk zijn voor inlichtingenverzameling, analyse en disseminatie tijdens inzet van de krijgsmacht.

Deze institutionele inbedding creëert een intiemere relatie met de voornaamste afnemers dan wat gebruikelijk is in het civiele inlichtingendomein. Een mogelijk gevolg hiervan is dat hierdoor meer druk zou kunnen ontstaan op een militaire inlichtingenproducent om analyses zo aan te passen dat ze niet nadelig zijn voor de defensieorganisatie,[3] bijvoorbeeld door waarschijnlijkheidsgradaties of dreigingslevels zo aan te passen dat een wijde parlementaire steun kan ontstaan voor militaire inzet.

Een tweede eigenschap van militaire inlichtingendiensten is de mix tussen burger- en militair personeel. Strategische militaire inlichtingendiensten zoals de MIVD hebben een unieke dubbele positie omdat ze middenin de dichotomie tussen civiele en militaire inlichtingencultuur staan.[4] Zo is de meerderheid van het personeel bij de MIVD burger.[5] Hierdoor kunnen er verschillen zijn in bijvoorbeeld leiderschapsstijl en carrière- en opleidingsmogelijkheden en kunnen er complicaties ontstaan met betrekking tot een gedeelde identiteit.[6] In de context van de producent-klantrelatie binnen het militaire inlichtingendomein kan dit met name tot uitdagingen leiden tussen militair en civiel personeel aan de verschillende zijden van deze relatie.

Hoewel in dit soort organisaties de meerderheid van het personeel burger is, zijn deze inlichtingenorganisaties desalniettemin onderdeel van militaire organisaties en worden daarmee ook beïnvloedt door culturele eigenschappen die als typisch militair worden beschouwd. Dit zijn onder meer een hoge waardering voor hiërarchie, regels en discipline, competenties en status, en duidelijke gezags- en verantwoordingslijnen.[7] Eigenschappen die doorgaans een hoge waardering genieten binnen militaire organisaties, zoals besluitvaardigheid en teamwerken, kunnen conflicteren met vereisten van het inlichtingenwerk, zoals kwalificaties, het vermijden van zwart-wit denken en continue vraagstelling en revisie.[8]

Een andere eigenschap is dat militair personeel snel roteert, vaak al na drie jaar. Deze snelle rotatie kan ervoor zorgen dat kennis en een

1 Philip Davies, 'The Problem of Defence Intelligence', *Intelligence and National Security*, Vol. 31, No. 6 (2016) 799.
2 B. de Graaf, E. Muller en J. van Reijn, *Inlichtingen- en veiligheidsdiensten* (Deventer, Wolters Kluwer, 2010).
3 S. Rietjens, 'Intelligence in defence organisations: a tour de force', *Intelligence and National Security*, Vol. 35, No. 5 (2020) 719.
4 J. Thomson, 'Governance costs and defence intelligence provisions in the UK: a case study in macroeconomic theory', *Intelligence and National Security*, Vol. 31, No. 6 (2016) 854.
5 Militaire Inlichtingen- en Veiligheidsdienst, *Openbaar Jaarverslag 2019* (Den Haag, ministerie van Defensie).
6 NATO STO HFM-226 TASK GROUP 2018; I. Goldenberg e.a., 'Integrated defence workforces: Challenges and enablers of military-civilian collaboration', *Journal of Military Studies*, Vol. 8 (2019) 33.
7 J. Soeters, 'Organizational Cultures in the Military', in: G. Caforio en M. Nuciari (red.), *Handbook of the Sociology of the Military* (New York, Springer, 2018) 254.
8 M. Herman, *Intelligence Power in Peace and War* (Cambridge, Cambridge University Press, 1996) 250.

goede relatie met inlichtingenproducenten en/of klanten niet behouden wordt in de organisatie op het moment dat de betrokken persoon een andere rol gaat vervullen. Aan de andere kant kan frequente rotatie er ook toe leiden dat producenten en klanten van inlichtingen ook de andere kant van de rol vervuld hebben (bijvoorbeeld eerst als analist bij de MIVD en daarna bij de J2 van de Directie Operaties, DOPS), wat kan leiden tot een beter begrip van elkaars taken en verantwoordelijkheden.

Een laatste aspect van militaire cultuur is het januskopkarakter, wat inhoudt dat militaire organisaties in twee tegengestelde situaties werken, namelijk zowel in 'warme situaties', zoals gevechten die directe actie vereisen, en 'koude situaties', zoals trainingen, oefeningen en voorbereiding voor inzet. In het verlengde hiervan kan gesproken worden van 'warme' inlichtingen, gericht op zaken als missieondersteuning en 'koude inlichtingen', gericht op langetermijndoelstellingen.

De heilige huisjes

Het weerbericht en de paraplu

In het debat over de producent-klantrelatie inlichtingen wordt de kwestie van nabijheid vaak geproblematiseerd: hoe dichtbij of veraf moeten producenten en klanten zich tot elkaar verhouden? Hierin zijn in grote lijnen twee scholen te onderscheiden. De traditionalisten zeggen dat er een duidelijke scheiding moet zijn tussen inlichtingenanalyse en beleid, omdat anders het risico gelopen wordt dat een inlichtingenproduct beïnvloed wordt door beleidsvoorkeuren en in extreme gevallen tot politisering zou kunnen leiden. De bij de MIVD alom bekende uitspraak 'Wij zijn van het weerbericht, maar we vertellen niet of je een paraplu mee moet nemen', resoneert hier duidelijk mee. Ook de overheveling van de J2-functionaliteit van de MIVD naar de DOPS naar aanleiding van het *Rapport Dessens* uit 2006 kan binnen dit traditionele kader geplaatst worden.[9] De activistische benadering daarentegen wijst erop dat er zonder interactie ook weinig relevantie is en pleit juist voor een hechte relatie tussen producenten en klanten van inlichtingen, waarbij inlichtingen gerelateerd zijn aan en gestuurd worden door beleidsdoeleinden en inlichtingenanalisten een diepdoorwrocht begrip moeten hebben van de totstandkoming van beleid.[10]

'Wij zijn van het weerbericht, maar we vertellen niet of je een paraplu mee moet nemen'

Politisering houdt in dat inlichtingen worden aangepast zodat ze beter aansluiten bij beleidsvoorkeuren.[11] Het wordt daarom ook wel *intelligence to please* genoemd.[12] Dit kan zowel onder duidelijke dwang plaatsvinden als door het creëren van een omgeving waarin analisten zich beperkt voelen in het trekken van conclusies die niet overeenkomen met voorkeuren vanuit de leiding of de klant.[13]

9 C. Dessens, *Inlichtingen en veiligheid Defensie. Kwaliteit, capaciteit en samenwerking* (Onderzoeksgroep Inlichtingen en Veiligheid Defensie, 2006).
10 Zie J. Davis, 'The Kent-Kendall Debate of 1949', *Studies in Intelligence* Vol. 35, No. 2 (1992) 91-103.
11 Zie onder andere. J. Rovner, 'Is Politicization Ever a Good Thing?', *Intelligence and National Security*, Vol. 28, No. 1 (2013) 55-67.
12 H. Ransom, 'The Politicization of Intelligence', in: S. Cimbala (red.), *Intelligence and the Intelligence Policy in a Democratic Society* (Dobs Ferry, Transnational Publishers, 1987) 26.
13 G. Hastedt, 'The Politics of Intelligence and the Politicization of Intelligence: The American Experience', *Intelligence and National Security* Vol. 28, No. 1 (2013) 5-31; Rovner, 'Is Politicization Ever a Good Thing?', 56.

Afghanistan, 2007: met name in inzetgebieden hebben militaire inlichtingenorganisaties een intieme relatie met de inlichtingenentiteiten van de krijgsmacht FOTO TEUN VOETEN

Naast het risico tot politisering of intelligence to please lopen militaire inlichtingenorganisaties mogelijk een nog groter risico op een fenomeen dat bekend staat als *situating the estimate*. Dit houdt in dat een dreigingsinschatting wordt gevormd op basis van de capaciteiten van de krijgsmacht en dat de dreigingen waartegen niet kan worden opgetreden niet worden meegenomen in de analyse.[14]

Militaire inlichtingenorganisaties hebben, met name in inzetgebieden, een intieme relatie met de inlichtingenentiteiten van de krijgsmacht, wat versterkt wordt door de inbedding in dezelfde 'moederorganisatie'. Zo gebruiken inlichtingendiensten deze entiteiten bijvoorbeeld als sensoren ter plaatse. Tegelijkertijd kunnen deze inlichtingenentiteiten in sommige gevallen ook gebruik maken van analyses van een militaire inlichtingendienst. Afhankelijk van het niveau en het type product is het dus mogelijk om tegelijkertijd inlichtingenproducent en klant te zijn. Hierbij valt ook te denken aan een J2-sectie die een strategisch inlichtingenproduct ontvangt van een militaire inlichtingendienst en dit product gebruikt om een analyse te produceren die bedoeld is voor het tactische of operationele niveau, al gaat dit in de Nederlandse context minder op door de huidige inrichting van de DOPS J2, die niet over analysecapaciteit beschikt. Waar deze in Nederland in het klantdomein geplaatst is, is een J2-sectie in landen als de VS of het VK, door de ruime analysecapaciteit, eerder een inlichtingenproducent. Hieraan is te zien dat de producent-klantrelatie, die vaak als dichotomie wordt voorgesteld, wellicht beter geconceptualiseerd zou kunnen worden als een gelaagd netwerk van verschillende inlichtingenentiteiten.

Hiernaast kunnen verschillende eigenschappen van militaire organisaties, zoals de snelle rotatie van militair personeel, een hechter gemeenschapsleven door legering en informele banden door opleiding en uitzending, bijdragen aan een

14 S. Badsey e.a. (red.), *The Falklands Conflict Twenty Years On. Lessons for the Future* (New York, Routledge, 2004) 97.

nauwere band tussen producenten en klanten van militaire inlichtingen. De mix tussen militair en burgerpersoneel kan daarentegen de afstand vergroten. Herman noemt dit 'het fundamentele probleem van de geloofwaardigheid van de burger', die een gebrek aan kennis heeft van militaire middelen en cultuur.[15] Waar officieren doorgaans over operationele kennis en technische expertise beschikken, hebben burgermedewerkers vaker ervaring op het strategische en beleidsniveau.[16] Dit kan elkaar aanvullen, maar ook leiden tot complicaties en wederzijds onbegrip, in het bijzonder wanneer het gaat om een militaire inlichtingenanalist en een civiele afnemer en vice versa.

Analytische objectiviteit als heilige graal

Een tweede heilig huisje binnen de inlichtingenproducent-klantrelatie is het ideaal van analytische objectiviteit. Het idee hierachter is dat dit de meest effectieve manier is om beïnvloeding van een inlichtingenproduct te vermijden, en dat hierdoor ook politisering voorkomen kan worden.[17]

Objectiviteit en de afstand van besluitvorming zoals bij het eerste heilige huisje worden doorgaans beschouwd als cruciaal in het ethos van een inlichtingenanalist.[18] Ze vormen de basis voor het concept *speaking truth to power*, wat vaak genoemd wordt als een belangrijke taak van de analist. Analytische objectiviteit, bijvoorbeeld door vooroordelen in een analytisch product te elimineren door middel van analysetechnieken, wordt gebruikt als een middel voor waarheidsvinding. Het streven naar objectiviteit en een zoektocht naar de waarheid zit ingebakken in het denken van inlichtingendiensten. Niet voor niets is het motto van de MIVD *meritum in veritatum discernendo*: de verdienste ligt in het onderkennen van de waarheid.[19]

Het probleem met het streven naar analytische objectiviteit is dat het de afwezigheid van vooringenomenheid vereist, iets wat erkend onmogelijk is. Sterker nog, cognitieve biases zijn nodig om van incomplete data een inschatting te maken.[20] Hiernaast vereist het zorgen dat een afnemer van inlichtingen ongewenste feiten en interpretaties onder ogen ziet een bias richting *warning*, wat vaak beschreven wordt als (overdreven) positieve beleidsmakers versus (overdreven) pessimistische inlichtingenanalyse.[21] Ook komt het vaak voor dat afnemers inlichtingen negeren die hun niet goed uitkomen, wat de waarde van analytische objectiviteit vermindert. Een hogere mate van objectiviteit maakt inlichtingen dus niet noodzakelijk invloedrijker,[22] zeker aangezien het nemen van beslissingen vaak gepaard gaat met subjectiviteit en besluitvormers vaak meerdere versies van 'de waarheid' onder ogen krijgen.[23]

Doordat complete analytische objectiviteit in de praktijk niet haalbaar is, komen alle analisten in feite te kort als dit als standaard wordt vereist. Het zou daarom nuttig kunnen zijn om het narratief te verplaatsen van termen als 'waarheidsvinding' en speaking truth to power naar relatievere beschouwingen als integriteit en *call it as you see it*.[24] In lijn met deze overwegingen pleit Woodard bijvoorbeeld voor objectieve eerlijkheid (het expliciet maken van aannames en redenaties) in plaats van beleidsneutraliteit.[25]

Het idee van speaking truth to power is hiernaast wellicht meer van toepassing op tactische inlichtingenondersteuning dan op strategische inlichtingenanalyse.[26] Vooral in de Koude Oorlog was dit van toepassing, toen de analytische taak voornamelijk gestoeld was op tactische puzzels (zoals de hoeveelheid wapens van de Sovjet-Unie en de locatie hiervan). Na de val van de Sovjet-Unie zijn analytische vraagstukken steeds

15 Herman, *Intelligence Power in Peace and War*, 249.
16 A. Wolfberg, 'When generals consume intelligence: the problems that arise and how they solve them', *Intelligence and National Security*, Vol. 36, No. 4 (2021) 472.
17 S. Marrin, 'Analytic objectivity and science: evaluating the US Intelligence Community's approach to applied epistomology', *Intelligence and National Security*, Vol. 35, No. 3 (2020) 350.
18 Marrin, 'Analytic objectivity', 353.
19 Militaire Inlichtingen en Veiligheidsdienst, *Openbaar Jaarverslag 2019.*
20 Marrin, 'Analytic objectivity', 354.
21 Marrin, 'Analytic objectivity', 354.
22 T. Fingar, 'Intelligence and Grand Strategy', *Orbis*, Vol. 56, No. 1 (2012) 128.
23 Marrin, 'Analytic objectivity', 355.
24 Marrin, 'Analytic objectivity', 360.
25 N. Woodard, 'Tasting the Forbidden Fruit. Unlocking the Potential of Positive Politicization', *Intelligence and National Security*, Vol. 28, No. 1 (2013) 91-108.
26 J. Kerbell en A. Olcott, 'Synthesizing with clients, not analyzing for customers', *Studies in Intelligence*, Vol. 54, No. 4 (2010) 13.

BRON: CIA-PUBLICATIE 'PRESIDENT NIXON AND THE ROLE OF INTELLIGENCE IN THE 1973 ARAB-ISRAELI WAR'

Sovjet-leider Leonid Brezjnev (links) overlegt met de Amerikaanse president Richard Nixon in oktober 1973: na de val van de Sovjet-Unie zijn analytische vraagstukken steeds complexer en strategischer geworden

complexer en strategischer geworden en meer richting mysteries gegaan waar geen eenduidig antwoord op is.[27] Hierdoor is het nog moeilijker geworden om analytische objectiviteit na te streven.

Dit verschil kan ook geïllustreerd worden door de theorie van Clausewitz met die van de Zwitserse strateeg Jomini te vergelijken. Waar aanhangers van Jomini het inlichtingendomein voornamelijk als een exacte wetenschap zien dat met wiskundige logica benaderd kan worden, stelt het Clausewitziaanse denken dat er altijd een bepaalde mate van onzekerheid zal zijn in inlichtingenanalyse.[28]

Hoewel inlichtingenorganisaties over het algemeen de Clausewitziaanse denkwijze aanhangen, is het streven naar analytische objectiviteit eigenlijk meer in lijn met het Jominiaanse denken.[29] Door militaire eigenschappen zoals besluitvaardigheid, discipline en duidelijke autoriteitslijnen is het militaire inlichtingendomein wellicht nog meer gestoeld op het Jominiaanse denken dan het civiele inlichtingendomein. Hiernaast leveren militaire inlichtingendiensten doorgaans ook operationele en tactische inlichtingen, bijvoorbeeld dreigingsappreciaties of voor missieondersteuning. Deze mengeling van strategische, operationele en tactische inlichtingenondersteuning kan er mogelijk voor zorgen dat ook strategische analyse meer volgens het Jominiaanse denken wordt uitgevoerd, en dus meer als een puzzel dan als een mysterie wordt behandeld. Een voorbeeld hiervan is het Intelligence Warning System (NIWS) van de NAVO, waarbij met een scala aan indicatoren gestreefd wordt vroegtijdig nieuwe dreigingen te onderkennen.

27 W. Agrell en G. Treverton, *National Intelligence and Science. Beyond the Great Divide in Analysis and Policy* (Oxford, Oxford University Press, 2014) 36; G. Treverton, 'Risks and Riddles. The Soviet Union was a puzzle. Al Qaeda is a mystery. Why we need to know the difference', *Smithsonian Magazine*, juni 2007.

28 S. Rietjens, 'Omgevingsbewustzijn voor militaire inzet: a mission (im)possible', *Militaire Spectator* 189 (2020) (4) 174-189; Agrell en Treverton, *National Intelligence and Science*, 36.

29 Agrell en Treverton, *National Intelligence and Science*, 36.

Inlichtingen vormen de basis voor besluitvorming

Volgens de traditionele opvatting voorzien inlichtingenanalisten besluitvormers van informatie, die dit vervolgens gebruiken om beslissingen te nemen. In de praktijk vormen inlichtingen, zeker op strategisch niveau, echter lang niet altijd de basis voor besluitvorming.[30] Waar voor afnemers inlichtingenproducten niet altijd relevant genoeg zijn, zijn inlichtingenanalisten vaak gefrustreerd als hun producten niet of verkeerd gebruikt worden.[31] Hoewel dit niet altijd een probleem hoeft te zijn omdat besluitvormers andere overwegingen mee kunnen laten tellen dan alleen dat wat in een inlichtingenanalyse staat, zijn de ontwikkelingen in de VS die leidden tot de invasie in Irak in 2003 een goed voorbeeld van wat er mis kan gaan als inlichtingen misbruikt of genegeerd worden, met alle gevolgen van dien. Zo werd er aan *cherry picking* gedaan, ofwel het selectieve gebruik van inlichtingen door afnemers, en aan *stovepiping* of *b-teaming* door het Office of Special Plans.[32] Dit houdt in dat ruwe inlichtingen geanalyseerd worden buiten een inlichtingendienst om. Gerelateerd hieraan gingen inlichtingen van de Britten in Nederland rechtstreeks naar de minister-president, zonder dat de Nederlandse inlichtingendiensten hier een oordeel over konden vellen.[33] Dit soort zaken kunnen ook plaatsvinden doordat er een te sterke waarde wordt gehecht aan hiërarchie en autoriteit en een historisch voorbeeld ligt in de aanloop naar Pearl Harbor. Admiraal Richmond Turner, de Director of War Plans van de Amerikaanse marine die zelf geen inlichtingenervaring had, beschouwde de oordelen van zijn eigen divisie als superieur aan die van het Office of Naval Intelligence (ONI), die in zijn ogen te weinig senioriteit had. Als gevolg hiervan begon Turner zijn eigen inlichtingenanalyses te produceren los van het ONI, wat uiteindelijk een belangrijke oorzaak was voor het niet tijdig onderkennen van de Japanse aanval op Pearl Harbor.[34]

Aan de basis van deze traditionele opvatting ligt de inlichtingencyclus, die het inlichtingenproces opdeelt in de vijf opeenvolgende stadia initiëren, verzamelen, verwerken, analyseren en verspreiden.[35] Dit model wordt in de inlichtingenliteratuur al enige tijd bekritiseerd als een oversimplificatie van een zeer complex proces.[36] Desondanks is de inlichtingencyclus nog steeds alomtegenwoordig in het denken over de inlichtingenproducent-klantrelatie en is onder andere te vinden in verscheidene militaire doctrines, waaronder de *Nederlandse Joint inlichtingenproducent-klantrelatie 2*.[37] Men zou kunnen stellen dat door verschillende eigenschappen van militaire organisaties het gebruik van een vereenvoudigde weergave van de realiteit door middel van een model de voorkeur geniet. Ten eerste komen stereotiepe

De inlichtingencyclus wordt in de inlichtingenliteratuur al enige tijd bekritiseerd als een oversimplificatie van een zeer complex proces

30 Zie bijvoorbeeld L. Johnson, 'Bricks and mortar for a theory of intelligence', *Comparative Strategy*, Vol. 22, No. 1 (2003) 1-28; S. Marrin, 'Why strategic intelligence analysis has limited influence on American foreign policy', *Intelligence and National Security*, Vol. 32, No. 6 (2017) 725-742; Rovner, 'Is Politicization Ever a Good Thing?, 2011; P. Pillar, *Intelligence and US Foreign Policy. Iraq, 9/11, and Misguided Reforms* (New York City, Columbia University Press, 2011).

31 R. Betts, *Enemies of Intelligence. Knowledge and Power in American National Security* (New York, Columbia University Press, 2007) 67.

32 G. Mitchell, 'Team B Intelligence Coups', *Quarterly Journal of Speech*, Vol. 92, No 2 (2006) 144-173.

33 *Rapport Commissie van onderzoek besluitvorming Irak* (commissie-Davids) (Den Haag, 2010) 318.

34 M. Handel (red.), *Intelligence and Military Operations* (Londen, Routledge, 1990) 25.

35 M. Phythian (red.), *Understanding the Intelligence Cycle* (New York, Routledge, 2013) 21; S. Marrin, 'Intelligence Analysis and Decision-making', in: P. Gill e.a. (red.), *Intelligence Theory. Key Questions and Debates* (New York, Routledge, 2009) 133.

36 Zie onder andere G. Evans, 'Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle', *Defence Studies*, Vol. 9, No. 1 (2009) 22-46; A Hulnick, 'What's wrong with the Intelligence Cycle', *Intelligence and National Security*, Vol. 21, No. 6 (2006) 959-979; G. Eriksson, 'A theoretical reframing of the intelligence-policy relation', *Intelligence and National Security*, Vol. 33, No. 4 (2018) 553-561; Marrin, 'Why strategic analysis has limited influence'.

37 *Joint Doctrine Publicatie 2. Inlichtingen* (Den Haag, ministerie van Defensie, 2012) 48.

militaire eigenschappen zoals een top-down organisatiestructuur en duidelijke gezagslijnen niet altijd overeen met de complexiteit van dag-tot-dag situaties. Doctrinair denken is sterk aanwezig binnen de militaire cultuur, wat gepaard gaat met het gebruik van modellen om een weerbarstige werkelijkheid weer te geven. Hiernaast heeft de snelle rotatie van militair personeel tot gevolg dat vaktechnische kennis en ervaring lastig behouden blijft binnen militaire inlichtingenorganisaties. Om deze kennis te waarborgen en adequaat over te dragen aan nieuwe medewerkers komen modellen als de inlichtingencyclus goed van pas. Desalniettemin draagt het uitleggen van complexe relaties zoals die tussen inlichtingenproducenten en klanten in termen van vereenvoudigde modellen als de inlichtingencyclus niet bij aan een dieper begrip van deze relatie. Hiervoor zijn alternatieven zoals het 'inlichtingenweb' van Gill en Phythian, dat erkent dat er meerdere complexe interacties plaatsvinden tussen de verschillende punten van zaken als doelstelling, collectie, analyse, wellicht meer passend.[38]

Ook het januskopkarakter van militaire organisaties beïnvloedt de impact die inlichtingenanalyses hebben op besluitvorming. In het spectrum van 'warme' naar 'koude' inlichtingen zijn besluitvormers over het algemeen ontvankelijker voor 'warme' inlichtingen, zoals operationeel-tactische inlichtingen die een directe beslissing vereisen, of inlichtingen die direct bijdragen aan besluitvorming rond militaire inzet. 'Koude' inlichtingen, zoals strategische inlichtingenanalyses gericht op de lange termijn, worden over het algemeen makkelijker aan de kant gezet omdat ze geen directe actie vereisen. Officieren doen aan de 'klantzijde' vaak pas ervaring op met strategische inlichtingen als zij hogere rangen bereiken.[39] Dit gebrek aan ervaring met 'koude' inlichtingen kan een reden zijn dat militaire besluitvormers vaak ontvankelijker zijn voor de 'warmere' kant van het spectrum. Dit is ook beschreven door Handel, die erop wijst dat generaals soms hun ervaring en werkwijze met tactisch-operationele inlichtingen toepassen op het strategische inlichtingendomein, dat een andere manier van werken vereist.[40] Dit is problematisch omdat een gebrek aan ervaring met de hogere niveaus van operationele en strategische inlichtingen kan leiden tot *intelligence failures* wanneer deze inlichtingen niet goed worden toegepast.[41]

Conclusie

Het doel van dit artikel was om aan de hand van een drietal heilige huisjes te onderzoeken in hoeverre de doorgaans gebruikelijke denkwijze over de inlichtingenproducent-klantrelatie ook standhoudt binnen het militaire inlichtingendomein.

Ten eerste komt naar voren dat door verschillende eigenschappen van militaire organisaties de inlichtingenproducent-klantrelatie complexer en meer gelaagd is dan doorgaans erkend wordt in de inlichtingenliteratuur. De dichotomie tussen producenten en klanten die in zowel de traditionele als in de activistische benadering te vinden is, is hierdoor wellicht minder van toepassing op het militaire inlichtingendomein. Waar het narratief deze relatie vaak schetst in het kader van separate rollen en taakstellingen, zou een voorstelling van deze relatie in meer overlappende en gelaagde rollen kunnen bijdragen aan een verdergaand begrip van het genetwerkte en veelzijdige karakter van de inlichtingenproducent-klantrelatie binnen het militaire domein.

Ten tweede volgt uit de hoge gradatie van institutionele inbedding dat militaire inlichtingenorganisaties wellicht ontvankelijker kunnen zijn voor (in)directe druk om inlichtingenanalyses te conformeren aan besluitvorming. Een gebrek aan empirische data maakt het vooralsnog onmogelijk om hier eenduidige uitspraken over te doen. Het streven naar analytische objectiviteit, wat gezien wordt als

38 Phythian, *Understanding the Intelligence Cycle*, 34.
39 Wolfberg, 'When generals consume intelligence', 460.
40 Handel, *Intelligence and Military Operations*, 26.
41 Handel, *Intelligence and Military Operations*; Wolfberg, 'When generals consume intelligence', 460.

Besluitvormers zijn over het algemeen ontvankelijker voor 'warme' inlichtingen, zoals operationeel-tactische inlichtingen, die een directe beslissing vereisen

FOTO MCD, EVA KLIJN

een manier om vrij van beïnvloeding te blijven, is door de Jominiaanse voorkeuren van militaire organisaties mogelijk sterker aanwezig, wat kan leiden tot een onhaalbaar streven naar absolute objectiviteit en de 'absolute waarheid'. Voor een betere toepassing van inlichtingenproducten kan het goed zijn om in plaats hiervan waarden te omarmen als eerlijkheid en call it as you see it, die in lijn zijn met militaire waarden en daarom goed zouden passen in een militaire inlichtingenorganisatie.

Ten derde zijn ook afnemers van militaire inlichtingenproducten niet altijd even ontvankelijk voor de inlichtingen die zij ontvangen, wat over en weer tot frustratie kan leiden. Een beter begrip van de inlichtingenproducent-klantrelatie, bijvoorbeeld door middel van het 'inlichtingenweb' of het januskopprincipe, zou kunnen bijdragen aan een verbeterd begrip van de manier waarop inlichtingen bijdragen aan besluitvorming.

Er kan dus gesteld worden dat de militaire inlichtingenproducent-klantrelatie andere overwegingen en zienswijzen vereist dan het civiele inlichtingenproces. Om te komen tot een beter en dieper begrip van deze processen in een militaire context is empirisch onderzoek noodzakelijk. ■

Gefrustreerde en gerealiseerde ambities

De Nederlandse militaire inlichtingen- en veiligheidsdienst(en), 1912-2022

Bob de Graaff*

Goede wijn moet rijpen. Dat gold ook voor de Nederlandse militaire inlichtingen- en veiligheidsdiensten, waarvoor als 'geboortedag' vaak 25 juni 1914 wordt aangehouden, de datum waarop de derde afdeling van de Generale Staf, GSIII, gestalte kreeg. Het lijkt echter meer gerechtvaardigd om het jaar 1912 als uitgangspunt te nemen, toen een Studiebureau Vreemde Legers in het leven werd geroepen. Wie de 110-jarige geschiedenis van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en zijn voorgangers overziet, moet echter concluderen dat in het geval van deze militaire diensten het rijpingsproces lang op zich liet wachten. En dat kwam niet door een gebrek aan ambities. In deze bijdrage wil ik in vogelvlucht de geschiedenis van de dienst en zijn voorgangers de revue laten passeren. Daarbij neem ik als uitgangspunt de ambities van de opeenvolgende diensten en de vraag naar de realisering daarvan.

Oefening met een Raven, een onbemand verkenningssysteem. Dit artikel bespreekt in vogelvlucht de geschiedenis van de Militaire Inlichtingen- en Veiligheidsdienst en zijn voorgangers

FOTO MCD, EVA KLIJN

* Bob de Graaff is emeritus hoogleraar intelligence en security studies. Eind 2022 verschijnt van zijn hand het boek *Ongekend en onderscheiden. De geheime geschiedenis van de MIVD* bij uitgeverij Boom. Het boek is het resultaat van een opdracht van de MIVD en het Nederlands Instituut voor Militaire Historie (NIMH). Voor zijn onderzoek kreeg hij toegang tot het archief van de MIVD. Tenzij expliciet anders vermeld, is dit artikel gebaseerd op de bevindingen opgedaan bij dit onderzoek.

1 M. de Meijer, *De geheime dienst in Nederland*, 1912-1947 (niet uitgegeven) 177.

Na de Tweede Wereldoorlog werd de lat nog hoger gelegd

Ambities en aspiraties

Aan ambities heeft het nooit ontbroken. Nadat in 1919 in het neutrale Nederland onder de vleugels van GSIII ook een binnenlandse veiligheidsdienst was geschoven, meende de leider daarvan, generaal-majoor J.W. van Oorschot, dat de taak van zijn dienst 'wel verre van een begrensd militaire er een was van veel wijdere, het geheele Volk omvattende, strekking'.[1] Toen aan het eind van de Tweede Wereldoorlog en kort daarna planvorming over een of meer Nederlandse militaire inlichtingen- en veiligheidsdiensten plaatsvond, werd de meetlat nog hoger gelegd. Diverse betrokkenen meenden dat, terwijl Nederland militair gezien moeite zou hebben zijn steentje bij te dragen aan nieuwe bondgenootschappelijke verhoudingen, het Nederlandse inlichtingenwerk dit ruim zou kunnen compenseren. Het militaire inlichtingenbedrijf zou Nederland in staat stellen internationaal in een hogere gewichtsklasse mee te doen.[2]

Dat dit nauwelijks lukte, lag ten dele aan het feit dat Nederland drie militaire diensten kreeg, de Landmachtinlichtingendienst (LAMID), de Luchtmachtinlichtingendienst (LUID) en de Marine Inlichtingendienst (MARID), die volstrekt gescheiden optrokken. Nadat de wetgever in 1987 in de eerste Wet op de inlichtingen- en veiligheidsdiensten had bepaald dat er één Militaire Inlichtingendienst (MID) zou zijn, duurde het maar liefst dertien jaar voordat deze dienst een feit was en deze de veren van de afzonderlijke diensten had afgeschud. De volgende wet, van 2002, bepaalde dat er naast de civiele Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zou zijn. De directeur daarvan tussen 2006 en 2011, Pieter Cobelens, streefde deelname van zijn dienst na in, wat hij noemde, de 'Champions League' van de westerse inlichtingen- en veiligheidsdiensten.[3]

Naast de internationale aspiraties was er vanaf de Tweede Wereldoorlog ook steeds een behoefte aan gelijkstelling met de civiele dienst, eerst de Binnenlandse Veiligheidsdienst (BVD) en later de AIVD. In het archief van de MIVD en zijn voorgangers is voortdurend ergernis waarneembaar over de hautaine opstelling van, wat men noemde, de 'nevendienst'. Lange tijd kwam dit doordat de BVD over bijzondere bevoegdheden beschikte, zoals telefoon tappen, het plaatsen van microfoons en het heimelijk binnendringen van woningen, die de militaire diensten werden onthouden. Op grond daarvan meende de BVD dat de militaire diensten slechts een zeer beperkte contra-inlichtingentaak hadden. Deze mocht zich niet uitstrekken voorbij de hekken van de militaire terreinen. Op grond van het verschil in bevoegdheden meende de Chef Generale Staf G.J. le Fèvre de Montigny in 1960 zelfs dat het onderscheid tussen de BVD en de militaire diensten niet gebaseerd moest zijn op de 'hekkentheorie'. Voor hem was het verschil simpel: de BVD bediende zich van onfatsoenlijke methoden en de LAMID van fatsoenlijke. Het zal geen verrassing zijn dat zijn voorstel het onder-

2 B. de Graaff en C. Wiebes, *Villa Maarheeze. De geschiedenis van de Inlichtingendienst Buitenland* (Den Haag, Sdu, 1998) 33-34; F.A.C. Kluiters, *De Nederlandse inlichtingen- en veiligheidsdiensten* (Den Haag, Sdu Uitgeverij Koninginnegracht, 1993) 43-44 en 240-241; F.A.C. Kluiters, *De Nederlandse inlichtingen- en veiligheidsdiensten. Supplement* (Den Haag, Sdu Uitgeverij Koninginnegracht, 1995) 155-156.

3 'Het werk in Uruzgan is echt Champions League', *BN De Stem*, 7 juni 2011; 'Directeur MIVD, Generaal-Majoor Pieter Cobelens verlaat binnenkort de dienst', in: *Ingelicht. Informatiemagazine voor de MIVD*, maart 2011, 4 (4-5); E. van Outeren en S. Derix, 'Zondebok bij de politiek, succesnummer bij NAVO', *NRC Handelsblad*, 1 juni 2011; O. den Hollander, 'Pieter Cobelens: "Nederland kan een digitale superpower worden"', *Quote*, januari 2021.

FOTO BEELDBANK NIMH

Chef Generale Staf G.J. le Fèvre de Montigny ontvangt een Britse generaal. Volgens De Montigny was het verschil tussen de BVD en de LAMID simpel: de eerste gebruikte onfatsoenlijke methoden, de tweede fatsoenlijke

scheid aldus in formele regelgeving vast te leggen strandde.

Eind jaren negentig baseerde het hoofd van de MID, brigadegeneraal J.C.F. (Hans) Knapp, zijn betoog om van de directeur van de dienst een tweesterrengeneraal te maken geheel op de buitenlandse en binnenlandse aspiraties van de dienst. In de omgang met de hoofden van buitenlandse partnerdiensten was de tweede ster volgens hem onmisbaar en op grond van de gelijkwaardigheid die inmiddels tussen de BVD en de MID bestond bovendien gerechtvaardigd. Er waren geen wezenlijke verschillen meer tussen beide diensten qua personeelsomvang en takenpakket en, wanneer de nieuwe wet (van 2002) van kracht zou zijn, evenmin qua bevoegdheden. Het betoog van Knapp werd echter de nek omgedraaid door de directeur-generaal Personeel van Defensie, die meende dat de MID nog steeds niet dezelfde maatschappelijke relevantie had als de BVD.[4]

4 Zie ook C. Wiebes, *Intelligence en de oorlog in Bosnië, 1992-1995. De rol van de inlichtingen- en veiligheidsdiensten* (Amsterdam, Boom, 2002) 120.

Hier wreekte zich dat de BVD meer 'smoel' had gekregen dan de MID, die bijvoorbeeld pas na Knapp, in 1998, zijn eerste jaarverslag uitbracht, terwijl de BVD dat toen al jaren deed. Bovendien duurde het daarna nog tien jaar voordat een persconferentie het verschijnen van het MI(V)D-jaarverslag begeleidde. Na de terroristische aanslagen van 11 september 2001 nam de politieke en publieke belangstelling voor de MIVD toe. Het aantal bezoeken van nationale gezagsdragers aan de dienst steeg sterk. De vaste Kamercommissie voor Inlichtingen- en Veiligheidsdiensten, die vele jaren uitsluitend een commissie voor de BVD was geweest, begon de diensten als gelijkwaardig te behandelen. Dit gold eveneens voor de in 2002 in het leven geroepen onafhankelijke Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. Ook het aanwijzingsbesluit vanaf 2003, waarin de nationale inlichtingen- en vanaf 2015 ook de veiligheidsbehoeften[5] voor beide diensten werden vastgelegd, droeg bij aan de gelijkwaardigheid.

Voor een breder publiek werd de gelijkwaardigheid visueel toen tijdens debatten in de aanloop naar het referendum over de derde Wet op de inlichtingen- en veiligheidsdiensten, van 2017, het hoofd van de MIVD, Onno Eichelsheim, en zijn AIVD-collega Rob Bertholee geregeld zij aan zij optraden. Het voorlopig hoogtepunt van de grotere zichtbaarheid van de dienst was de persconferentie in november 2018, waarop Eichelsheim uit de doeken deed hoe zijn dienst een hackoperatie van de Russische militaire inlichtingendienst GROe bij de organisatie voor het verbod op chemische wapens, OPCW, in Den Haag had verijdeld.

Hoewel het tussen de MIVD en de AIVD altijd een beetje Ajax-Feyenoord zal blijven, zoals Cobelens het in 2011 bij zijn afscheid noemde,[6] werken de beide diensten inmiddels op tal van terreinen op voet van gelijkheid samen. Bovendien staat legitimering van hun bestaan in eigen land nauwelijks ter discussie en hebben zij beide een behoorlijk internationaal aanzien.

Financiën

Hoe komt het dat het zo lang heeft geduurd voordat de militaire diensten het aanzien bereikten waarnaar zij steeds streefden? Bovenal was dit een kwestie van financiën. Het in 1912 opgerichte Studiebureau Vreemde Legers en zelfs aanvankelijk nog GSIII waren eenmansbedrijfjes. Weliswaar kon GSIII tijdens de Eerste Wereldoorlog uitgroeien tot een personeelsbestand van twee dozijn medewerkers, maar dat was weinig voor een neutraal land dat een van de belangrijkste 'spionnennesten' voor de oorlogvoerende landen werd.[7] Het noopte het toenmalige hoofd van GSIII, H.A.C. (Han) Fabius, tot invoering van een systeem dat even goed paste bij het neutraliteitsbeleid van de regering als bij de stand van de financiën. Individuele medewerkers van de dienst onderhielden elk afzonderlijk contact met de in Nederland gestationeerde militaire attachés van de oorlogvoerende landen. Met deze militaire attachés en informeel ook met de leiders van de in Nederland actieve buitenlandse spionagenetwerken werd afgesproken dat deze inlichtingendiensten weliswaar mochten opereren op Nederlands grondgebied, maar dat zij slechts tegen andere landen en niet tegen Nederland zelf mochten spioneren, dat zij zich moesten onthouden van het gebruik van geweld of het op ander wijze overtreden van Nederlandse wetten, en dat zij hun informatie moesten delen met de Nederlandse dienst.[8] Door, in

5 In wat toen ging heten: de geïntegreerde aanwijzing.

6 'Directeur MIVD, Generaal-Majoor Pieter Cobelens verlaat binnenkort de dienst'.

7 E. Ruis, *Spionnennest 1914-1918. Spionage vanuit Nederland in België, Duitsland en Engeland* (s.l., Just Publishers, 2012); W. Klinkert, '"Espionage Is Practised Here on a Vast Scale". The Neutral Netherlands, 1914-1940', in: F. Baudet, E. Braat, J. van Woensel en A. Wever (red.), *Perspectives on Military Intelligence from the First World War to Mali. Between Learning and Law* (The Hague: Asser Press/Springer, 2017) 23-54.

8 Zie bijvoorbeeld H.A.C. Fabius, 'De inlichtingendienst van den Generalen Staf. Het z.g. bureau G.S. III. Herinneringen uit de mobilisatiejaren 1914-1919', *Bijdragen voor Vaderlandsche Geschiedenis en Oudheidkunde*, reeks 7, deel 8 (1937), 199-200 en 210-211 (196-212); A. Wolting, 'De eerste jaren van de Militaire Inlichtingendienst (GSIIIJ914-1917)', in: *Militaire Spectator* 134 (1965) (12) 566-51, 569; Ruis, *Spionnennest*, 78-79, 153, 192, 209, 227-228, 239; W. Klinkert, 'A spy's paradise? German espionage in the Netherlands, 1914-1918', in: *Journal of Intelligence History* 12 (2013) (1) 21-35, 21 en 24; idem, 'Fabius', 389; M. Smith, *Six. A History of Britain's Secret Intelligence Service* (London, Dialogue, 2010) 71-72; idem, 'Hendrik Anton Cornelis Fabius, 1878-1959. Stille strijder achter de schermen', in: W. Klinkert, S. Kruizinga en P. Moeyes, *Nederland neutraal. De Eerste Wereldoorlog 1914-1918* (Amsterdam, Boom, 2014) 374-421; 'Neutraal Nederland was werkterrein van spionnen en contra-spionnen. Men liet agenten rustig hun gang gaan en trok profijt uit gegevens van beide partijen', *Het Parool*, 2 juli 1949.

Inlichtingenpersoneel van de luchtmacht bekijkt foto's. Verschillende onderzoekscommissies benadrukten de noodzaak voor voldoende eigen capaciteit bij de militaire inlichtingendienst

FOTO BEELDBANK NIMH

elk geval formeel, alle partijen op dezelfde manier te behandelen werd de neutraliteit gehandhaafd en zat GSIII ook nog eens voor een dubbeltje op de eerste rij.

Toen in 1919 een Centrale Inlichtingendienst werd opgericht, camoufleerde de regering dit onderdeel door deze binnenlandse veiligheidsdienst als GSIIIB onder te brengen bij de generale staf, waarbij GSIIIA belast bleef met inlichtingenvergaring ten aanzien van het buitenland. Juist deze camouflage zat uitbreiding van GSIIIB in de weg, want de regering betaalde de dienst uit het krappe fonds voor geheime uitgaven van het ministerie van Oorlog. Omdat de regering de Centrale Inlichtingendienst alias GSIIIB niet in de publieke schijnwerpers wilde zetten, konden de (geheime) uitgaven ook niet drastisch worden verhoogd, want dit zou de aandacht trekken van het parlement.[9] Gedurende een groot deel van zijn bestaan telde GSIIIB daarom slechts een hoofd en een administratieve kracht, die vanaf 1930 dan nog werden bijgestaan door de pro deo werkende broer van het hoofd van GSIIIB. Toen in de tweede helft van de jaren dertig in zowel Nederland als Indië bij de marine inlichtingenelementen tot stand kwamen, was het personeel daarvan in beide gevallen ook op één hand te tellen.

De opgelegde financiële beperkingen hadden uiteindelijk een desastreuze uitwerking. Het stelsel dat Fabius tijdens de Eerste Wereldoorlog had geïntroduceerd raakte in de jaren dertig in onbalans, doordat Duitsland er niet langer aan meewerkte. GSIII werkte echter door alsof er niks was veranderd. Toen in november 1939 twee Britse inlichtingenofficieren bij Venlo besprekingen voerden met, naar zij veronderstelden, vertegenwoordigers van de Duitse militaire oppositie tegen Hitler, werden zij dan

9 Zie bijvoorbeeld Nationaal Archief, Den Haag, 2.04.26.01, ministerie van Binnenlandse Zaken, inv.nr. 541, exh. 11 oktober 1919 nr. 1095.

ook begeleid door een officier van GSIIIA, luitenant Dirk Klop. Tegenover de Duitse gesprekpartners had hij zich als Brit voorgedaan. Nadat een Duits SS-commando op 9 november de Britten en Klop over de grens had ontvoerd, troffen de Duitsers op het lichaam van Klop, die bij het incident dodelijk was getroffen, papieren aan waaruit zijn Nederlanderschap bleek. Daarmee was het Nederlandse neutraliteitsbeleid ernstig in diskrediet gebracht. Diensthoofd Van Oorschot moest aftreden. En toen de Duitsers in mei 1940 Nederland binnenvielen, noemden zij het optreden van Klop als een van de neutraliteitsschendingen door de Nederlandse overheid die hun invasie moest legitimeren.[10]

Het Venlo-incident maakte duidelijk dat de Nederlandse regering goed moest nadenken over de vraag wat het land zelf op het gebied van militaire inlichtingen verrichtte en wat het met vertrouwen kon overlaten aan buitenlandse partners. Toen de Nederlandse regering tijdens de bezetting van Nederland en Indië inlichtingenoperaties moest opzetten vanuit respectievelijk Engeland en Australië en Ceylon (Sri Lanka) drong dit inzicht zich nog duidelijker op. Omdat de Nederlandse regering en het Indische gouvernement geen stay-behind-organisaties hadden achtergelaten en het verzet moeite had de weg naar vrij gebied te vinden, waren Nederland en Indië in respectievelijk Europa en Azië, in elk geval aanvankelijk, het gebied waaruit de geallieerden de minste inlichtingen bereikten.[11] Dit veroorzaakte uiteraard irritatie bij de Britten en Amerikanen, die daarom dreigden eigen agenten uit te zenden, wat natuurlijk een affront voor de Nederlandse soevereiniteit en een bedreiging van de nationale belangen zou zijn geweest. Gebrek aan onder meer transport- en communicatiemiddelen maakte de Nederlandse inlichtingenorganisaties bovendien afhankelijk van de Britse en Amerikaanse partners.

Deze les was na de oorlog wel geleerd. De inrichting van het Nederlandse inlichtingenlandschap was echter zodanig dat de militaire diensten weinig ruilmateriaal hadden met buitenlandse diensten. Buitenlandse agentenoperaties waren over het algemeen voorbehouden aan de civiele Buitenlandse Inlichtingendienst (BID), in 1972 omgedoopt in Inlichtingendienst Buitenland (IDB). In hoofdzaak hadden de Nederlandse diensten slechts op het terrein van verbindingsinlichtingen, door informatie van de militaire attachés in Belgrado en Warschau (de enige twee Nederlandse posten achter het IJzeren Gordijn), en door onderzeebootpatrouilles[12] zelf verworven materiaal dat interessant was voor de partners.

Dit veranderde na de opheffing van de IDB begin jaren negentig. Vanaf dat moment ging de MID en later de MIVD interessante inlichtingenoperaties met menselijke bronnen uitvoeren, die de dienst in de contacten met buitenlandse zusterdiensten prestige bezorgden. Belangrijk was ook de conclusie waartoe kort na elkaar twee commissies kwamen die benadrukten dat de MIVD voldoende eigen capaciteit moest hebben om zelfstandige verwerving en analyse van inlichtingen mogelijk te blijven maken. Dat was allereerst de commissie-Dessens, die in 2005 en 2006 onderzoek deed naar de rechtmatigheid en doelmatigheid van de inlichtingen- en veiligheidscapaciteit bij Defensie, en daarna in 2010 de commissie-Davids, die de besluitvorming op weg naar de Irakoorlog van 2003 onderzocht.[13] Daarmee werd een stevige bodem gelegd onder een inmiddels aanzienlijk uitgebreide personeelscapaciteit. Dit fundament werd nog versterkt door het stelsel dat de MIVD in 2012 zelf ontwikkelde en dat bekendheid kreeg als

10 B. de Graaff, 'From seduction to abduction: how the Venlo Incident occurred', in: B. de Graaf, B. de Jong en W. Platje (red.), *Battleground Western Europe. Intelligence Operations in Germany and the Netherlands in the Twentieth Century* (Amsterdam, Het Spinhuis, 2007) 49-70; B. de Graaff, 'Trefpunt Venlo: Amerikaans-Belgisch-Brits-Frans-Nederlandse spionagesamenwerking ten aanzien van nazi-Duitsland in 1939', in: *Mededelingen van de Sectie Militaire Geschiedenis van de Landmachtstaf*, deel 15, 's-Gravenhage 1993, 105-142.

11 L. de Jong, *Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog*, IX ('s-Gravenhage, Martinus Nijhoff, 1979) 890, 917, 927, 954 en 969; L. de Jong, *XIV*, 280-281; B. de Graaff, 'Hot intelligence in the tropics. Dutch intelligence operations in the Netherlands East Indies during the Second World War', in: *Journal of Contemporary History* 22 (1987) 568-569 (563-584); Ch. Cruickshank, *SOE in the Far East* (Oxford en New York, Oxford University Press, 1983) 137 en 150.

12 W. Platje, *Een zee van geheimen. Inlichtingenoperaties tijdens de Koude Oorlog* (Amsterdam, Boom, 2010) 22 en 197-198.

13 Onderzoeksgroep Inlichtingen en Veiligheid Defensie, *Inlichtingen en Veiligheid Defensie: Kwaliteit, Capaciteit en Samenwerking*, 's-Gravenhage 2006; *Rapport commissie van onderzoek besluitvorming Irak* (Amsterdam, Boom, 2010).

Wegen en Prioriteren. Het was bedoeld om de afnemers van de producten van de dienst ervan te doordringen welke kosten gemoeid waren met een bepaalde vraag.

Regeringsdienst of bevelhebbersdienst?

Realisering van een bepaald ambitieniveau was lange tijd ook moeilijk doordat de militaire inlichtingen- en veiligheidsdiensten geregeld in een spagaat hebben gestaan ten aanzien van de vraag waartoe zij op aarde waren. Tot 1940 was GSIII gedeeltelijk een bevelhebbersdienst. Dit gold in het bijzonder voor GSIIIA, dat informatie moest verzamelen over de slagordes en intenties van buitenlandse legers. Tegelijk was GSIIIB vooral een regeringsdienst. Hij was in 1919 ingesteld door de regering, omdat deze een herhaling wilde voorkomen van wat er in november 1918 was gebeurd ten tijde van de zogeheten Troelstra-revolutie. Toen rond de wapenstilstand aan het eind van de Eerste Wereldoorlog de tronen in Europa wankelden, meende de leider van de sociaaldemocraten, P.J. Troelstra, dat Nederland ook wel een revolutie kon gebruiken. Veel kwam daar niet van, maar enkele gezagsdragers waren zodanig geïmponeerd geweest dat zij, bij wijze van spreken, reeds met de pootjes omhoog op de rug waren gaan liggen. De Centrale Inlichtingendienst/GSIIIB had daarom expliciet tot taak eventuele dreigingen tot hun ware proporties terug te brengen. Het leidde bij deze dienst tot een neiging om dreigingen te minimaliseren en vooral best case scenario's te schetsen.

Na de Tweede Wereldoorlog meenden de LAMID, LUID en MARID dat zij er primair en vrijwel uitsluitend waren voor de bevelhebbers van de drie respectievelijke krijgsmachtdelen. Omgekeerd hadden de opeenvolgende ministers, eerst van Oorlog en Marine en later van Defensie, decennialang weinig belangstelling voor de militaire diensten. Dit veranderde pas echt in de eerste helft van de jaren tachtig. De vermeende betrokkenheid van de militaire attaché in Suriname, Hans Valk,[14] bij de coup van Bouterse en een aantal contra-inlichtingenincidenten met betrekking tot de Vereniging van Dienstplichtige Militairen (VVDM) en antimilitaristen, legden het gebrek aan politiek sturing toen pijnlijk bloot. Dit droeg bij aan de eis van het parlement bij de besprekingen van het voorstel dat zou uitmonden in de wet van 1987, dat de drie diensten zouden worden samengevoegd tot één Militaire Inlichtingendienst.

De inrichting van het Nederlandse inlichtingenlandschap was zodanig dat de militaire diensten weinig ruilmateriaal hadden met buitenlandse diensten

Er volgde echter nog meer dan een decennium van strijd tussen de opeenvolgende hoofden van de MID en de centrale organisatie enerzijds en de bevelhebbers en hun vertegenwoordigers bij de centrale organisatie anderzijds. Centraal daarbij stond de vraag voor wie de MID er nu eigenlijk moest zijn, het 'Plein' of de bevelhebbers, en of de dienst zich moest beperken tot strategische inlichtingen of dat hij ook operationele inlichtingen moest verschaffen. Het leidde eind jaren negentig tot een grote malaise onder het personeel van de MID, dat voortdurend werd geconfronteerd met klachten dat de inlichtingenproductie niet werd gewaardeerd door de afnemers bij de krijgsmacht.

14 E. de Vries, *Hans Valk. Over een Nederlandse kolonel en een coup in Suriname (1980)* (Zutphen, Walburg Pers, 2021).

Achtereenvolgende benoemingen van directeuren met een sterke operationele ervaring, zoals Joop van Reijn (1999-2002), Bert Dedden (2002-2006) en Pieter Cobelens (2006-2011), leidden ertoe dat de MI(V)D zich als een strategische dienst met een operationele doelstelling ging zien. Nadat de dienst was overgegaan tot ondersteuning van de uitgezonden eenheden op locatie kwam zelfs tactische inlichtingenondersteuning soms op het bordje van de MIVD terecht. Het was ook een uitvloeisel van het feit dat bij crisisbeheersingsoperaties het scherpe onderscheid tussen strategische, operationele en tactische niveaus vaak wegviel. Niettemin bleef er discussie mogelijk over de verhoudingen waarin en de wijze waarop op de verschillende niveaus inlichtingensteun kon worden verleend. Zo verrichtte de MIVD enkele jaren, onder Dedden, de J2-functie van de Commandant der Strijdkrachten, maar werd dit later weer teruggedraaid.

Ook het aanwijzingsbesluit en de geïntegreerde aanwijzing maakten het nog steeds mogelijk dat de MIVD verscheurd zou raken tussen de wensen van de regering en die van de militaire afnemers. Dit was bijvoorbeeld in de jaren negentig het lot geweest van het Technisch Informatie- en Verwerkingscentrum, voorheen MARID VI of Wiskundig Centrum (WKC), dat interceptie verrichtte voor zowel de regering als de marine. Bijna had de Admiraliteitsraad het centrum opgeheven, omdat het nut ervan voor het eigen krijgsmachtdeel onvoldoende duidelijk was en men in dat geval liever een fregat had.[15]

15 Zie ook M.W. Jensen en G. Platje, *De MARID. De Marine Inlichtingendienst van binnenuit belicht* (Den Haag, Sdu Uitgevers, 1997) 389-390; Wiebes, *Intelligence en de oorlog in Bosnië*, 145.

Problematisch was ook dat de inlichtingenketen, dat wil zeggen de relatie van de MIVD met overige inlichtingenelementen van Defensie, onvoldoende hecht was. De commissie-Dessens constateerde dit al in 2006[16] en dit probleem lijkt nog altijd niet geheel geadresseerd te zijn. Op de achtergrond lijkt de oude controverse tussen de centrale organisatie en de bevelhebbers nog steeds een rol te spelen. Afgezien van, op zich begrijpelijke, belangentegenstellingen, is waarschijnlijk ook een oorzaak dat de centrale organisatie er voortdurend voor is teruggeschrokken om zelf invulling te geven aan een overkoepelende inlichtingenfilosofie.[17] Zij heeft dit altijd overgelaten aan eerst de School Militaire Inlichtingendienst en later aan het Defensie Inlichtingen- en Veiligheidsinstituut (DIVI).

Nieuwe ambities?

Wellicht is het zelf ter hand nemen van de formulering van een inlichtingenfilosofie een ambitie die de MIVD zou moeten koesteren. Daar lijkt ook des te meer behoefte aan te bestaan nu enkele traditionele uitgangspunten van het militaire inlichtingenwerk aan het verschuiven zijn. Waar er tot voor kort een scherpe waterscheiding bestond tussen inlichtingen en beleid, lijkt de MIVD steeds meer op te schuiven naar het schetsen van het handelingsperspectief. En waar de MIVD nog steeds voornamelijk streeft naar het presenteren van objectiveerbare gegevens in de beslotenheid van het regeringsberaad, zijn de Britse en Amerikaanse partners er in het conflict rond Oekraïne toe overgegaan gegevens over het verloop van de oorlog en intenties van het Russische bewind dagelijks uit te venten.[18]

Het verleden heeft bewezen dat de opeenvolgende militaire inlichtingendiensten zichzelf onder zich wijzigende omstandigheden steeds opnieuw moesten uitvinden. Te lang in een bepaalde modus stilstaan droeg risico's met zich mee. Tegelijk heeft de MIVD de afgelopen twee decennia laten zien actief en tijdig koerswijzigingen in de eigen werkwijze te kunnen doorzetten, bijvoorbeeld met offensieve operaties met menselijke bronnen of op het cyberterrein. Dat veel ambities uit het verleden inmiddels zijn gerealiseerd, mag echter geen reden zijn op de lauweren te gaan rusten. Het tempo waarin de wijzigingen in de taakomgeving zich voltrekken lijkt namelijk te versnellen. Aanvankelijk voltrokken de veranderingen zich in een laag tempo. Na bijna dertig jaar neutraliteitsbeleid volgde veertig jaar bondgenootschappelijke samenwerking tijdens de Koude Oorlog. Maar daarna volgden de veranderingen elkaar snel op, van ondersteuning ten behoeve van crisisbeheersingsoperaties tussen ruwweg 1990 en 2010 naar terrorismebestrijding vanaf 2001, naar cyberactiviteiten in het tweede decennium van de 21e eeuw, met recent weer een verschuiving richting het interstatelijk en misschien zelfs het grootschalig conflict. Bovendien verdringt het ene dreigingsaspect niet langer het andere, maar bestaan verschillende aspecten naast elkaar. Tijd dus voor een ambitieuze inlichtingendienst om zich te bezinnen op de toekomst van de eigen werkwijze en het debat daarover te faciliteren. ■

De MIVD heeft de afgelopen twee decennia laten zien actief en tijdig koerswijzigingen in de eigen werkwijze te kunnen doorzetten, bijvoorbeeld met offensieve operaties met menselijke bronnen of op het cyberterrein

FOTO MCD, EVA KLIJN

16 Onderzoeksgroep Inlichtingen en Veiligheid Defensie, Inlichtingen en Veiligheid Defensie: kwaliteit, Capaciteit en Samenwerking, 's-Gravenhage 2006, 73, 90, 202 en 221-222.

17 Zie bijvoorbeeld www.stichtingargus.nl, Verslag Directieberaad MIVD, 5 november 2003.

18 B. de Jong, 'Amerikaanse inlichtingendiensten en de Russische invasie', in: *Clingendael Spectator*, 6 april 2022; W.P. Strobel, 'Intelligence Sharing Marks New U.S. Front In Information War', *The Wall Street Journal*, 5 april 2022; '"A real stroke of genius": US leads efforts to publicize Ukraine intelligence. Release of Russia's military woes is latest twist in novel spying strategy', *Financial Times*, 6 april 2022; K. Adam, 'How U.K. intelligence came to tweet the lowdown on the war in Ukraine', *The Washington Post*, 23 april 2022.

De mysterieuze linguïst in Den Haag

Jaus Müller

Onlangs stond er op vacaturesites van de Rijksoverheid een advertentie met een wat cryptische kop: ‘Linguïst in Den Haag’. Uit de advertentietekst bleek dat het hier niet zomaar een doorsnee vertaalfunctie schaal 11 betrof: ‘Jij gaat aan de slag bij het bureau Contraspionage van de afdeling Contra-inlichtingen en Veiligheid en draagt bij aan de bescherming van Defensiebelangen tegen interne en externe bedreigingen op korte en langere termijn’. De Militaire Inlichtingen- en Veiligheidsdienst (MIVD), die deze advertentie plaatste, was niet zomaar op zoek naar aan allround-talenwonder: een hbo-vertaalopleiding of universitaire studie in de Chinese taal Mandarijn gold als expliciete functievereiste.

Dat de MIVD specifiek op zoek is naar Mandarijn-sprekende contra-inlichtingenexperts laat zien waar de inlichtingendienst onder meer op focust: het Verre Oosten. Hoewel de activiteiten van de dienst bijna altijd geheim blijven, is wel uit het openbare jaarverslag van de dienst af te leiden waar het vergrootglas op ligt: in het eerste hoofdstuk van het jaarverslag, dat in april 2022 werd gepubliceerd, passeren achtereenvolgens de Russische Federatie, China en Afghanistan de revue (Afghanistan krijgt inmiddels al heel wat minder tekst dan voorgaande jaren).[1]

Inlichtingencapaciteit is schaars. Iemand die te veel James Bond kijkt, denkt misschien dat inlichtingenofficieren vooral aan internationale cocktailbars hangen en tussen de wodka-martini’s geheimen opvangen. De realiteit is dat het echte inlichtingenwerk veel saaier is en bovendien schuilgaat achter een complex vraag- en aanbodmanagement. Inlichtingendiensten werken namelijk met klanten, ook wel ‘behoeftestellers’ genoemd. Bij de MIVD zijn dit onder meer de Bestuursstaf en de vier operationele commando’s (landmacht, marine, luchtmacht en de marechaussee), die continu om inlichtingen van de dienst zitten te springen. Al die belangen willen wel eens schuren. Sinds de inval in Oekraïne domineert bijvoorbeeld de vraag naar inlichtingen over Rusland, terwijl internationale veiligheidsexperts het erover eens zijn dat de langetermijnfocus misschien wel meer op China moet liggen.

Voor het mogelijke (politiek gestuurde) kortetermijndenken waarschuwde bijzonder hoogleraar Governance of Intelligence and Security Services aan de Universiteit Leiden Paul Abels in zijn afscheidsrede, afgelopen mei. ‘Behoeftestellers hebben een sterke neiging te vragen naar de bekende bedreigingen van gisteren, terwijl de werkelijkheid steeds weer hun voorstellingsvermogen overtreft’, aldus Abels. ‘In theorie wordt de diensten weliswaar ruimte gelaten voor de zogeheten ‘scantaak’ om ongekende dreigingen op het spoor te komen, maar de focus ligt bovenal op het bevredigen van de behoeftestellers en elke inzet op een ander nieuw terrein zal daaraan afbreuk doen. Bovendien zijn de diensten altijd overvraagd, wat onvermijdelijk ook ten koste zal gaan van de capaciteit en de scherpte op het vlak van het onderkennen van nieuwe dreigingen.’

Inlichtingenwerk is dus continu keuzes maken: de MIVD heeft bij wijze van spreken maar advertentiebudget voor één linguïst. Moet die nou

Russisch of toch maar Chinees spreken? Sinds de Russische inval in Oekraïne lijkt het gerechtvaardigd om alle reservecapaciteit van de inlichtingendienst op Rusland te zetten. Maar begin augustus startte het Chinese Volksbevrijdingsleger een omvangrijke oefening in de wateren rond Taiwan. Moeten we dan kijken naar het Oosten (Rusland) of het Verre Oosten (China)? Even snel wat personeel verplaatsen van de Rusland-afdeling naar de China-verdieping bij de MIVD dan maar? Zo werkt het niet in de inlichtingenwereld. Personeel opleiden kost tijd (Mandarijn leer je niet op een achternamiddag) en netwerken, kennis en vertrouwen opbouwen duurt ook nog eens jaren.

Nou kun je ook denken: waarom moeten we daar nou allemaal tijd en geld aan besteden? Waarom kan Nederland niet vertrouwen op bijvoorbeeld Amerikaanse inlichtingen als het gaat om Taiwan? In theorie zou het kunnen, maar de geschiedenis leert ons dat zelfs de VS soms de kwalijke neiging heeft niet altijd de waarheid te spreken. Neem het moment waarop Colin Powell (die overigens ook maar naar voren werd geschoven door president Bush om dit leugenachtige klusje op te knappen) in 2003 in de VN-Veiligheidsraad de wereld met een stalen gezicht voorloog dat een of ander buisje zandbakzand eigenlijk Iraaks antrax was. Dat gold als grondslag waarom ook Nederland politieke en/of militaire steun zou moeten verlenen aan een invasie van Irak. De MIVD (en in mindere mate de AIVD) trokken claims over mogelijke Iraakse massavernietigingswapens stelselmatig in twijfel. In een reactie op Powells presentatie schreef de MIVD bijvoorbeeld in 2003 in een interne notitie: 'De smoking gun is nog niet gevonden!'[2]

Had het kabinet-Balkenende I wat meer naar de genuanceerde inlichtingenofficieren geluisterd en minder naar de praatjes van Powell, dan had Nederland geen politieke steun hoeven te verlenen aan de internationaalrechtelijk illegale invasie van 2003. Achteraf gezien sloegen de kritische analyses van de MIVD namelijk de spijker op de kop: de wapens van de toenmalige Iraakse leider Saddam zijn immers nooit aangetroffen. Op belangrijke punten weken de

Moet die taalkundige Chinees, of misschien toch Russisch spreken?

Nederlandse inlichtingenrapportages destijds af van de Britse en Amerikaanse berichten, schreef de onderzoekscommissie-Davids in 2010: 'Deze andere conclusies leken niet zozeer gebaseerd op andere (eigen) inlichtingenbronnen, als wel op een eigen militair-technische analyse van de aangedragen informatie'. Zie hier het belang van goed geïnformeerde, goed opgeleide inlichtingenanalisten, die eigenstandig informatie bestudeerden en op grond daarvan een reeks ontnuchterende analyses maakten. De zowat oorlogsdronken ministers in het kabinet-Balkenende legden die adviezen helaas naast zich neer.

Al met al dus best handig, die ter zake kundige inlichtingenanalisten. Zeker als straks een of andere Amerikaanse functionaris iets roept over een al dan niet onafwendbare dreiging van de Chinese strijdkrachten. Dan is het toch prettig om te weten dat de MIVD in elk geval bijtijds die Chinese linguïst in Den Haag heeft aangetrokken om zélf te kunnen beoordelen wat ervan klopt. Dan maar hopen dat toekomstige ministers – anders dan in 2003 met Irak – wél naar de MIVD willen luisteren. ■

1 Zie: Militaire Inlichtingen- en Veiligheidsdienst, *Openbaar Jaarverslag 2021* (Den Haag, 28 april 2022).
2 Geciteerd in *Rapport commissie-Davids 2010* (Den Haag, 2010) 307.

‘Betaalde agenten (minste soort)’, ‘toneelspel’ en volkskarakter

‘De Inlichtingendienst is niet alleen voor de afdeeling operatiën, doch ook voor de beoordeling van den militair politieken toestand reeds in vredestijd een onmisbaar verkennings-orgaan van den Generalen Staf. Geen bevel-hebber zal nalaten, alvorens bevelen te geven, eerst te onderzoeken, wat er van den vijand bekend is.’[1] Zo vatte toenmalig ritmeester H.A.C. Fabius in 1921 in de *Militaire Spectator* het

De Nederlandse luitenant-kolonel Th.F.J. Muller Massis (voorste rij links) bezoekt met militaire attachés van andere neutrale landen het industriecomplex Gutehoffnungshütte in Oberhausen tijdens WO1

FOTO BEELDBANK NIMH

Het is de taak van het inlichtingenwerk, 'gegevens over de potentiële vijand te verzamelen, waar en hoe dan ook!'

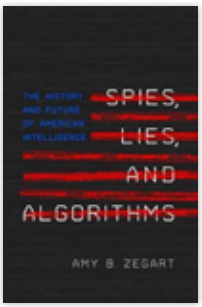
bestaansrecht samen van de militaire inlichtingendienst, waarvan hij als feitelijke grondlegger geldt.
Zelf droeg Fabius ijverig bij aan het in kaart brengen van de militair-politieke situatie in andere landen en publiceerde daar vanaf 1914 overzichten van in de *Militaire Spectator*. In 1913 aan het hoofd gekomen van het Studiebureau Vreemde Legers overzag hij de transformatie tot sectie GSIII een jaar later.

In zijn artikel uit 1921 keek Fabius terug op de invloed die WO1, c.q. de Nederlandse neutraliteitspolitiek, en het daaropvolgende revolutiegevaar in Europa hadden gehad op het inlichtingendomein. Hij constateerde dat de departementen van Oorlog, Marine, Koloniën, Buitenlandse Zaken en Justitie daarin alle belangen hadden, maar achtte voor de beoordeling van berichten 'eene streng doorgevoerde centralisatie noodzakelijk'. In zijn stuk ging Fabius ook in op de manieren waarop inlichtingen werden verkregen. Zo behoorden tot de leveranciers ook de militaire attachés, die 'niets geheimzinnigs' deden, maar zich uitsluitend bezighielden met de 'studie van de legerinrichting' in het land van plaatsing. Met agenten, 'die toch evengoed onder valsch mom hem direct of indirect kunnen bespieden', zou de attaché zich niet inlaten.

In het geval van een langer durende oorlog was volgens Fabius waakzaamheid geboden tegen valse propagandaberichten met politieke bedoelingen. Die konden afkomstig zijn van 'bewuste en onbewuste agenten'. Tot de eerste categorie rekende hij 'betaalde agenten (minste soort)', tot de tweede groep behoorden mensen die uit 'overdreven sympathiegevoelens onbewuste werktuigen' waren van de tegenpartij. In WO1 waren in Nederland agenten actief geweest die 'via onzijdig gebied' inlichtingen wilden inwinnen over hun vijand, of over het neutrale Nederland zelf, en die laatsten noemde Fabius 'verspieders in den zin van het Wetboek van Strafrecht' tegen wie daadwerkelijk opgetreden moest worden.

Luitenant-kolonel A. Wolting haalde in de *Militaire Spectator* een interview aan waarin gezegd werd dat Nederlandse officieren zich ook in de aanloop naar WO2 'te goed voelden voor spionage', omdat het 'toneelspel' niet bij het Nederlandse volkskarakter zou passen. Maar het is uiteindelijk de taak van het inlichtingenwerk, 'gegevens over de potentiële vijand te verzamelen, waar en hoe dan ook!', schreef Wolting.[2] ■

1 H.A.C. Fabius, 'De Inlichtingendienst bij den Generalen Staf', *Militaire Spectator* 90 (1921) 397-408.
2 A. Wolting, 'De eerste jaren van de Militaire Inlichtingendienst (GSIII, 1914-1917)', *Militaire Spectator* 134 (1965) 566-571.



Spies, Lies, and Algorithms

The History of American Intelligence
Door Amy B. Zegart
Princeton (Princeton University Press) 2022
424 blz.
ISBN 9780691147130
€ 30,-

Er is geen tekort aan *spytainment* oftewel entertainment over spionage. Van boeken tot films en series: onder meer Homeland, CSI, 24, en personages zoals Jason Bourne, Jack Ryan en natuurlijk James Bond. Maar, zo stelt Amy Zegart, terwijl spytainment overal is, zijn *spy facts* schaars. De maatschappelijke kennis over het waarom en hoe van inlichtingendiensten is zeer beperkt, niet in de eerste plaats omdat deze diensten zelf van nature geheim dan wel geheimzinnig zijn. Ook in de wetenschap, met name in internationale betrekkingen en in de bredere politieke wetenschappen, is er relatief weinig aandacht voor inlichtingenwerk. In haar tweede hoofdstuk legt Zegart, die verbonden is aan Stanford University, scherp uit waarom zo'n gebrek aan maatschappelijke kennis over inlichtingen problematisch is. Als de enige bron spytainment is, dan krijgt het publiek een vertekend beeld van de inlichtingenwereld. Haar eigen enquêtes tonen aan dat fans van spytainment meer macht en capaciteiten toeschrijven aan inlichtingendiensten dan ze daadwerkelijk bezitten, vaker voorstander zijn van het martelen van terreurverdachten en inschatten dat er minder toezicht is dan in werkelijkheid. Dit kan complottheoriën voeden, debatten over surveillance bemoeilijken en misvattingen over martelen verspreiden. Dit laatste is immers zowel onethisch als ineffectief.

Het gebrek aan kennis werkt door op politiek-bestuurlijk niveau, waarbij Zegart stelt dat er meer Congresleden zijn met kennis van melkpoeder dan kennis van inlichtingendiensten. De decaan van West Point, brigade-generaal Patrick Finnegan, werd ooit zo bezorgd dat de serie 24 het martelen van terreurverdachten verheerlijkte bij de cadetten, dat hij langs de filmset ging om te vragen of ze ook een aflevering konden maken waar martelen averechts werkt. Toen hij in uniform op de set met dit verzoek verscheen, dacht men dat hij een acteur was.

18 inlichtingendiensten

De misvattingen over inlichtingen vormen de opmaat voor Zegarts boek *Spies, Lies, and Algorithms*, een ambitieus werk om een gedegen achtergrond over inlichtingen en spionage aan te bieden. Als politiek wetenschapper doet Zegart al dertig jaar onderzoek naar Amerikaanse inlichtingendiensten. Ze schreef eerder het boek *Spying Blind. The CIA, the FBI, and the Origins of 9/11*. Zoals ze zelf aangeeft is ze geen bewoner van de inlichtingenwereld (ze heeft nooit voor een dienst gewerkt), maar een bezoeker. Als buitenstaander – die naast literatuuronderzoek veel heeft gesproken met werknemers van inlichtingendiensten – heeft ze een frisse blik op deze nogal gesloten wereld. Enerzijds heeft ze begrip voor de uitdaging waarvoor diensten staan en de hoge verwachtingen waaraan ze moeten voldoen. Zo moeten inlichtingendiensten hoogwaardige inlichtingen generen, tijdig anticiperen op internationale ontwikkelingen en gebeurtenissen (liefst voorspellen), en dit alles zonder inbreuk te maken op de privacy van anderen. Dit noemde James Clapper, destijds de directeur van de Amerikaanse inlichtingengemeenschap (DNI) ooit het probleem van 'immaculate collection'. Aan de andere kant neemt Zegart geen blad voor de mond als het gaat om het falen van de diensten; zowel analytische missers als organisatorische misstanden. Haar boek is doelbewust breed van opzet – de subtitel luidt 'het verleden en de toekomst van Amerikaanse inlichtingen'. Dit betreft een enorm onderzoeksveld. De VS telt inmiddels 18 inlichtingendiensten (maar een organisatie telt pas mee als die een drieletterafkorting heeft), meer dan 100.000 werknemers, zo'n 4 miljoen 'afnemers' die een veiligheidsclearance bezitten, en dat alles voor een prijskaartje van 85 miljard dollar per jaar. Kortom, meer dan het bnp van een aanzienlijk aantal landen.

Valkuilen in het denkproces

De kern van het boek wordt gevormd door vier hoofstukken: een historische achtergrond van Amerikaanse inlichtingen; de beginselen van het inlichtingenwerk (*knowns and unknowns*), waarom analyse zo moeilijk is, en *covert action*. Alle hoofdstukken zijn voorzien van tabelletjes en tekstblokjes die bepaalde casuïstiek uitwerken. De historische context is origineel omdat Zegart teruggrijpt naar de Amerikaanse Onafhankelijkheidsoorlog, waarin George Washington mede

door spionage, list en bedrog toch de overhand kreeg over de Engelsen, die immers bekend staan als meesters van het genre. Ook worden enkele voorbeelden uit de Koreaanse Oorlog mooi beschreven. Zo was generaal Douglas MacArthur overtuigd dat indien China betrokken zou raken bij de oorlog, zijn soldaten geen enkele kans hadden tegen de goed getrainde Amerikaanse militairen. Het liep anders. Het doet denken aan de verwachting van de Russische president Poetin begin 2022 dat hij Oekraïne er binnen enkele dagen onder zou krijgen. Dit conflict wordt overigens niet in het boek beschreven; toen lag het al bij de drukker. Het hoofdstuk over analyse is eveneens zeer de moeite waard en beschrijft verschillende valkuilen in het denkproces (zoals *cognitive biases*). Elk hoofdstuk is voorzien van goed beschreven *case studies*. Van de FBI-mol Robert Hanssen, tot de niet-bestaande massavernietigingswapens van Saddam en de jacht op Osama bin Laden; Zegart beschrijft het allemaal in prachtig detail.

Digitale thema's

Een klein punt van kritiek is de nogal magere behandeling van het onderwerp cyber. Ook het woord *algorithm* in de titel komt er in het boek maar bekaaid vanaf. Dit is wellicht onvermijdelijk gezien de brede focus van het werk. Het hoofdstuk over Open Source Intelligence richt zich vooral op nucleaire proliferatie, maar had net zo goed meer aandacht kunnen besteden aan Bellingcat en algoritmes, die zo effectief zijn gebleken in het ontmaskeren van Russische inlichtingenofficieren. Het laatste hoofdstuk gaat met een sneltreinvaart door de thema's van online desinformatie en offensieve en defensieve cyberoperaties. Dit had een extra hoofdstukje verdiend, met wat meer conceptueel onderscheid tussen de ingewikkelde digitale thema's. Dit neemt niet weg dat het nieuwste werk van Zegart zeker een plek verdient in de boekenkast. Voor diegenen die enigszins ingevoerd zijn in inlichtingenstudies biedt het werk een frisse en brede blik, waarbij vooral het hoofdstuk over maatschappelijke kennis en perceptie en het hoofdstuk over het Amerikaanse toezichtstelsel nieuwe data en inzichten toevoegen aan de bestaande literatuur. Daarnaast is het boek een goudmijn aan bronverwijzingen. De tekst neemt ongeveer 275 pagina's in beslag, maar bovendien levert Zegart nog zo'n honderd pagina's aan eindnoten en een korte bibliografie. Toch heeft het boek het meeste te bieden aan mensen die geïnteresseerd zijn in inlichtingen, maar eigenlijk nog geen overzicht of grip hebben op het veld. Kortom, wie het onderscheid tussen een *case officer* (of operateur) en een bron of een agent niet kent, wordt geadviseerd om snel dit boek aan te schaffen. Ongetwijfeld zal *Spies, Lies, and Algorithms* ook de fans van spytainment aanspreken, want al is het vanuit een wetenschappelijke invalshoek geschreven, de mooie anekdotes, goed beschreven verhalen en vlotte schrijfstijl maken het boek bijzonder *entertaining*. ■

Mr. dr. Sergei Boeke, Politiek Adviseur JSEC

Hackers

Over de vrijheidsstrijders van het internet
Door Gerard Janssen
Amsterdam (Thomas Rap) 2022
304 blz.
ISBN 9789400408371
€ 22,99

Hackers worden vaak stereotiep afgebeeld: hoodies, een schemerige ruimte, een beeldscherm met onbegrijpelijke regels computertaal. Gerard Janssen, schrijver en journalist, verdiepte zich de afgelopen jaren in deze mysterieuze wereld waarmee hij, net als waarschijnlijk de meeste lezers, onbekend was. Het boek *Hackers* is de neerslag van zijn zoektocht.

Inbreken in een computer(systeem) wordt hacken genoemd. Hacken gebeurt vaak met kwade bedoelingen, maar kan ook gebeuren om een systeem op veiligheid te testen. Janssens boek gaat over wie deze hackers eigenlijk zijn. Het is geen analyse hoe hacken technisch in zijn werk gaat, wat daarvan de impact is of hoe ertegen op te treden. Janssen schrijft daar overigens wel over, maar dan bedoeld om uit te leggen hoe een hacker denkt en functioneert. Janssens zoektocht start vanuit journalistieke noodzaak: hij moet feiten hebben en deugdelijke bronnen. Maar, zo geeft hij zelf toe, het is ook een wereld die hem fascineert: een Marvel Comics-wereld met daarin personen met 'online superkrachten'. Voor aanknopingspunten hoeft hij niet ver weg, want Nederland blijkt zowel over een capabele hackersgemeen-

schap te beschikken als veel IT-kennis en ervaring om tegen de uitwassen van hacken te beschermen. Het is bijvoorbeeld een Nederlander geweest die de slechte beveiliging van toenmalig president Trumps twitter-account aan het Witte Huis doorgaf en we kennen Fox-IT, dat in de media toelichting komt geven wanneer weer eens een grote hack heeft plaats gevonden.

Bewakers en kwaadwillenden

Hacken begon goed bedoeld met nieuwsgierige studenten die al in de jaren vijftig van de vorige eeuw hun computers onderling spelletjes lieten spelen en die berichten op elkaars beeldschermen toverden. Om dit te kunnen, moesten zij het functioneren van het digitale gangenstelsel van de computer, het besturingsprogramma en toepassingssoftware doorgronden. En, decennia later, hoe de communicatie via internet verloopt. Het idee was hiermee mensen en techniek verder te helpen, bijvoorbeeld door kwetsbaarheden op te sporen die een risico vormen voor veilig gebruik van internet en al wat daarmee verbonden is of ervan afhankelijk. Deze hackers, zoals ze dan inmiddels worden genoemd, zien zichzelf als de bewakers van het vrije internet, voor hen het 'laatste grote bolwerk van vrijheid van denken, ideeën en meningsuiting'. Want, stelden zij vast, overheden en grote bedrijven willen controle houden en '(verkiezen) functionaliteit altijd boven veiligheid (van de gebruiker)'.

Al snel ontstond ook een groep hackers die haar kennis gebruikte om informatie te stelen en te misbruiken om daar zelf van te profiteren. Hen is de cultuur van het ethische hacken, waarmee het verschil tussen de goed- en de kwaadwillenden wordt aangegeven, volkomen vreemd. Zij zijn de weg ingeslagen van het verspreiden van kwaadaardige virussen, technieken om phishing toe te passen, DDOS-aanvallen te lanceren, et cetera. Dit is de criminele kant van het hacken, zo beschrijft de auteur, die vooral in Rusland welig tiert. Het is dan ook zeker op zijn plaats dat Janssen het OM citeert over het strafbare karakter van hacken. Daarnaast noemt hij het bestaan van hackers met (politiek) activistische doelstellingen.

Voor zijn zoektocht dringt Janssen gaandeweg steeds verder door in de hackerswereld. Er volgen beschrijvingen van allerlei bijzondere ontmoetingen, vaak op plaatsen waar hackers zich het veiligst en prettigst voelen: hun *hackerspaces*, of tijdens grote hackersbijeenkomsten in binnen- en buitenland. De hackerswereld is echt niet alleen 'ondergronds' te vinden. Wanneer hij hun vertrouwen weet te winnen, geven de hackers, hoewel mondjesmaat, Janssen informatie over waartoe zij in staat zijn: hoe zij IT-systemen van overheden, bedrijven en organisaties weten binnen te dringen, wat zij aan informatie aantreffen en wat zij daarmee zouden kunnen. Maar ook, hoe laks of zelfs vijandig vervolgens gereageerd wordt wanneer een dergelijk veiligheidslek wordt gemeld. Janssen hoedt zich er overigens wel voor zelf niet in de criminele delen van deze wereld verzeild te raken. Wat hij hiervan te weten komt en vertelt, hoort hij uit de tweede hand van hackers en beveiligingsexperts.

Persoonlijke kenmerken en eigenschappen

De gesprekken en ontmoetingen leveren Janssen tevens de informatie om meer over de hackers zelf te kunnen vertellen. Janssen besteedt ruim aandacht aan persoonlijke kenmerken en eigenschappen van zijn gesprekspartners. Het is een ontnuchterend verhaal over wat als onschuldige uitdaging begint – die er nu eenmaal bijhoort als je jong bent en veel van computers weet – en vaak blijkt te leiden tot een afgezonderd en wantrouwend bestaan. Het is een gesloten wereld. De buitenwereld vertrouwt hen niet, zij vertrouwen de buitenwereld niet. Complotdenken is hackers niet vreemd. Sommigen zijn soms letterlijk voortdurend op de vlucht. Het hackermilieu blijft mysterieus, met eigen rituelen en omgangsvormen. Het *nerdy*-imago, dat hackers zelf met plezier lijken te bevestigen, blijft evenmin onbesproken. Janssen doet zijn best daar positieve eigenschappen naast te plaatsen, zoals de onderlinge tolerantie, het idealisme en de bereidheid elkaar te willen helpen en – op persoonlijk niveau – hun doorzettingsvermogen en inventiviteit; ze zijn volgens hem intelligent en kritisch. Die positieve eigenschappen en het feit dat veel hackers in het dagelijks leven gewone en verantwoordelijke banen blijken te hebben, vaak juist in de IT-wereld, laat het over het algemeen negatieve beeld dat van hackers bestaat, in dit boek echter niet kantelen.

Voor het schrijven van zijn boek is Janssen sterk afhankelijk geweest van de bereidwilligheid van hackers om kennis en informatie met hem te delen. Een paradoxale situatie: de schrijver die transparantie wil en de gesprekspartners die liever in het verborgene blijven. Deze spanning is merkbaar bij het lezen van dit boek. Niet alles wordt gezegd en ook niet alles is opgeschreven, geeft Janssen toe.

Janssen heeft een onderhoudend boek geschreven dat niet snel verveelt. De

sfeer van de hackerswereld lijkt hij goed te vangen, onder meer door het kleurrijke hackersjargon te gebruiken. Om die exotische begrippen te kunnen plaatsen heeft de auteur, heel nuttig, een uitgebreide verklarende woordenlijst opgenomen. Voor de leek die meer over hackers wil weten dan alleen de gebruikelijke stereotyperingen en wil weten hoe breed hacken wordt toegepast, is dit boek zeker de moeite waard. ■

LtKol b.d. drs. Jan-Leendert Voetelink

Wij zijn Bellingcat

Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden
Door Eliot Higgins
Amsterdam (Spectrum) 2022
272 blz.
ISBN 9789000369669
€ 23,99

In 1979 schrijft de Italiaanse historicus Carlo Ginzburg een artikel over een nieuwe vorm van wetenschappelijk denken aan het einde van de negentiende eeuw.[1] Daarin bespreekt hij een serie artikelen uit 1874-1876 van de Italiaanse kunsthistoricus Giovanni Morelli. Morelli attaqueerde hierin de toenmalige praktijk van het attribueren van schilderijen. De Europese musea zouden volhangen met schilderijen die aan de verkeerde kunstenaars waren toegeschreven. De zogenaamde kunstkenners gingen volgens Morelli verkeerd te werk. Ze richtten zich namelijk op de meest in het oog springende aspecten van schilderijen, zoals de glimlach die Leonardo da Vinci zijn geportretteerden vaak gaf. Elementen die gemakkelijk waren te vervalsen, stelde Morelli, niet in de laatste plaats omdat juist die kunststukjes in bepaalde scholen gedoceerd werden.

Om die reden was het juist zaak om de 'meest verwaarloosbare details' te bestuderen: oorlellen, nagels en de vorm van vingers en tenen.[2] Niet geheel toevallig, betoogt Ginzburg, zien we dezelfde vorm van aandacht voor het detail terug in de boeken van Arthur Conan Doyle over Sherlock Holmes. Ook Holmes richt zich uitdrukkelijk op de kleinste details, die iedereen over het hoofd ziet en lost zo de meest complexe misdrijven op. Ginzburg ziet hierin een nieuw wetenschappelijk paradigma: het sporenparadigma (*paradigm of the trace*) met oog voor wat zich op de achtergrond en niet op de voorgrond bevindt. Je zult je op het 'oneindig kleine' moeten richten, aldus Ginzburg: alleen het marginale, de details – de vingernagel of weggeworpen lucifer – stelt de oplettende observator in staat om door te dringen tot een diepere werkelijkheid.[3]

Bellingcat

Eliot Higgins, de oprichter van het *open source*-platform Bellingcat, lijkt wel wat op Morelli. In zijn (wat moeizaam) vertaalde boek *Wij zijn Bellingcat. Hoe gewone mensen de onderzoeksjournalisten van de toekomst werden* schetst Higgins een ontstaansgeschiedenis van dit collectief van digitale burgerspeurders en journalisten. Net als Morelli – die zijn methode beproefde en een aantal spraakmakende schilderijen aan andere kunstenaars wist toe te schrijven – is Higgins er veel aan gelegen om te laten zien wat nauwgezet online onderzoek kan opleveren. En niet zonder reden: Bellingcat heeft inmiddels een indrukwekkend portfolio – en als portfolio kan dit boek ook het beste worden gelezen. Het bestaat in hoofdzaak uit samenvattingen van het verloop en de resultaten van Bellingcats digitale speurwerk tijdens de Arabische Lente, de Syrische Burgeroorlog, het MH17-onderzoek, extreemrechts geweld in de Verenigde Staten, executies van Islamitische Staat, geweldsmisdrijven in Libië en de moord op Sergej Skripal.
De rode draad – en kerngedachte van Bellingcat – in deze onderzoeken is dat de waarheid schuilt in de details. Ginzburg had zich geen mooiere pendant van het sporenparadigma kunnen wensen, al stelt Bellingcat *digitale* sporen centraal. Tijdens de Arabische Lente in 2011 merkte Higgins op dat menig journalist beeldmateriaal van dubieuze oorsprong (meestal betrokken partijen) gebruikte. Veel foto's en video's die als bewijs dienden, werden daardoor verkeerd geduid. Hij stelde zich ten doel om foto- en videomateriaal dat via sociale media of anderszins de wereld in werd geslingerd te dateren

1 Carlo Ginzburg, 'Clues. Roots of a Scientific Paradigm', *Theory and* Society 7 (1979) (3) 273-288.
2 Ginzburg, 'Clues', 273-274.
3 Ginzburg, 'Clues', 280.

en *geolokaliseren*. Het MH17-onderzoek en de moord op Skripal zijn daarvan misschien wel de spectaculairste voorbeelden.

Of Bellingcat daarmee fungeert als een 'geheime dienst voor gewone mensen' (blz. 20)? Het staat buiten kijf dat Bellingcat bewonderenswaardig én relevant onderzoek verricht. Het opsporen en verifiëren van online materiaal ten behoeve van waarheidsvinding vergt systematisch, minutieus en tijdrovend werk waar veel van valt te leren. Zeker wat betreft attributievraagstukken – digitaal of anderszins – wat tot het werkterrein van inlichtingen- en veiligheidsdiensten behoort. Maar de doelstellingen, activiteiten en omgang met gegevens die deze diensten al dan niet in openbare bronnen verwerven, zijn breder en verschillen van Bellingcat, zodanig dat de karakterisering 'geheime dienst' de plank misslaat. Inlichtingen- en veiligheidsdiensten in een democratie staan ten dienste van de veiligheid van staat en samenleving. Onafhankelijkheid, objectiviteit en *speaking truth to power* is het veelgehoorde adagium. Toch staat hun werk niet buiten het politieke domein. Bij een politiek besluit tot een militaire missie of het bestrijden van jihadistisch terrorisme, ontkomen militaire en civiele diensten er niet aan daarover regelmatig te rapporteren. Diensten kunnen professionele distantie houden, maar staan niet los van de politiek. Daarentegen stelt Higgins niets te maken te hebben met 'politieke agenda's' (blz. 34). Al zou je de onderwerpkeuze van Bellingcat ook als een politieke handeling kunnen zien: waarom kijken naar het afluisterschandaal van Rupert Murdoch? En alleen al het feit dat Bellingcat samenwerkt met politiediensten betekent stellingname tegen bijvoorbeeld de Russische en Syrische staat. En ook de 'oorlogsverklaring' aan de 'contrafeitelijke gemeenschap' is natuurlijk niet apolitiek.

Een tweede belangrijk element van Bellingcats identiteit betreft de distantie tot het onderwerp. Op verschillende plekken in het boek benadrukt Higgins dat het ontbreken van taal- en cultuurkennis Bellingcat juist in staat stelt naar de details te kijken. Voor inlichtingen- en veiligheidsdiensten is de Bellingcat-methode van het digitaal uitpluizen weliswaar van belang, maar zonder militaire experts, linguïsten, historici, of technisch specialisten kan enkel vastgesteld worden waar en wanneer een foto of video is gemaakt. De betekenis van wat te zien is, gezegd of gedaan wordt, vergt actieve interpretatie op basis van relevante – en dus met de context verbonden – kennis en kunde.

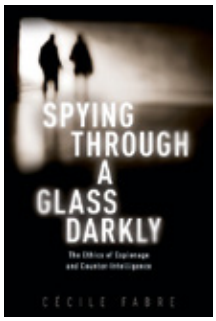
Hiermee stuiten we op een laatste verschil. Naast attributiewerkzaamheden naar gebeurtenissen die in het verleden liggen – hetzij om daders aan te wijzen, hetzij om er lering uit te trekken – zijn geheime diensten er voor *early* en *strategic warning*. Zij dienen te waarschuwen voor nationale veiligheidsrisico's om andere spelers in staat te stellen maatregelen te treffen. Dat veronderstelt dat zij uitspraken doen over mogelijke, toekomstige handelingen van staten, groepen en individuen. Daarbij volstaat het niet om transparant te zijn, zoals Bellingcat; de feiten spreken immers niet voor zich zoals voor de digitale forensische opsporing waarmee Bellingcat zich welbeschouwd bezighoudt. De context waarin uitspraken en handelingen begrepen moeten worden speelt juist een grote rol in de interpretatie van een dreiging.

Geheime dienst of Sherlock Holmes?

Higgins kan in zijn enthousiasme over het online onderzoek van Bellingcat worden aangewreven wat critici Morelli anderhalve eeuw geleden verweten: positivisme – voor het gemak begrepen als het onwankelbare geloof in het onweerlegbare bestaan van (waarnemings)feiten. Volgens Ginzburg is dit fundamenteel voor het sporenparadigma, dat vraagt om aandacht voor het oneindig kleine en marginale. Daarin schuilen immers de feiten die toegang verschaffen tot een dieperliggende waarheid. Higgins gelooft welbeschouwd hetzelfde. De feiten liggen voor het oprapen in het openbare domein; enkel verscholen in de details, zoals de metadata van een bestand, een minaret op de achtergrond, of een vage rookpluim die één seconde in beeld is. Dat maakt Bellingcat echter nog geen geheime dienst voor gewone mensen, eerder een publieke Sherlock Holmes – een detective die in het kader van daderonderzoek aan waarheidsvinding doet. Dat doet niets af aan het belang van dit openbronnenspeurwerk. Een onafhankelijke organisatie, die feitelijk checkt en daar grondig en innovatief in optreedt, is een belangrijke bondgenoot voor gewone burgers, zeker in een tijd van *information overload* en desinformatie. ■

Dr. C.W. Hijzen, onderzoeksfellow aan het Institute of Security and Global Affairs van de Universiteit Leiden
Dr. A. Claver, ministerie van Defensie

SIGNALERINGEN



Spying Through a Glass Darkly

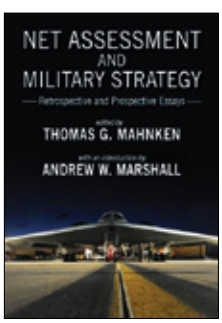
The Ethics of Espionage and Counter Intelligence
Door Cecile Fabre
Oxford (Oxford University Press) 2022
272 blz.
ISBN 9780198833765
€ 36,-

In *Spying Through a Glass Darkly* behandelt Cecile Fabre, hoogleraar politieke wetenschappen aan de University of Oxford, de ethische kant van spionage en *counter intelligence*. De auteur stelt onder meer aan de orde of het medewerkers van veiligheidsdiensten moreel toegestaan is te bedriegen, mensen om te kopen of af te persen of te manipuleren om staatsgeheimen te achterhalen. En is het moreel verantwoord dat staten hun eigen bevolking massaal monitoren? Volgens Fabre zijn dergelijke operaties in de context van oorlog of buitenlandse politiek uiteindelijk alleen gerechtvaardigd als middel – meer ook niet – voor het beschermen van de eigen veiligheid en die van bondgenoten.

Ongekend en onderscheidend

De geheime geschiedenis van de MIVD
Door Bob de Graaff
Amsterdam (Uitgeverij Boom) 2022
448 blz.
ISBN 9789024444649
€ 34,90

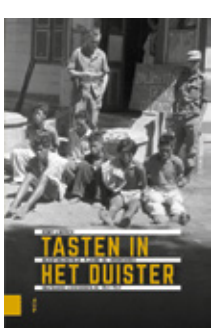
Bob de Graaff beschrijft in *Ongekend en onderscheidend* de geschiedenis van de MIVD en zijn voorgangers en hoe die sinds 1912 internationaal opereerden, zoals in de neutraliteitsperiode voor WO2, de Koude Oorlog en de strijd tegen het terrorisme in de 21e eeuw. De inlichtingendiensten van landmacht, luchtmacht en marine werden eind jaren tachtig gedwongen in één dienst te gaan samenwerken. Na een stroeve start professionaliseerde de dienst in hoog tempo en verwierf aanzien, ook bij buitenlandse partnerdiensten. De Graaff beschrijft deze ontwikkelingen aan de hand van casussen zoals het tegengaan van Russische spionage in Nederland en de inlichtingenondersteuning ten behoeve van de Nederlandse troepen in Afghanistan.



Net assessment and military strategy

Retrospective and prospective essays
Door Thomas G. Mahnken en Andrew W. Marshall (red.)
Amherst (Cambria Press) 2020
272 blz.
ISBN 9781621965398
€ 40,-

In de bundel *Net assessment and military strategy* leggen deskundigen uit hoe bij een *net assessment* een multidisciplinaire benadering wordt toegepast om de sterke en zwakke punten op militair gebied van een concurrent of tegenstander in kaart te brengen. Tijdens de Koude Oorlog gaven dergelijke analyses hoge beleidsmakers kritische inzichten in de relatieve militaire slagkracht van de VS ten opzichte van de Sovjet-Unie over een bepaalde periode. In de bundel wordt echter niet alleen teruggekeken, maar komt ook de toekomst van net assessment aan bod, met als belangrijkste onderwerpen de wedijver met China, de strijd tegen de radicale islam en – als erfenis van de Sovjet-Unie – Rusland.



Tasten in het duister

Inlichtingenstrijd tijdens de Indonesische onafhankelijkheidsoorlog 1945-1949
Door Rémy Limpach
Amsterdam (Amsterdam University Press) 2023
272 blz.
ISBN 9789463727082
€ 24,99

In hun jacht op militaire successen voerden Nederland en Indonesië tijdens de Indonesische onafhankelijkheidsoorlog van 1945-1949 een grimmige inlichtingenstrijd. Daarbij gebruikten zij spionage, infiltratie en andere – veelal extreem gewelddadige – middelen, onder meer bij het verhoren van gevangenen, concludeert Rémy Limpach in *Tasten in het duister*. De auteur legt het zwaartepunt bij het optreden van de Nederlandse troepeninlichtingendiensten. Hij beschrijft onder meer hoe de Nederlanders en de Indonesiërs een wijdvertakt alarmsysteem opzetten, dat de eigen eenheden vroegtijdig voor aanvallen moest waarschuwen. Limpachs publicatie is onderdeel van de serie *Onafhankelijkheid, Dekolonisatie, Geweld en Oorlog in Indonesië 1945-1950*.