Jaargang 193 nummer 9 - 2024

MILITAIRE SPECTATOR

DE DIGITALE STRIJD ROND HET GAZACONFLICT

- Gastcolumn secretaris-generaal Defensie
- Interview met generaal-majoor Denny Traas
- De theorie van Biddle en de oorlog in Oekraïne
- Straffen of leren?
- Interview met Rémy Limpach

FOTO MCD, CINTHIA NIJSSEN

In *Militaire Spectator* 10-2024 verschijnt onder meer: 'Onbemande systemen: kansen en uitdagingen voor de Nederlandse krijgsmacht' van Jeroen Vleij, Mark Levels en Jean-Pierre Schouwenaars.

De verwachting is dat de wereldwijde markt voor militaire drones – voor gebruik op zee, op land en in de lucht – in 2030 een waarde van zo'n 36 miljard dollar zal hebben. Onbemande systemen worden inmiddels door de krijgsmachten van meer dan honderd landen gebruikt. Ten minste tien landen hebben daadwerkelijk militaire drones ingezet om aanvallen uit te voeren en nog eens dertig landen bereiden zich voor op het gebruik van drones als aanvalswapen, zo blijkt uit diverse bronnen.

De oorlog in Oekraïne toont het effect van *unmanned combat vehicles* bij operaties. Zowel de Oekraïense als de Russische krijgsmacht zet drones in om (fragmentatie)munitie te droppen, de effectiviteit van artilleriebeschietingen waar te nemen, verkenningen uit te voeren of voor aanvallen in de diepte.

Onderzoek onder meerdere onderdelen van de Nederlandse landmacht die pionieren met autonome systemen laat zien dat de voor innovatie benodigde mindset zich soms lastig verhoudt tot de dagelijkse realiteit van de militair in het veld. Maar er zijn meer randvoorwaarden dan mindset alleen. Welke uitdagingen en kansen liggen hier voor de Nederlandse krijgsmacht? ■

Weg met die regelknechterij!

Op donderdag 5 september boden minister Ruben Brekelmans en staatssecretaris Gijs Tuinman de *Defensienota 2024* aan met het motto 'Sterk, Slim en Samen'. De nota schetst een somber beeld over toegenomen dreiging. Veiligheid is niet meer vanzelfsprekend en Nederland moet weerbaarder worden. Militaire weerbaarheid vereist volgens de nota 'uitbreiding van de gevechtskracht' en een 'schaalbare krijgsmacht'. Dat zijn mooie termen voor enerzijds investeren in meer en zwaardere middelen, zoals tanks, F-35's en fregatten, en anderzijds een krijgsmacht die groter wordt als een dreiging toeneemt en slinkt als die weer afneemt. Reservisten en de verdere ontwikkeling van het dienjaar spelen daarbij een belangrijke rol, aldus de nota.

De nota constateert ook dat de huidige wet- en regelgeving niet meer in overeenstemming is met het dreigingsbeeld. Werk aan de winkel voor Defensie! Naast het vervaardigen van nieuwe wetten die onder meer knelpunten in de gereedstelling voorafgaand aan conflicten wegnemen, stelt de nota zich ten doel de eigen regelgeving eenvoudiger en duidelijker te maken. Die eenvoud is een interessant voornemen, want daar schort het nogal aan bij Defensie. En dit vraagt om nadere uitleg.

Toen Maarten Schurink vorig jaar aantrad als secretaris-generaal bij het ministerie van Defensie viel hem op dat militairen vaak de term *mission command* (opdrachtgerichte commandovoering) gebruiken. Die term en de bijbehorende stijl van leidinggeven waren nog onbekend bij hem. Hij ging zich erin verdiepen en wil nu graag dat het hele ministerie, tot aan de bestuursraad aan toe, zich meer op mission command gaat richten. Schurink legt dit uit in zijn reactie op het vorige editoriaal, te lezen als gastcolumn in deze *Militaire Spectator*.
Hulde aan Schurink dat hij de uitdaging is aangegaan om op het vorige editoriaal te reageren. En dapper dat hij mission command ook opdraagt aan het kerndepartement, dat zeker niet de eenvoudigste plek is om volgens die principes te handelen. In deze beleidsarena draait het om het spel met de knikkers waarbij politieke wensen en gevoeligheden maar ook diverse, soms zelfs strijdige, krijgsmachtdeelbelangen vaak een hoofdrol spelen. In deze omgeving is niet van nature sprake van wederzijds vertrouwen, het cruciale element in mission command.

Het gaat Schurink vooral om de mensen zelf in de organisatie en niet de regels. Een hoopvolle constatering, want al die regels nemen vaak de plaats in van onderling vertrouwen en staan soepele samenwerking en mission command in de weg. Veel militairen ergeren zich vooral aan de ver doorgevoerde wet- en regelgeving in vredestijd, zoals Arbowetgeving, werk- en rusttijdenbesluit, waardoor er niet meer op realistische wijze voor hoofdtaak 1 kan worden geoefend. Deze 'overjuridificering', want zo mag je het wel noemen, leidt tot angst en bemoeizucht van bovenaf, want… o wee, als je de regels niet naleeft!

In 2021 pleitte George Dimitriu in de *Militaire Spectator* al voor een krijgsmacht die gebaseerd is op vertrouwen in plaats van één waarin regels en controle de boventoon voeren.[1] De nieuwe *Defensienota* biedt de mogelijkheid een goed fundament te leggen voor een krijgsmacht waarin ruimte is voor mission command en die oefeningen kan houden waarbij een oorlogssituatie beter kan worden nagebootst zonder verstikkende regels. Immers, je kunt nog zulke 'peppy' spulletjes hebben en over goed en voldoende personeel beschikken, maar als de aansturing vervolgens zeer krampachtig is… Tja, dan heb je nog steeds niets. Dus weg met die regelknechterij! ■

1 George Dimitriu, 'De moderne leider heeft buikpijn. Kiezen tussen angst en vertrouwen', *Militaire Spectator* 190 (2021) (7/8) 370-379.

KVBK
KONINKLIJKE VERENIGING TER BEOEFENING VAN DE KRIJGSWETENSCHAP

UITGAVE
Koninklijke Vereniging ter Beoefening van de Krijgswetenschap
www.kvbk.nl
E info@kvbk.nl
linkedin.com/company/kvbk/

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

De Militaire Spectator is aangesloten bij de European Military Press Association

LIDMAATSCHAP

Particulier lid	€ 30,-
Particulier lid buitenland + € 15,- verzendkosten	€ 30,-
Instellingen binnenland	€ 35,-
Instellingen buitenland + € 15,- verzendkosten	€ 35,-
Evenementenlid	€ 10,-

OPMAAK
Coco Bookmedia

DRUK
Wilco Meppel
ISSN 0026-3869

Coverfoto: Mascotte van een Trojaans 'cyberpaard' bij de Universiteit van Tel Aviv, 2019
Foto ANP/EPA, Jim Hollander


FOTO US NAVY, JORDAN KIRK JOHNSON

494

Tunnelvisie? De digitale strijd rond het Gazaconflict

Kraesten Arnold

In de digitale oorlogvoering tussen Israël en Hamas blijkt de terreurgroep een serieuze informatie- en inlichtingendreiging te zijn.

'Nederland, pak een leidende rol in de NAVO'

Leonie Boskeljon-Horst, Freek Groen en Maarten Katsman

Generaal-majoor Denny Traas, commandant van het Deployable Air Command and Control Centre van de NAVO, vertelt in een gesprek met de *Militaire Spectator* onder meer hoe het DACCC reageert op de oorlog in Oekraïne.

530

MILITAIRESPECTATOR

JAARGANG 193 NUMMER 9 – 2024

FOTO MCD, CINTHIA NIJSSEN

508

FOTO MCD, GREGORY FRENI

518

De theorie van Biddle en de oorlog in Oekraïne

Carel Sellmeijer

De theorie van Biddle helpt bij het verklaren van denkbeelden over toekomstig landoptreden en de werkelijkheid van militaire operaties in Oekraïne.

Straffen of leren?

Leonie Boskeljon-Horst, Eva van Baarle en Anke Snoek

Een organisatie die straft als er een incident plaatsvindt verhindert dat medewerkers er van leren en maakt een restauratieve *just culture* bijna onmogelijk.

EN VERDER

De redactie verheugt zich zeer over deze gastcolumn van secretaris-generaal van Defensie Maarten Schurink. Zijn reactie onderstreept de waarde van de *Militaire Spectator* als een platform voor discussie.

Richard Tieskens, hoofdredacteur

Samenwerking en vertrouwen

Maarten Schurink, secretaris-generaal Defensie

In het editoriaal in de *Militaire Spectator* van juli werd ik uitgedaagd eens een column te schrijven over het belang van oog hebben voor de mens en het opbouwen van vertrouwen in het gereedstellen voor hoofdtaak 1.[1] Ik werd opgeroepen een antwoord te geven op de vraag waar we in hoofdtaak 1 de tijd en ruimte vinden voor het worden van één, zoals Stanley McChrystal dat noemt, *team of teams*: of we in staat zijn ons te richten op ons hoofdwapensysteem – de mens – en niet alleen op de regels en processen. Bij dezen.

Kort na mijn start kreeg ik het boek *Turn the Ship Around! A True Story of Turning Followers into Leaders*.[2] Ik heb dat in één ruk uitgelezen. Een prachtig verhaal van een onderzeebootcommandant die, vooral door aandacht aan de mens te geven, zijn bemanning met grote stappen beter maakte. Natuurlijk was het ook daar aan boord noodzakelijk om de regels te volgen en de procedures en processen soepeler te maken en liepen er projecten ter bevordering van de samenhang tussen initiatieven en een soepele bedrijfsvoering. Maar met samenwerking en vertrouwen kom je verder.

Wij zijn zelf het fundament van ons succes. Wij kunnen effectief reageren op crises en opereren als één geheel, regels niet. Juist als de dreiging toeneemt is daarom ruimte voor kwetsbaarheid en voor het maken van fouten cruciaal. Juist dan zijn openheid, vertrouwen en samenwerking niet alleen belangrijk voor het welzijn van onze mensen, maar ook voor onze operationele effectiviteit.

Hoewel dit logisch klinkt, is het in de praktijk helaas niet zo eenvoudig. Onze *can do*-mentaliteit, waar we als Defensie ook trots op (mogen) zijn, maakt ons enorm resultaatgericht. Dit is goed. Alleen verliezen we daarbij soms de aandacht voor elkaar uit het oog, ik ook. Het resultaat is vaak zo belangrijk, maar als je resultaten wil blijven bereiken is die focus niet genoeg. Als bestuursraad (het hoogste overlegorgaan van het ministerie) hebben we daarom een aantal principes opgenomen bovenaan onze wekelijkse agenda. Deze wijzen ons iedere week opnieuw op het belang van samenwerking, openheid, werkplezier en *mission command*, zodat we deze steeds verder kunnen internaliseren. Zo beginnen we sinds een jaar iedere bestuursraad met een *check in*-ronde: hoe zit iedereen erbij? Hoe gaat het met de mens achter je collega? En hoewel we initieel geneigd waren snel door te gaan naar de inhoud, merk ik dat het *juist* deze incheckronde is die ons meer verbindt als mensen, en daarmee onze effectiviteit als team versterkt.

Een organisatie die in staat is om te leren van haar fouten, is een organisatie die sterker wordt. Dit vraagt om een cultuur waarin we niet bang zijn om verantwoordelijkheid te nemen, waarin we fouten durven maken en waarin we deze fouten zien als kansen om te leren en te groeien. Dit is geen gemakkelijke opgave in een omgeving vol regels en procedures, maar het is wel een noodzakelijke stap. Snel en effectief handelen kan alleen als we vertragende processen loslaten, afstappen van de manier waarop we het 'altijd al hebben gedaan', vertrouwen op de mensen die het dichtst bij de problemen staan en hun de ruimte geven om beslissingen te nemen en aanmoedigen verantwoordelijkheid te dragen.

1 'Team of teams', editoriaal, *Militaire Spectator* 193 (2024) (7/8) 429.
2 L. David Marquet, *Turn the Ship Around! A True Story of Turning Followers into Leaders* (Londen, Penguin, 2015).

FOTO MCD, PHIL NIJHUIS

Het vergroten van het onderling vertrouwen en het verbeteren van onze samenwerking vraagt tijd, aandacht en toewijding van ons allemaal. Collega's in een leidinggevende functie op elk niveau hebben hierin een voorbeeldfunctie. We moeten actief werken aan het creëren van een cultuur waarin iedereen zich veilig voelt om bij te dragen, lef te tonen en creatief te denken. Een cultuur waarin ieders expertise wordt gewaardeerd en waarin we elkaar steunen in plaats van afrekenen. Daarom moeten wij allemaal, leidinggevenden voorop, werken via mission command: geef vrijheid van handelen mét bevoegdheden. En spreek elkaar – ook mij! – erop aan wanneer het toch te veel over het 'hoe' gaat. Alleen samen kunnen we deze cultuuromslag maken.

De uitdagingen waar we voor staan zijn groot, maar ik ben ervan overtuigd dat we deze kunnen overwinnen door samen te werken als één team. Laten we ons richten op onze grootste kracht: onze mensen. Laten we samen de tijd en ruimte maken voor het worden van één team of teams. Binnen Defensie, en in samenwerking met de maatschappij. Want we verdedigen de veiligheid van Nederland samen. Samen bouwen we aan een defensieorganisatie die niet alleen in staat is om te reageren op externe dreigingen, maar ook intern sterk en toekomstbestendig is. Een organisatie gereed voor hoofdtaak 1. ■

Tunnelvisie? De digitale strijd rond het Gazaconflict

Luitenant-kolonel ing. K.L. Arnold EMSD MSc*

Op 7 oktober 2023 lanceerde Hamas[1] een aanval op Israëlisch grondgebied, waarbij extreem geweld werd ingezet. Israël reageerde met operatie Iron Swords en viel de Gazastrook binnen. Vrijwel tegelijkertijd begonnen andere entiteiten zich actief te bemoeien met dit conflict. Zij vochten niet fysiek, noch ter plaatse, maar aan het online cyberfront. In tegenstelling tot het intense kinetische conflict is informatie over de digitale oorlogsvoering slechts beperkt beschikbaar. Eén aspect is al wel duidelijk: de strijdende cyberpartijen lijken vooralsnog niet in staat geweest om kritieke systemen of diensten beslissende strategische schade toe te brengen. Dat roept vragen op over de relevantie van cyberoorlogvoering. Hebben de strijdende partijen eigenlijk wel cybercapaciteit? Als de strijd eenmaal losbarst, spelen cyberaanvallen dan nog wel een rol? Heeft Hamas digitale infrastructuur die het aanvallen waard is? Als er aanvallen zijn, wat zijn dan de doelwitten en welke effecten zijn mogelijk?

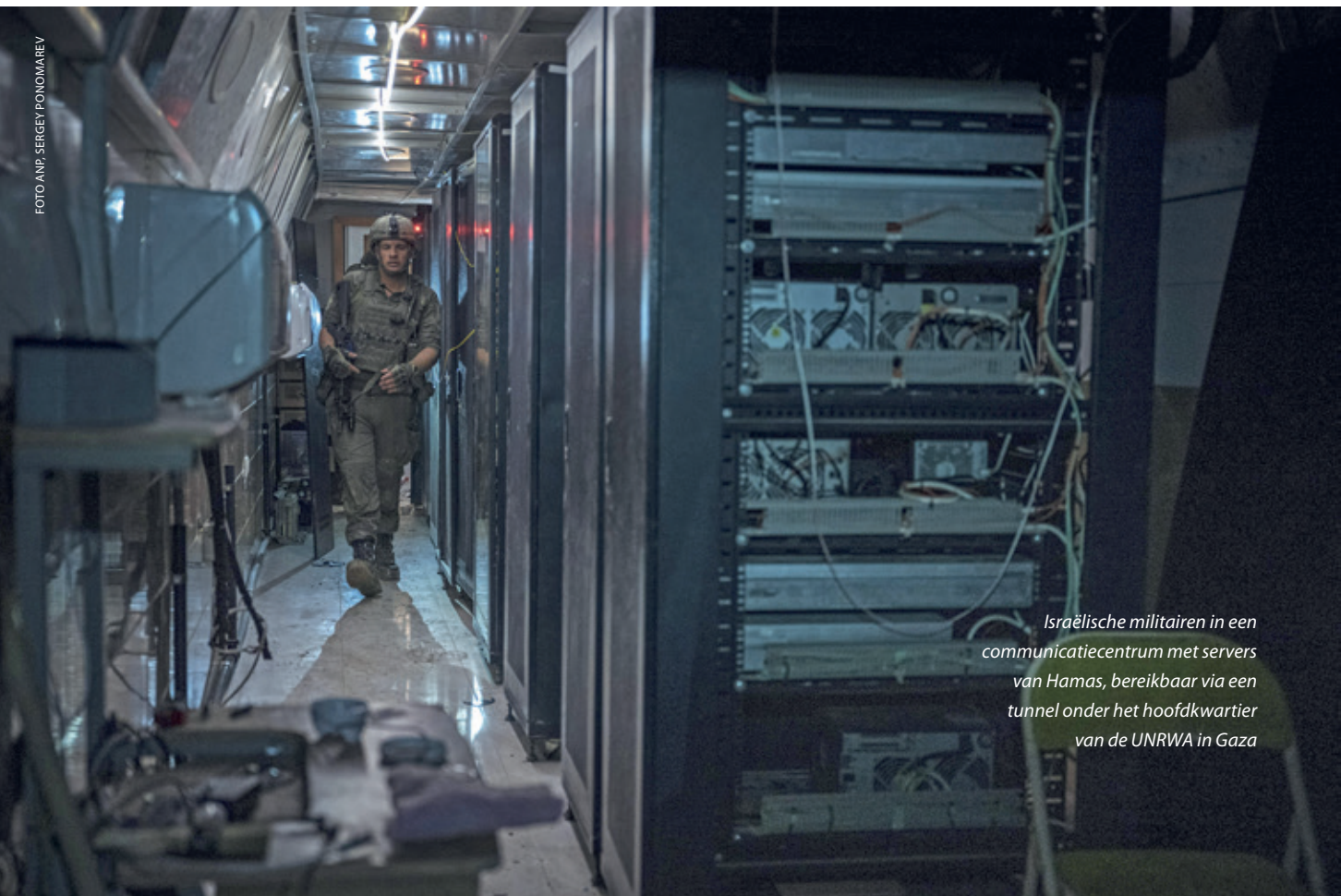


FOTO ANP, SERGEY PONOMAREV

Israëlische militairen in een communicatiecentrum met servers van Hamas, bereikbaar via een tunnel onder het hoofdkwartier van de UNRWA in Gaza

Cyberoorlogvoering kent meerdere aspecten. Hacken van computers en netwerken is één ding, maar het gebruik ervan om anderen te beïnvloeden is van een andere orde. Dit artikel gaat in op de cyberoorlogvoering rond het Hamas-Israëlconflict, om te bezien in hoeverre cyberoperaties relevant zijn in dit hedendaagse gewapende, irreguliere conflict. De inzet van cybermiddelen in het huidige conflict vormt een unieke casestudie over een digitale strijd, gevoerd tussen een gedigitaliseerde natiestaat en een hybride terroristische organisatie.

Dit artikel schetst eerst het cyberpotentieel van beide partijen, waarna een overzicht volgt van cyberaanvallen uit het recente verleden. In het huidige conflict komen eerst 'hard cyber-operaties' aan bod en vervolgens cyber-enabled beïnvloedingsoperaties ('soft cyberoperaties').[2] Het blijkt dat cyberoorlogvoering en de strijdende partijen onderdeel zijn van een breder geopolitiek conflict.

Scheve verhoudingen?

Israël heeft een uitgebreid cyberpotentieel, met honderden hightechbedrijven die met hun hoogopgeleide en bekwame personeel geavanceerde producten en diensten creëren. Het land vormt dan ook een van de grootste cybersecurity-ecosystemen ter wereld.[3] Het International Institute for Strategic Studies beschouwt Israël daarom als 'Tier Two' cyberstaat.[4] Het land excelleert in cyberbeveiliging en (cyber)inlichtingen verzamelen,[5] maar heeft ook een sterk ontwikkelde offensieve (cyberwapen)capaciteit.[6]

Men kan redelijkerwijs aannemen dat een niet-statelijke organisatie als Hamas dergelijke middelen, kennis en ervaring niet heeft.[7] Israël heeft bovendien de controle over de internet-infrastructuur en telecommunicatiefrequenties in Gaza. Tel daarbij op de chronische elektriciteitstekorten in het Palestijnse gebied, en het is des te opmerkelijker dat Hamas überhaupt een cyberdreiging *zou kunnen* vormen. Daar staat tegenover dat de groep de afgelopen vijftien jaar met geld, middelen en training is ondersteund door statelijke actoren vanuit Qatar, Iran en Turkije.[8] De digitale slagkracht van Hamas is daarnaast versterkt door een ideologische en strategische alliantie met Hezbollah en Iran.[9]

Cyberspace wordt niet beperkt door geografische grenzen. Dit impliceert dat elke actor, vanuit elke locatie waar een internetverbinding voorhanden is, actief betrokken kan raken bij deze cyberoorlog; niet alleen als aanvaller, maar ook als slachtoffer.

* Lt-kol Kraesten Arnold is als cyberonderzoeker en -docent verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie te Breda. Zijn focus ligt met name op offensieve cyberoperaties door statelijke actoren.

1 Een Arabisch acroniem voor Harakat al-Muqawamah al-Islamiyyah ('de Islamitische Verzetsbeweging').

2 Hard cyberoperaties zijn cyberaanvallen gericht tegen cyberspace zelf, zoals hardware en software. Soft cyberoperaties gebruiken cyberspace voor bijvoorbeeld informatieoperaties of psychologische oorlogvoering. Zie: Peter B.M.J. Pijpers en Kraesten L. Arnold, 'Conquering the invisible battleground', *Atlantisch Perspectief* 44 (2020) (4).

3 Naast de bekende high-tech clusters Silicon Valley en Washington, D.C. Bron: Tali Hataku en Erran Camel, *The Dynamics of the Largest Cybersecurity Industrial Clusters: San Francisco Bay Area, Washington D.C. and Israel*, Blavatnik Interdisciplinary Cyber Research Center (ICRC), januari 2021. Zie: https://icrc.tau.ac.il/sites/cyberstudies-english.tau.ac.il/files/media_server/all-units/Cyber%20DIGITAL%20Final%20unlocked-1.pdf.

4 Tezamen met Australië, Canada, China, Frankrijk, Duitsland, Rusland, Nederland en het Verenigd Koninkrijk. De Verenigde Staten (VS) zijn overigens de enige 'Tier One' staat. Bron: 'Cyber Capabilities and national Power: A Net Assessment', The International Institute for Strategic Studies (IISS), IISS research Paper, 28 juni 2021, 10. Zie: https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power.

5 Het Israëlische *NSO Group Technologies* is bijvoorbeeld de maker van de beruchte 'Pegasus' spionagesoftware; wereldwijd in gebruik bij overheden en waarmee, naar verluidt, de AIVD in 2019 de telefoon van Ridouan Taghi wist te hacken. Bron: Huib Modderkolk, 'AIVD gebruikt omstreden Israëlische hacksoftware', *de Volkskrant*, 2 juni 2022. Zie: https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/.

6 De meest tot de verbeelding sprekende cyberaanval tot op heden (de Stuxnet-cyberaanval tegen het Iraanse kernwapenprogramma in de periode 2007-2010) wordt toegeschreven aan een Amerikaans-Israëlisch samenwerkingsverband. Bron: Kim Zetter,*Countdown to zero day: Stuxnet and the launch of the world's first digital weapon* (Crown, 2015).

7 Desondanks bleek Hamas aan de vooravond van de 7 oktober-inval over een Militaire Inlichtingendienst te beschikken die bestond uit zo'n 2.100 krachten, verdeeld over vijf subafdelingen: observatie, cyber, signals intelligence (SIGINT), open source intelligence (OSINT), en human intelligence (HUMINT). Bron: Itay Ilnai, *The road to Oct. 7: How Hamas got the intelligence it needed*, Israel Hayom, 16 maart 2024. Zie: https://www.israelhayom.com/2024/03/16/the-road-to-oct-7-how-hamas-got-the-intelligence-it-needed/.

8 Jean-Luc Mounier, 'Qatar, Iran, Turkey and beyond: Hamas's network of allies', *France24*, 14 oktober 2023. Zie: https://www.france24.com/en/middle-east/20231014-qatar-iran-turkey-and-beyond-the-galaxy-of-hamas-supporters.

9 Marcin Andrzej Piotrowski, 'Iran's Relations with Hezbollah and Hamas Evolving', The Polish Institute of International Affairs, 24 oktober 2023. Zie: https://www.pism.pl/publications/irans-relations-with-hezbollah-and-hamas-evolving.

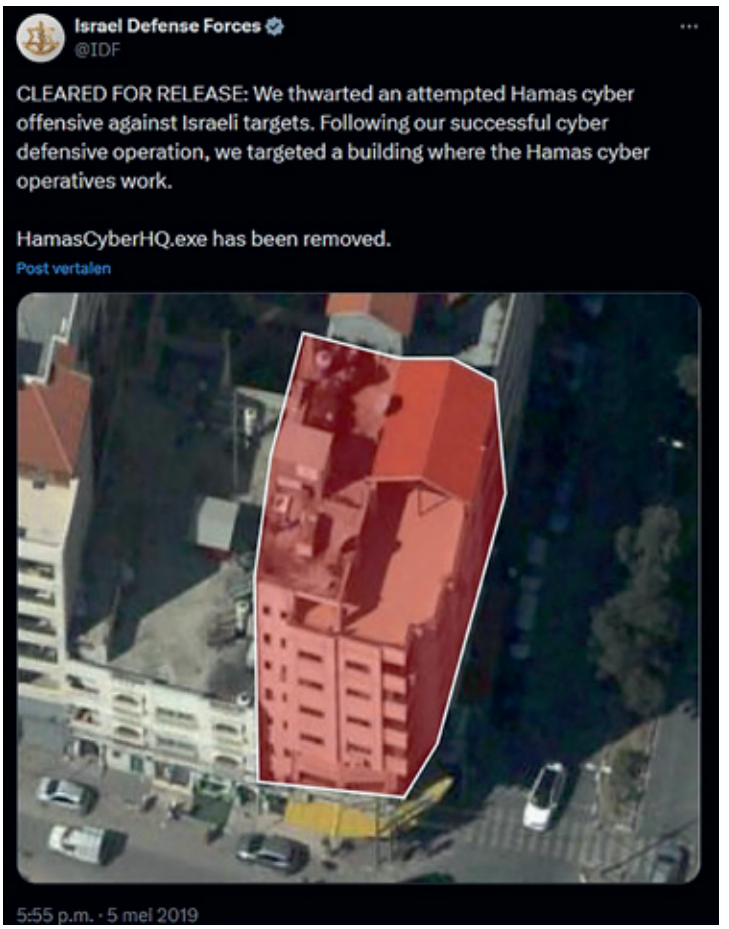


FOTO ISRAEL DEFENSE FORCES

Het Twitterbericht waarin de IDF de eerste kinetische vergeldingsactie voor een cyberaanval bekend maakte

Voorafgaande virtuele vijandelijkheden

Tijdens een eerder Gaza-conflict (2009) benutte zowel Hamas als Israël uitgebreid de inherente voordelen van sociale media. Het intense fysieke grondgevecht kreeg daarmee een digitale weerspiegeling. Beide partijen verkondigden online hun respectievelijke narratief en zochten, en vonden, steun van patriottische hackers en activisten elders in de wereld. Foto's, videobeelden, cartoons, objectieve informatie en propaganda werden verspreid, bewust hergebruikt (misinformatie) of ronduit vervalst (desinformatie). Beide partijen richtten zich daarnaast op het verstoren van websites, platforms, accounts en blogs die steun verleenden aan de tegenpartij.[10]

Traditionele media hadden ook destijds vrijwel geen toegang tot de grondstrijd. Voor informatieverspreiding leunden beide partijen zwaar op het internet en sociale media. Iedere niet-professionele *citizen journalist* kon voortaan in *real time* de strijd vastleggen, bewerken en uploaden. Traditionele mediabedrijven gebruikten de online informatie om die vervolgens via reguliere mediakanalen te verspreiden. Deze indirecte nieuwsverspreiding zorgde vervolgens weer voor een verhoogde focus op het conflict via socialemediaplatforms.[11]

In 2012 kondigde de woordvoerder van de Israëlische strijdkrachten een aanval op Gaza aan via Twitter. De tegenstanders verzandden in een *battle of the narratives* waarbij ze nieuwsberichten, verhalen en afbeeldingen deelden die vooral de misstappen van de ander benadrukten. Via hashtags (#) als #BringBackOurBoys, #GazaUnderAttack en #IsraelUnderFire trachtten beide zijdes hun gelijk te halen.[12]

Tot 2014 betrof de cyberoorlog voornamelijk 'digitale beïnvloeding' of 'soft cyberoperaties'. Sindsdien richtten zowel pro-Palestijnse als pro-Israëlische groepen zich ook op het hacken van computers en netwerken via Distributed-Denial-of-Service (DDoS)-aanvallen en defacements;[13] vervelend, maar met een relatief beperkte (herstelbare) schade. Dat veranderde in

10 David Patrikarakos, *War in 140 characters: how social media is reshaping conflict in the twenty-first century* (First Edition, New York, Basic Books, 2017).

11 Naila Hamdy, 'Arab media adopt citizen journalism to change the dynamics of conflict coverage', *Global Media Journal Arabian Edition* 1 (2010) (1) 4.

12 Patrikarakos, *War in 140 characters*.

13 Bij een Denial-of-Service (DoS)-aanval wordt een computer, netwerk of applicatie bestookt met zoveel opdrachten of verzoeken dat de werking van die computer of dat netwerk ernstig wordt beperkt of zelfs onmogelijk gemaakt. Voor een Distributed DoS-aanval worden meerdere computers gebruikt. Bij een website defacement verandert de aanvaller 'het uiterlijk' van een website door die te vullen met andere inhoud (tekstueel en/of visueel), zoals politieke, sociale of religieuze boodschappen.

2018, toen een aan Hamas-gelieerde hackergroep een nepversie wist te maken van Israëls raketwaarschuwingsapp 'RedAlert'. De vervalste app imiteerde de reguliere versie, maar zodra deze was gedownload, kreeg de aanvaller via de gemanipuleerde software de volledige controle over de betreffende mobiele telefoon. Naar verluidt werd de spionagesoftware (spyware) in een vroeg stadium ontdekt en was uiteindelijk weinig schade aangericht.[14]

In 2018 manipuleerde een aan Hamas-gelieerde groep de legitieme (WK-voetbal) softwareapplicatie 'Golden Cup' met spyware. Om vroegtijdige ontdekking van de gemanipuleerde software te voorkomen en beveiligingsmaatregelen te omzeilen, werd de spyware pas actief *nadat* de app was gedownload.[15] Na installatie van de app zochten de aanvallers via fictieve personages contact met hun slachtoffers, waaronder vele Israëlische militairen. Een soortgelijke truc werd uitgehaald via een fitness-app voor hardlopers.

In 2020 slaagde een aan Hamas-gelieerde groep (*Arid Viper*)[16] erin mobiele telefoons van IDF-soldaten te hacken. Ditmaal maakten de aanvallers gebruik van populaire dating-apps waarop (gefingeerde) vrouwelijke immigranten Israëlische soldaten versierden. Achter de geloofwaardig opgebouwde profielen schuilden hackers. Was het initiële contact gelegd, dan werden de slachtoffers verleid extra software te downloaden. De slachtoffers haalden daarmee zelf een 'digitaal Trojaans paard' binnen, waarna de aanvaller ongemerkt de volledige controle over geïnfecteerde mobieltjes had.[17]

Dankzij de geïnstalleerde spyware verkregen de hackers de volledige controle over de mobiele telefoons van hun slachtoffers. De apparaten veranderden in ultieme spionageapparatuur. Het stelde de aanvallers in staat het apparaat onopgemerkt te volgen, heimelijk foto's en videobeelden te maken, en stiekem geluidsopnames te maken en te versturen. Zo verzamelden de hackers ongemerkt inlichtingen over Israëlische troepen, troepenbewegingen, bases en militair materieel rondom de Gazastrook.[18]

In 2019, in een periode dat vanuit Gaza honderden raketten werden gelanceerd richting Israël, initieerde een aan Hamas-gelieerde hackergroep – eveneens vanuit Gaza – een cyberaanval op Israël. Over de exacte doelwitten of verwachte effecten van deze cyberaanval is nauwelijks openlijk informatie beschikbaar. Wat wel bekend is, is dat Israël deze cyberaanval tijdig onderkende en verijdelde, om vervolgens met een luchtaanval het gebouw in Gaza van waaruit de cyberaanval plaatsvond te vernietigen. Deze reactie is daarmee, voor zover bekend, de eerste kinetische vergeldingsactie voor een (geplande) cyberaanval. De IDF maakte deze actie op een nogal ironische wijze bekend: 'HamasCyberHQ.exe has been removed',[19] als ware het gebouw en zijn bewoners een softwareprogramma dat was gewist.

Ondanks Israëls optimistische claim volgden ook daarna nog cyberaanvallen; weliswaar niet vanuit Gaza, maar daarbuiten. De meest voor de hand liggende reden hiervoor is dat Hamas ook buiten Gaza beschikt over de nodige cyberfaciliteiten, zoals in Turkije,[20] Iran en Qatar.[21]

14 Toi Staff, 'Hamas tries to hack Israelis with fake rocket warning app', *The Times of Israel*, 10 augustus 2018. Zie: https://www.timesofisrael.com/hamas-tries-to-hac-israelis-with-fake-rocket-warning-app/.

15 Taylor Armerding, 'Golden Cup App Was a World Cup of Trouble', *Synopsys*, 12 juli 2022. Zie: https://www.synopsys.com/blogs/software-security/golden-cup-app-world-cup-trouble/.

16 De groep *Arid Viper* is een Arabisch sprekende, politiek gemotiveerde Advanced Persistent Threat (APT). Een APT betreft een veelal statelijke tegenstander die beschikt over technologisch hoogwaardige kennis en voldoende middelen om langdurig en via meerdere aanvalspaden zijn doelen te bereiken. De groep staat ook (onder meer) bekend onder de naam 'APT-C-23'.

17 Cybereason Nocturnus, 'Operation Bearded Barbie: APT-C-23 Campaign Targeting Israeli Officials'. Zie: https://www.cybereason.com/blog/operation-bearded-barbie-apt-c-23-campaign-targeting-israeli-officials.

18 Yaniv Kubovich, 'Hamas Cyber Ops Spied on Hundreds of Israeli Soldiers Using Fake World Cup, Dating Apps', Haaretz, 3 juli 2018. Zie: https://www.haaretz.com/israel-news/hamas-cyber-ops-spied-on-israeli-soldiers-using-fake-world-cup-app-1.6241773.

19 IDF woordvoerder op Twitter, 5 mei 2019. Zie: https://twitter.com/IDF/status/1125066395010699264.

20 Anshel Pfeffer, 'Hamas Uses Secret Cyberwar Base in Turkey to Target Enemies', *The Times* (UK), 22 oktober, 2020. Zie: https://www.thetimes.co.uk/article/hamas-running-secret-cyberwar-hq-in-turkey-29mz50sxs.

21 Simon Handler, 'The cyber strategy and operations of Hamas: Green flags and green hats', Atlantic Council Report, 7 november 2022. Zie: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-cyber-strategy-and-operations-of-hamas-green-flags-and-green-hats/.

(Geen) digitale voorwaarschuwing?

'Harde' cyberaanvallen door Hamas, gericht op fysieke schade, deden zich de afgelopen jaren niet meer voor. De terreurgroep leek zich te focussen op cyberspionage en digitale beïnvloedingsoperaties. Israël, het land met de hoogstaande reputatie omtrent cyberbeveiliging en (cyber)inlichtingen verzamelen, dat bovendien controle uitoefent over de telecommunicatiefrequenties en internetinfrastructuur in de Gazastrook, leek zich dan ook weinig zorgen te maken over de digitale slagkracht van zijn tegenstander.

Israël wist dat Palestijnse militanten gebruik maakten van bekabelde communicatiemiddelen om afluisteren te bemoeilijken. Maar dat Hamas-planners hun specifieke terreurdaad kennelijk voorbereidden door alléén te communiceren (en te coördineren) via bekabelde verbindingen in de Gazatunnels spreekt tot de verbeelding. Door geen draadloze, digitale communicatiemiddelen te gebruiken, vermeden ze interceptie en analyse van signalen uit satelliet- en radiocommunicatie door de Israëlische militaire inlichtingendienst.[22]

Die dienst wist overigens dat een Hamas cyberactor (Gaza Cybergang) actief het internet verkende, op zoek naar IP-adressen van beveiligingscamera's die online toegankelijk waren.[23] Waren de IP-adressen eenmaal bekend en hadden de legitieme gebruikers het wachtwoord niet gewijzigd, dan konden de aanvallers heimelijk toegang krijgen tot die camera's via de (online beschikbare) standaard wachtwoorden.

De hackers verkregen daarmee real-time videobeelden van verschillende dorpen, militaire bases en de bredere Gaza-grensstreek. Naar later bleek verzamelde Hamas zo bruikbare inlichtingen in de aanloop naar zijn aanvallen op 7 oktober.[24]

De cyberstrijd barst los

Toen die aanval eenmaal begon, barstte ook de cyberstrijd los. De hard en soft cyberoperaties van beide zijdes vormen een unieke casestudie over een digitale strijd.

Hard cyberoperaties

Het merendeel van de cyberaanvallen rond het uitbarsten van het '7-oktoberconflict' betrof Distributed-Denial-of-Service (DDoS)-aanvallen, gericht op het (tijdelijk) verstoren van toegang tot, of het gebruik van, de aangevallen websites of applicaties en daarmee de (digitale) bedrijfsvoering van de slachtoffers. Het nagestreefde effect is veelal onzekerheid en chaos creëren onder de burgerbevolking, zeker als aanvallen zijn gericht op civiele objecten als nieuwswebsites, banken of de gezondheidszorg.

Pro-Palestijnse aanvallers voerden zo'n twaalf minuten na de Hamas-inval DDoS-aanvallen uit op Israëlische websites. Hoewel pro-Israëlische actoren soortgelijke aanvallen uitvoerden tegen Palestijnse websites, lag het aantal getroffen Israëlische entiteiten significant hoger dan het aantal Palestijnse.[25] De direct aangerichte schade van een DDoS-aanval is vaak beperkt en herstelbaar, maar doordat deze aanvallen vaak de aandacht trekken, kunnen ze ook dienen als bliksemafleider voor een heimelijke aanval op andere doelwitten. Of dat hier het geval was, is momenteel niet vast te stellen.

Andere cyberaanvallen betroffen website defacements, een soort digitale graffiti waarbij het 'uiterlijk' (de startpagina) van de aangevallen website werd aangepast, vaak met een specifieke politieke of religieuze boodschap. Deze cyberaanvallen zijn uitgevoerd door beide zijdes, maar ook hier overtrof het aantal pro-Palestijnse acties de pro-Israëlische. Tussen 7 en 16 oktober

22 Pamela Brown en Zachary Cohen, 'Hamas operatives used phone lines installed in tunnels under Gaza to plan Israel attack', CNN Politics, 25 oktober 2023. Zie: https://edition.cnn.com/2023/10/24/politics/intelligence-hamas-israel-attack-tunnels-phone-lines/index.html.

23 Het Internet Protocol (IP) is een wereldwijd afgesproken verzameling regels voor de wijze waarop computers op een computernetwerk (zoals het internet) met elkaar kunnen communiceren. Een IP-adres is een uniek identificatienummer ('digitaal postadres') dat door een Internet Service Provider wordt toegekend aan een apparaat dat is aangesloten op internet of een lokaal netwerk.

24 Ilnai, *The road to Oct. 7*.

25 Tanner Wagner, *Escalation of Threats in the Middle East*, CyberPeace Institute, 6 november 2023. Zie: https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east.

FOTO X.COM, CYB3R DRAG0NZ TEAM

Een hack-and-leak-operatie en website defacement ineen, geclaimd door het pro-Palestijnse Cyb3r Drag0nz Team. Het doelwit was een civiel object: BrainIT, een bedrijf dat escape rooms exploiteert. De hackers claimen gegevens van 40.000 klanten te hebben gelekt

werden ruim 500 defacementoperaties uitgevoerd tegen Israëlische websites.[26]

Een ander type cyberaanvallen betreft hack-and-leak-operaties. Daarbij steelt de aanvaller geclassificeerde of anderszins gevoelige informatie om die vervolgens te publiceren. Meerdere pro-Palestijnse activistische hackers claimden dat zij geclassificeerde defensie-informatie hadden buitgemaakt door militaire systemen en kritieke infrastructuur te hacken. Deze beweringen zijn lastig te verifiëren, aangezien geen van de slachtoffers dergelijke aanvallen meldde. Bovendien leken de gelekte gegevens te zijn 'hergebruikt'; afkomstig van eerdere cyberaanvallen en onterecht gepresenteerd als nieuw.[27]

Beide partijen gebruiken daarnaast social engineering-technieken om mensen te manipuleren (vijandelijke strijders in het bijzonder) en zo informatie te ontfutselen over vijandelijke troepenlocaties, -bewegingen, aanvalsplannen of andere relevante informatie. Met een techniek die bekend staat als catphishing of honey trapping doen hackers zich bijvoorbeeld voor als een aantrekkelijke jongedame, om zo initieel contact te leggen en vervolgens heimelijk inlichtingen te vergaren via tekst-, spraak- en/of videoberichten. Op basis van online verkregen informatie kan een gerichte kinetische aanval volgen.

De pro-Palestijnse cyberaanvallen lijken niet bewust afgestemd op Hamas' kinetische acties op 7 oktober. In 2022 ging Ruslands grootschalige grondoffensief tegen Oekraïne gepaard met destructieve 'wiperware' cyberaanvallen; kwaadaardige software, bedoeld om data en

26 Darkowl, 'Hacktivist Groups Use Defacements in the Israel Hamas Conflict', 26 oktober 2023. Zie: https://www.darkowl.com/blog-content/hacktivist-groups-use-defacements-in-the-israel-hamas-conflict/.

27 Omree Wechsler, 'The Cyberwarfare Front of the Israel-Gaza War', *The National Interest*, 5 november 2023. Zie: https://nationalinterest.org/feature/cyberwarfare-front-israel-gaza-war-207163.

Opvallend in dit conflict is het sterk toegenomen gebruik van zogeheten n-day vulnerabilities

computers van de slachtoffers blijvend te vernietigen.[28] Die Russische cyberaanvallen werden voorbereid en uitgevoerd in de weken voor, tijdens en vlak na de invasie. In het Hamas-Israëlconflict verschenen de eerste cyberaanvallen pas na het publiekelijk bekend worden van Hamas' fysieke aanval. Wel werden ook hier nieuwe varianten van destructieve wiperware ingezet, en ontdekt.[29]

Opvallend in dit conflict is het sterk toegenomen gebruik van zogeheten n-day vulnerabilities als manier om een computersysteem of netwerk ongeautoriseerd binnen te dringen.[30] Bepaalde statelijke of staatsgesteunde aanvallers houden bijvoorbeeld scherp in de gaten wanneer een fabrikant (zoals Microsoft) nieuw gevonden kwetsbaarheden en bijbehorende oplossingen (patches) openbaar maakt. Door zeer snel de gepubliceerde kwetsbaarheden én de bijbehorende patches te analyseren, kan een aanvaller manieren ontwikkelen om die gevonden kwetsbaarheid te misbruiken en nog niet-gepatchte computers aan te vallen. Diverse anti-Israëlische groepen gebruiken deze aanvalsmethode en wisselen hierover onderling informatie uit.[31]

Pro-Hamas hackers bestookten voornamelijk Israëlische kranten- en mediawebsites. De grondstrijd werd vergezeld door cyberoorlogvoering die voornamelijk was gericht tegen websites die in die hectische periode snel cruciale informatie aan vooral de burgerbevolking konden verstrekken. Naast de media waren in mindere mate ook de softwareindustrie, de financiële sector, regeringswebsites en verschillende ziekenhuizen het doelwit van gerichte cyberaanvallen.[32]

Aan Palestijnse zijde was de financiële sector het voornaamste getroffen doelwit (76 procent van alle DDoS-aanvallen). De internetsector werd eveneens getroffen, maar Palestijnse media daarentegen vrijwel niet. Het feit dat veel meer cyberaanvallen waren gericht tegen Israëlische dan Palestijnse doelwitten, is waarschijnlijk een logisch gevolg van Israëls verregaande digitalisatie, waardoor het land automatisch een groter aanvalsoppervlak biedt.

Een stabiele internetverbinding was in Gaza al geen zekerheid, maar sinds de IDF de strook binnenviel, is de connectiviteit nog verder teruggelopen. Dit komt deels door fysieke schade van kinetische aanvallen op communicatienetwerken en internetdiensten, en deels door voortdurende uitval van elektriciteit. Aangezien de Palestijnse internet-infrastructuur nauwelijks *mobiele* internetdiensten kent, heeft schade aan het vaste netwerk ook direct gevolgen voor allerlei civiele diensten (waaronder medische). Op 17 januari 2024 werd een vrijwel volledige telecommunicatie black-out in de Gazastrook geconstateerd die zes dagen duurde.

Computers en computerprogramma's spelen overigens op nog een andere wijze een rol in dit conflict. De IDF gebruikt voor target selection

28 K.L Arnold en S. van Dorst, 'Wiperware: een nieuw cyberwapen voor de militaire toolbox?', *Militaire Spectator* 192 (2023) (11). Zie: https://militairespectator.nl/artikelen/wiperware-een-nieuw-cyberwapen-voor-de-militaire-toolbox.

29 Trustwave, 'Overview of the cyber warfare used in Israel-Hamas war', 5 december 2023. Zie: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyberwarfare-used-in-israel-hamas-war/.

30 De term n-day vulnerability is gebaseerd op een zero-day vulnerability: een kwetsbaarheid in een software (of hardware) product die kan worden uitgebuit vóórdat de maker van het product die kwetsbaarheid heeft verholpen. N-day vulnerabilities zijn kwetsbaarheden waarvoor (sinds een n-aantal dagen) oplossingen (patches) beschikbaar zijn. Echter, zolang een computersysteem niet tijdig wordt gepatcht, blijft het systeem kwetsbaar voor een cyberaanval. Door snel de gepubliceerde kwetsbaarheid én de bijbehorende patch te analyseren en te vergelijken, kan een aanvaller een manier ontwikkelen om die gevonden kwetsbaarheid te misbruiken om niet-gepatchte computers aan te vallen.

31 Israel National Cyber Directorate (INCD), 'Iron Swords' War in Cyber Sphere: Insights, Recommendations and Mitigations', 7 januari 2024, V1.0, 8.

32 'Health Ministry disconnects the remote connection of several hospitals following cyber attack', *Jerusalem Post*, 21 oktober 2023. Zie: https://www.jpost.com/breaking-news/article-769508.

onder meer kunstmatige intelligentie. Met computerprogramma's als *Where's Daddy*, *Lavender* en *The Gospel* identificeert en lokaliseert het leger uit te schakelen Hamas-strijders. Omdat dit evenwel besluitvormingsondersteunende programma's zijn en geen cyberoorlogvoering betreft, vallen deze programma's buiten de scope van dit artikel.

Digitale beïnvloeding

Toen Hamas-strijders op 7 oktober de aanval openden op Israël werden hun acties live gestreamd door strijders zelf en mediapersoneel dat met hen optrok. Beelden van gruwelijkheden, waaronder executies, werden live uitgezonden en verspreid via sociale media.[33] Dit past in een strategie waarbij cyberspace wordt benut voor psychologische oorlogsvoering en informatieoperaties. Publiciteit is dan ook een essentiële component voor het succes van een terroristische actie. Hamas heeft op ongekende schaal digitale middelen ingezet om dat schokeffect te bereiken.[34]

Ook Israël voert actief psychologische (beïnvloedings)operaties uit. De Influence Unit van de IDF plaatst verhalen in de pers om bewust de perceptie van de oorlog te sturen; niet alleen de publieke opinie, maar ook de tegenstander. Techbedrijven ontwikkelden digitale middelen om te meten hoe de publieke opinie reageert op de berichtgevingen van het leger.[35]

Op tactisch en operationeel niveau gaat dit conflict voornamelijk om raketten en kogels, en het daaruit voortvloeiende menselijk leed en zichtbare schade. Op strategisch niveau gaat de strijd evenwel om het beïnvloeden (manipuleren) van de bevolking; de perceptie van de publieke opinie en het politieke besluitvormingsproces. De te beïnvloeden doelgroep (targeted audience) bestaat niet alleen uit de eigen bevolking en de eigen politiek leiders, maar ook uit aanhangers, steunverleners en geldschieters buiten de regio; en politiek leiders wereldwijd. Voor beide strijdende partijen lijkt internationale steun het Centre of Gravity te zijn.[36] De (perceptie van) aantallen burgerslachtoffers zijn daarbij een luguber middel. Naast het verspreiden van 'zuivere feiten' hieromtrent spelen ook leugens, onjuistheden en regelrechte desinformatie een belangrijke rol bij de beeld- en meningsvorming. Dat dit gebeurt in een oorlog is niet nieuw, maar dankzij cyberspace (in dit geval de mogelijkheid dat 'ieder individu' zelf tekst, foto's en videobeelden kan maken, hergebruiken, vervalsen en online verspreiden) gaat dit tegenwoordig makkelijker, sneller, anoniemer, goedkoper en vooral heimelijker dan voorheen.

Hoe kunnen beïnvloedingsoperaties een rol spelen in het creëren van effecten zoals het veranderen van een mening, besluit en gedrag? Met een bepaalde intentie voor ogen, kiest een partij een strategisch narratief. Die overkoepelende verhaallijn wordt vervolgens geoperationaliseerd; opgesplitst in kleinere verhalen (frames). Framing heeft als doel het beoogde doelpubliek aan te zetten tot vooraf bepaalde beslissingen en acties die overeenkomen met wat de actor achter die beïnvloedingsoperatie wenst. Vooral sterk contrasterende waarden, normen en opvattingen zijn bij uitstek geschikt om tweespalt te creëren, of in stand te houden;[37] een ideaal concept in een gewapend conflict.

Volgens de 'gebruikelijke' verhaallijnen benadrukt de IDF het eigen gebruik van precisiewapens en het gebruik van burgers als menselijk schild door Hamas. Laatstgenoemde accentueert graag de menselijke ellende vanwege onophou-

33 N.n 'Hamas Attack on Israel: AP Photographer who accompanied terrorists wins award for clicking Shani Louk's half-naked body', *Organiser*, 29 maart 2024. Zie: https://organiser.org/2024/03/29/229969/world/hamas-attack-on-israel-ap-photographer-who-accompanied-terrorists-wins-award-for- clicking-shani-louks-half-naked-body/.

34 Veronica Neifakh, '4 Stages of Hamas' Psychological Warfare', *The Media Line*, 29 mei 2024. Zie: https://themedialine.org/top-stories/4-stages-of-hamas-psychological-warfare/.

35 Eric Cortellessa en Vera Bergengruen, 'Inside the Israel-hamas Information War', *Time Magazine*, 22 december 2023. Zie: https://time.com/6549544/israel-and-hamas-the-media-war/.

36 Het Centre of Gravity (zwaartepunt) is een militair concept dat verwijst naar de primaire bron waaraan een krijgsmacht zijn kracht ontleent om de strijd te kunnen voortzetten. De term is geïntroduceerd door Carl C. von Clausewitz in zijn werk *Vom Kriege (On War)*. Zie bijvoorbeeld M.E. Howard en P. Paret (red.), *On War* (Princeton University Press, 2008).

37 B.M.J. Pijpers en P.A.L. Ducheine, 'Influence Operations in Cyberspace – How They Really Work', Amsterdam Law School Research Paper No. 2020-61, Amsterdam Center for International Law No. 2020-31, 24 september 2020. Zie: https://ssrn.com/abstract=3698642.

delijke Israëlische aanvallen op Palestijnse burgers. Beelden die wreedheden en massale sterfgevallen tonen, worden evenwel vaak verspreid zonder de nodige context, waardoor het bijna onmogelijk is hun oorsprong te verifiëren. Aanhangers van beide zijden ge- of misbruiken moderne technologie en tonen, creëren, wijzigen en delen audio- en video-materiaal dat hun beweringen, frame en narratief moet ondersteunen.

Een dramatisch voorbeeld hiervan is de explosie nabij het Al-Ahli ziekenhuis waarbij naar verluidt honderden doden en gewonden vielen onder Palestijnse vluchtelingen die daar een veilig toevluchtsoord zochten. Hamas beschuldigde Israël en Israël beschuldigde Hamas.[38] Aanhangers van beide kanten brachten hun standpunten – en vermeend 'bewijsmateriaal' – via socialemediaplatforms naar voren om de publieke opinie en politieke beslissingen te beïnvloeden, waarbij ze dankbaar gebruikmaakten van de moeilijkheid om die bewijzen te weerleggen. Een vervalst bericht of gemanipuleerd beeld is, met dank aan kunstmatige intelligentie, tegenwoordig snel te maken. Bewijzen dat iets wel/niet authentiek is (factchecken), kost veel meer tijd. Dat dit uiteindelijk toch mogelijk is, bleek een maand na de explosie.[39]

Het gebruik van (sociale) media om de perceptie en besluitvorming van conflicten te beïnvloeden is geen noviteit, maar door dit conflict heeft deze vorm van digitale oorlogvoering wel een ongeëvenaard niveau bereikt in omvang en intensiteit. Dat geldt niet alleen voor real-time gegevens, maar ook voor bewust gemanipuleerde informatie. Met kunstmatige intelligentie gemaakte beelden hebben het potentieel om het vertrouwen van het publiek in *alle* verspreide informatie te ondermijnen. Wetende dat audio, video- en ander beeldmateriaal kan worden vervaardigd met computersoftware, kan zelfs authentiek materiaal al snel worden bestempeld als 'fake'. Het resultaat is een virtueel slagveld waar online polarisatie nieuw geweld kan aanwakkeren.[40]

Soms komen cyberaanvallen en digitale beïnvloedingsoperaties samen. Hackergroep *CyberAv3ngers* claimde een cyberaanval op een Israëlische energiecentrale en deelde foto's van de vermeende hack met daarbij een Palestijnse vlag en politieke boodschappen. Daarmee suggereerden de aanvallers dat deze computeraanval was uitgevoerd ter ondersteuning van de Palestijnse zaak. De gegevens waren echter afkomstig van een eerdere cyberaanval (2022); destijds uitgevoerd door een andere hackergroep en voor een ander doel.[41]

Meer dan twee strijdende partijen

Eind oktober 2023 waren 116 hackergroepen actief betrokken bij de cyberoorlogvoering tussen Hamas en Israël. Het merendeel (90) daarvan was pro-Palestijns, opereerde voornamelijk vanuit Azië en het Midden-Oosten en had aantoonbare religieuze motieven.[42] Opvallend is dat ook enkele beruchte pro-Russische hackergroepen zich achter Hamas zaak leken te scharen. Zij opereerden althans tegen Israël.[43] Dat land vond 23 hackergroepen aan zijn zijde. Drie hackergroepen bestempelden zichzelf als onpartijdig. Zij bestookten beide vechtende partijen.[44] Tegen het einde van 2023 steeg het aantal betrokken hackerscollectieven naar 133; het merendeel pro-Hamas.

38 Todd C. Helmus en William Marcellino, 'Lies, Misinformation Play Key Role in Israel-Hamas Fight', Rand Corporation, 31 oktober 2023. Zie: https://www.rand.org/blog/2023/10/lies-misinformation-play-key-role-in-israel-hamas-fight.html.

39 Amerikaanse en Franse inlichtingendiensten alsook onafhankelijke factcheckers van Associated Press kwamen tot de conclusie dat de explosie (waarschijnlijk) is veroorzaakt door een afgedwaalde raket, afgevuurd vanuit Gaza. Bron: Michael Biesecker, 'New AP analysis of last month's deadly Gaza hospital explosion rules out widely cited video', 22 november 2023. Zie https://apnews.com/article/israel-palestinians-hamas-war-hospital-rocket-gaza-e0fa550faa4678f024797b72132452e3.

40 P.W. Singer en Emerson T. Brooking, 'Gaza and the Future of Information Warfare. The Digital Front of the Israel-Hamas Conflict Is a Preview of Fights to Come', *Foreign Affairs*, 5 december 2023. Zie: https://www.foreignaffairs.com/middle-east/gaza-and-future-information-warfare.

41 N.n., 'A hack in hand is worth two in the bush', *Kaspersky SecureList*, 16 oktober 2023. Zie: https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/.

42 M. Sahariya, 'The Evolving Landscape of Cyber Warfare in the Israel-Palestine: A Comprehensive Analysis', *Falconfeeds*, 18 oktober 2023. Zie: https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis–356011.

43 Tanner Wagner, 'Escalation of Threats in the Middle East', CyberPeace Institute, 6 november 2023. Zie: https://cyberpeaceinstitute.org/news/escalation-of-threats-middle-east.

44 Jurgita Lapienytė, 'Hacktivists in Palestine and Israel after SCADA and other industrial control systems', *Cybernews*, 15 november 2023. Zie: https://cybernews.com/cyber-war/palestine-israel-scada-under-attack/.

FOTO U.S. CYBER COMMAND

Het U.S. Cyber Command is 'always in the fight'. Meerdere partijen houden zich op in de 'regionale cyberspace' in het Midden-Oosten, en van het U.S. Cyber Command is bekend dat het, sinds het oplaaien van het recente conflict, Israël actief steunt

Verschillende activistische hackergroepen benutten online communicatieplatforms, zoals Telegram, om medestanders te mobiliseren, specifieke doelwitten aan te wijzen en de kwetsbaarheden daarin te openbaren, alsook kwaadaardige softwareprogramma's te delen, waarmee anderen vervolgens cyberaanvallen kunnen uitvoeren.[45] In een poging de dreiging van dergelijke vijandige hackergroepen te neutraliseren, infiltreerde het Israëlische cybersecuritybedrijf Radware heimelijk in verscheidene (online) communities van Telegram. Medewerkers van het bedrijf deden zich voor als sympathisanten die zich wilden mengen in de strijd tegen Israël. Aldus verkreeg het bedrijf inzicht in aanvalsmethoden en technieken van deze hackers, en de rationale achter hun doelkeuzes. Door de kwaadaardige software te analyseren, konden potentiële slachtoffers tijdig worden voorzien van tegenmaatregelen.[46]

Het gezelschap dat zich toelegt op cyberoorlogvoering is behoorlijk divers en dat geldt ook voor het soort cyberaanvallen. Ideologisch gedreven activistische hackers gebruiken veelal vervelende, maar relatief onschadelijke DDoS-aanvallen, hack-and-leak-operaties en defacements, waarmee zij een politieke of religieuze boodschap afgeven. Aangezien de aanvallers doorgaans bewust de publiciteit zoeken om hun actie te claimen, worden dergelijke aanvallen snel ontdekt. Daarnaast zijn ze hierdoor vrij eenvoudig te attribueren aan een specifieke dader. Dit staat in schril contrast met meer substantiële, heimelijke cyberaanvallen, waarbij aanvallers trachten ontdekking van hun identiteit of achterliggende intenties te verhullen. Niet vreemd dus dat een deel van de pro-Palestijnse

45 Steve Emerson, 'An Analysis of the Israel-Palestine Conflict from a Cybersecurity Perspective, October 2023', *Medium*, 5 november 2023. Zie: https://blogs.crushingsecurity.com/an-analysis-of-the-israel-palestine-conflict-from-a-cybersecurity-perspective-october-2023-858c4c20f0ac.

46 Sara Miller, 'Infiltrating Anti-Israel Cyber Attackers To Hunt Their Targets & Tools', *NoCamels*, 23 november 2023. Zie: https://nocamels.com/2023/11/infiltrating-anti-israel-cyber-attackers-to-hunt-their-targets-tools/.

en pro-Israëlische cyberaanvallen niet is geclaimd door de aanvallers.

Hieruit zou je kunnen opmaken dat naast de activistische hackers nog een ander type aanvaller actief is: statelijke of staatsgesteunde actoren (APT's).[47] In het huidige conflict zouden aan Hamas, Hezbollah of Iran gelieerde APT's zich goed kunnen voordoen als activistische hackergroepen en zich met de (cyber)strijd in Gaza kunnen bemoeien om hun identiteit en werkelijke intenties te verhullen.[48] Daarnaast is het echter ook mogelijk dat andere landen zich heimelijk ophouden in de 'regionale cyberspace'. Hetzij om inlichtingen te vergaren, hetzij om een van de strijdende partijen actief te steunen (defensief en/of offensief). Van het U.S. Cyber Command is bekend dat het, sinds het oplaaien van het recente conflict, Israël actief steunt op dit gebied.[49]

Ook de technologisch geavanceerde, pro-Israëlische hackergroep *Predatory Sparrow* is opgedoken in het huidige cyberconflict. Deze actor, waarschijnlijk gelieerd aan de Israëlische overheid, heeft in het verleden naar verluidt verschillende destructieve en spraakmakende cyberaanvallen uitgevoerd in Iran.[50] De groep, vermoedelijk verantwoordelijk voor een cyberaanval op het Iraanse spoorwegennetwerk in 2021, en op een staalfabriek in 2022, beweerde dit keer de website van het Iraanse overheidsnieuwsagentschap ontoegankelijk te hebben gemaakt; op zijn minst tijdelijk.[51] Meerdere Israëlische (tech)bedrijven spannen zich overigens in op zoek naar aanwijzingen over het lot van de Israëlische gijzelaars en hun verblijfplaats.[52] Ook de Israëlische *NSO Group Technologies* is actief op dit gebied.

Het pro-Israëlische hackerscollectief *WeRedEvils* claimde het Iraanse elektriciteitsnet en kernreactoren te hebben gehackt, alsook faciliteiten van de Iraanse Revolutionaire Garde en de Iraanse website *Tasnim News*. Hoewel Iran geen stroomstoringen meldde, deelden de aanvallers een uitgebreide verzameling bestanden inzake de genoemde digitale inbraken. Dezelfde groep zou daarnaast verantwoordelijk zijn voor een cyberaanval op het pro-Hamas Telegram-kanaal *GazaNow*.[53]

Opvallende afwezigen in de eerste dagen van dit cyberconflict waren de notoire hackergroepen van de Iraanse veiligheidsdiensten en de Revolutionaire Garde. De vraag daarbij is of Teheran zich bewust afzijdig hield van dit cyberconflict, of dat zijn cybereenheden simpelweg niet waren voorbereid op de inzet van cyberwapens ter ondersteuning van Hamas' inval. Iraanse operators leken initieel vooral reactief te zijn. Dat wil zeggen, zij gebruikten reeds aanwezige toegang tot systemen van hun slachtoffers, alsook bestaande digitale infrastructuur en middelen. Pas elf dagen na de fysieke inval van Hamas werden twee afzonderlijke cyberaanvallen vanuit Iran waargenomen. Beide gericht tegen Israëlische infrastructuur en met een destructief oogmerk. Deze incidenten hadden weliswaar slechts beperkte (bewezen) effecten, maar de aanvallers trachtten via online beïnvloedingsoperaties het succes en de impact van beide aanvallen uit te vergroten.[54]

47 Een Advanced Persistent Threat (APT) is een dreiging die wordt gevormd door een hackerscollectief met uiteenlopende specialismen. Een dergelijke groep is vaak in staat om ongemerkt een computersysteem of -netwerk binnen te dringen en daar een langere periode ongemerkt te blijven om informatie te verzamelen. De meeste van dit soort groepen betreffen statelijke, staatsgesteunde, of staats-gedoogde (criminele) actoren die tot doel hebben andere regeringen te ondermijnen.

48 Tom Hegel en Aleksandar Milenkoski, 'The Israel-Hamas War |Cyber Domain State-Sponsored Activity of Interest', *SentinelOne*, 24 oktober 2023. Zie: https://www.sentinelone.com/labs/the-israel-hamas-war-cyber-domain-state-sponsored-activity-of-interest/.

49 General Timothy D. Haugh, Commander U.S. Cyber Command, 'Posture Statement of Timothy D. Haugh 2024', 12 april 2024. See: https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/.

50 Farnaz Fassihi en Ronen Bergman, 'Israel and Iran Broaden Cyberwar to attack Civilian Targets', *The New York Times*, 27 november 2021. Zie: https://archive.ph/30DGG.

51 AJ Vicens, 'Savvy Israel-linked hacking group re-emerges amid Gaza fighting', *CyberScoop*, 10 oktober 2023. Zie: https://cyberscoop.com/predatory-sparrow-israel-gaza-cyber/.

52 David Swan, 'Cyber Intelligence Report 10 – 23 November 2023', CSCIS (Centre for Strategic Cyberspace & International Studies), 23 november 2023. Zie: https://cscis.org/2023/11/24/cyberwarfare-how-russia-hacked-denmark/.

53 David Israel, 'Israeli Hackers Claim They Shut Down Revolutionary Guards' Nuclear Projects', *The Jewish Press*, 24 oktober 2023. Zie: https://www.jewishpress.com/news/middle-east/iran-news/israeli-hackers-claim-they-shut-down-revolutionary-guards-nuclear-projects/2023/10/24/.

54 N.n., 'Reactive and opportunistic: Iran's role in the Israel-Hamas war', *Microsoft Threat Intelligence blog*, 9 november 2023. Zie: https://www.microsoft.com/en-us/security/blog/2023/11/09/microsoft-shares-threat-intelligence-at-cyberwarcon-2023/.

Een van de hackergroepen lijkt sterk verbonden aan de Iraanse APT *Agonizing Serpens*. Deze groep richt zijn kwaadaardige software (malware) voornamelijk op Israëlische doelwitten in uiteenlopende industrieën en verschillende landen.[55] De aanvallers maakten voor hun destructieve cyberwapen gebruik van één oude en drie nieuwe wiperware-versies, om data én computers van hun slachtoffers permanent te vernietigen. Behalve meerdere wiperware-varianten gebruikten de hackers ook stealth en andere technieken om (cyber)verdedigings-maatregelen te omzeilen, ongemerkt te opereren en hun eigen digitale sporen uit te wissen. Hoewel de aanvallen (tijdig) zijn onderkend, toont dit de toegenomen capaciteit van deze aanvallers.

Naarmate het conflict voortduurt, willen Iraanse partijen wellicht een pro-actievere houding aannemen. Echter, het doelkeuzeproces en het verkrijgen van toegang tot specifieke doelwitten vergt doorgaans veel tijd. Om ongemerkt een computernetwerk binnen te dringen en daar gedurende langere tijd ongemerkt te verblijven (bijvoorbeeld om inlichtingen te verzamelen), is specifiek ontwikkelde (tailored to the mission) software nodig. Aangezien die software specifiek wordt afgestemd op een bepaald doelwit, heeft die een beperkte herbruikbaarheid wat betreft inzet tegen willekeurige andere doelwitten. Dit maakt dat specifieke intelligence gathering-software minder geschikt is om snel om te bouwen naar tactisch of operationeel bruikbare cyberwapens die kunnen worden ingezet tegen verschillende doelwitten.

Geopolitiek cyberconflict

Hoewel de naam anders doet vermoeden, is hackerscollectief *Anonymous Sudan* geen onder-afdeling van het activistische hackerscollectief *Anonymous*, en evenmin Sudanees. Het betreft vermoedelijk een groep die nauwe banden onderhoudt met Rusland.[56] Binnen een uur na de initiële raketaanvallen van Hamas op Israël voerde de groep samen met hackers van *AnonGhost* cyberaanvallen uit. Ze claimden daarbij Israëls Iron Dome-luchtverdedigings-systeem te hebben gecompromitteerd, evenals Israëls RedAlert-raketwaarschuwings-programma; een app die voornamelijk burgers voorziet van real-time gegevens over inkomende raketten.[57] Een van de gevolgen was dat gebruikers van de RedAlert-app valse berichten ontvingen over nucleaire wapens. De makers van de RedAlert-app werden gelijktijdig bestookt met DDoS-aanvallen, waardoor de producent voor langere tijd online onbereikbaar was. Een andere pro-Russische hackergroep (*KillNet*) richtte zich, uit wraak voor Israëls steun aan Oekraïne, op Israëlische overheidswebsites en financiële instellingen.[58]

In tegenstelling tot het kinetisch gevecht dat zich beperkt tot een specifieke geografische regio, vindt de conflict-gerelateerde cyber-oorlogsvoering ook elders plaats. Aanvallers en slachtoffers bevinden zich (ver) buiten de conflictzone. Meerdere hackergroepen richtten hun pijlen op derde landen (zoals de VS, India en Frankrijk), voornamelijk als reactie op de steun van die landen aan Israël. Hackergroep *CyberAv3ngers,* gelieerd aan de Iraanse Revolutionaire Garde, viel meerdere (civiele) Industriële Controle Systemen (ICS) aan; systemen die veelal onderdeel zijn van de vitale infrastructuur van een land. *CyberAv3ngers* claimde tevens, deels terecht, deels gefingeerd, cyberaanvallen op verscheidene Israëlische industriële sectoren (water, energie, scheepvaart en logistiek). Diezelfde groep viel bovendien drinkwatervoor-zienings- en waterzuiveringsinstallaties aan in meerdere Amerikaanse staten. De aanvaller legitimeerde die aanvallen met de quote 'Every Equipment "Made in Israel" is Cyber Av3ngers Legal Target!'[59] Een korte zoekslag op internet leert overigens dat het specifiek aangevallen

55 Or Chechik, Tom Fakterman, Daniel Frank en Assaf Dahan, 'Agonizing Serpens (Aka Agrius) Targeting the Israeli Higher Education and Tech Sectors', *Palo Alto Unit 42*, 6 november 2023. Zie: https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/.

56 Vilius Petkauskas, 'Anonymous Sudan: neither anonymous nor Sudanese', *Cybernews*, 23 june 2023. Zie: https://cybernews.com/editorial/anonymous-sudan-explained/.

57 M. Sahariya, 'The Evolving Landscape of Cyber Warfare in the Israel-Palestine'.

58 Ryan Gallagher en Jordan Robertson, 'Cyberattacks Targeting Israel Are Rising After Hamas Assault', *Time Magazine,* 10 oktober 1023. Zie: https://time.com/6322175/israel-hamas-cyberattacks-hackers/.

59 Zie: https://twitter.com/CyberAveng3rs/status/1728743948246569469.

Israëlische computeronderdeel voorkomt in nog eens 1800 apparaten wereldwijd;[60] alle dus potentieel doelwit.

Volgens het Israëlische Nationale Cyberdirectoraat (INCD) hebben meer dan vijftien, aan Iran en Hezbollah gelieerde, statelijke en staatsgesteunde hackergroepen cyberaanvallen uitgevoerd op Israëls vitale diensten en infrastructuur. Het INCD constateerde dat tegenstanders ook verscheidene doelgroepen (waaronder anti-Israëlische activisten) aanspoorden om cyberaanvallen op Israël uit te voeren door hen te voorzien van specifieke doelwitten alsook de benodigde middelen voor bijvoorbeeld DDoS-aanvallen; ook te gebruiken zonder technische kennis.[61] Het aantal cyberaanvallen op Israël is sinds 7 oktober verdrievoudigd, mede doordat Iran en zijn proxies (waaronder Hezbollah) hun inspanningen coördineerden. Dat de aanvallen weinig schade aanrichtten, dankt Israël naar eigen zeggen aan zijn proactieve cyberdefensie. Deze aanpak ontleende het land aan de bevindingen in de cyberoorlogvoering tussen Rusland en Oekraïne. De aldaar geleerde lessen betreffen voornamelijk een intensieve samenwerking met industriële en internationale partners, het delen van cyberdreigingsinformatie en voorzorgsmaatregelen tegen dreigende cyberaanvallen.[62]

Ook pro-Israëlische hackers opereren over de grens. Vermoedelijk in reactie op de Iraanse bemoeienis met het conflict voerde hackergroep *Predatory Sparrow* een cyberaanval uit op Iraanse benzinestations waardoor zo'n 70 procent daarvan (tijdelijk) niet meer werkte.[63] Iran kreeg twee jaar eerder een soortgelijke cyberaanval op de brandstofvoorziening te verduren; destijds vermoedelijk uitgevoerd door hackers vanuit Israël en de VS.

Het Gaza-conflict lijkt daarmee onderdeel van een grotere machtsstrijd om invloed in het Midden-Oosten en het streven naar een multipolaire wereld met meerdere machtsblokken. Daarbij spelen ook andere dan rechtstreeks betrokken partijen een rol, zoals China[64] en Rusland.[65]

Conclusie

Sinds 2009 maken Hamas en Israël gebruik van sociale media om hun strijd ook online uit te vechten. Tot 2014 beperkte de cyberoorlog zich voornamelijk tot digitale beïnvloeding (soft cyberoperaties). Vanaf dat jaar richtten aanhangers van beide zijdes zich ook op het hacken van computers (hard cyberoperaties), al richtten die cyberaanvallen (voor zover momenteel te achterhalen) slechts beperkte, herstelbare schade aan. Hamas bleek zich de afgelopen jaren vooral te hebben bekwaamd in cyberspionage om zich voor te bereiden op '7 oktober'. Tot die datum was de Israëlische perceptie dat Hamas, in vergelijking met Rusland of China, geen serieuze cyber- of inlichtingendreiging vormde. Dit was een pijnlijke inschattingsfout. Een sterk gedigitaliseerde staat kan online onconventioneel worden bevochten en ondermijnd zonder daar adequate maatregelen tegenover te kunnen stellen.

In het huidige conflict heeft cyberoorlogvoering door (aanhangers van) beide strijdende partijen, voor zover bekend, nog geen doorslaggevende rol gespeeld. Duidelijk is wel dat de virtuele oorlogvoering ook, of juist, plaatsvindt *buiten* het specifieke gebied waar de grootste fysieke schade wordt aangericht. De meeste aanvallers én slachtoffers van cyberaanvallen bevinden zich juist buiten Gaza.

60 Het aangevallen onderdeel betrof een Programmable Logic Controller (PLC) van het Israëlische bedrijf Unitronics. Een PLC is een microcomputer die industriële machines en processen aanstuurt. Pierluigi Paganini, 'Iranian hacker group Cyber Av3ngers hacked the Municipal Water Authority of Aliquippa in Pennsylvania', *Security Affairs*, 27 november 2023. Zie: https://securityaffairs.com/154818/hacktivism/cyber-av3ngers-hacked-municipal-water-authority-of-aliquippa.html.

61 INCD, 'Iron Swords' War in Cyber Sphere', 5.

62 Wechsler, 'The Cyberwarfare Front of the Israel-Gaza War'.

63 N.n, 'Iran petrol stations hit by cyberattack, oil minister says', *Reuters*, 18 december 2023. Zie: https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/.

64 National Contagion Research Institute, 'A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives', *Intelligence Report*, december 2023.

65 Maria Shamrai, 'How Russia uses the Israel-Gaza Crisis in its disinformation campaign against the West', International Centre for Counter-Terrorism (ICCT), 8 december 2023. Zie: https://www.icct.nl/publication/how-russia-uses-israel-gaza-crisis-its-disinformation-campaign-against-west.

FOTO ANP ATEF SAFADI

Israëls luchtverdedigingssysteem Iron Dome in actie. Een hackergroep claimde Iron Dome en de waarschuwingsapp RedAlert te hebben gecompromitteerd

Het hacken van computersystemen speelt een ondersteunende rol in deze strijd. Het beïnvloeden van de publieke opinie en politieke besluitvormers lijkt een cruciale rol te spelen. Dankzij moderne technologie (sociale media in combinatie met kunstmatige intelligentie) kan informatie over de strijd niet alleen eenvoudig worden gemaakt en verspreid, maar ook hergebruikt of ronduit vervalst. Het Centre of Gravity lijkt voor beide strijdende partijen de internationale steun te zijn. Burgerslachtoffers zijn een luguber middel in de strijd om perceptie.

Twee op het eerste gezicht niet-gerelateerde conflicten (Rusland-Oekraïne en Hamas-Israël) zijn in zeker opzicht toch met elkaar verbonden dankzij Iran. Rusland ontvangt wapens (zoals drones) en munitie vanuit dat land en levert in ruil daarvoor digitale capaciteiten, die Iran inzet om de Palestijnse zaak via cyberoorlogvoering te beïnvloeden.

Rusland ontwikkelde meerdere destructieve cyberwapens (wiperware) die het inzette tegen Oekraïne. Gaandeweg konden Russische hackers bestaande wiperware snel modificeren, verbeteren en inzetten tegen nieuwe doelwitten. Als het Gaza-conflict voortduurt, zou ook Iran nieuwe, meer agressieve cyberwapens kunnen ontwikkelen en inzetten tegen Israël of zijn bondgenoten.

Online activisme kan een bruikbare dekmantel vormen. Irans statelijke of staatsgesteunde cybergroepen kunnen cyberaanvallen uitvoeren zonder eenvoudig als dader te worden herkend. Dergelijke cyberaanvallen zullen dit kinetisch reeds geëscaleerde conflict waarschijnlijk niet verder doen verslechteren en evenmin zullen cyberwapens de doorslaggevende factor vormen in de strijd.

Door zich actief te mengen in deze cyberstrijd kunnen andere landen niet alleen een van beide strijdende partijen van dienst zijn, maar bovenal hun eigen geopolitieke strategische doelen nastreven. Als de fysieke strijd rond Gaza eenmaal is geluwd, zal het cyberconflict ongetwijfeld voortduren. Verscheidene landen zullen in een constant (cyber)conflict met elkaar verwikkeld blijven. ■

De theorie van Biddle en de oorlog in Oekraïne

Het moderne systeem van militair optreden

Luitenant-kolonel drs. Carel Sellmeijer*

Komen de denkbeelden van de Nederlandse krijgsmacht over toekomstig landoptreden overeen met de werkelijkheid van militaire operaties in Oekraïne? Een van de invalshoeken om die vraag te beantwoorden is de theorie van Stephen Biddle over het moderne systeem van militair optreden. Biddle raakte in de jaren 80 gefascineerd door het debat over de Revolution in Military Affairs, dat onder meer draaide om het belang van technologie voor de uitkomst van oorlogen. Hij begon te schrijven over de discrepantie die hij zag tussen zijn werk als analist in het Pentagon, met een focus op de hardware van oorlogvoering, en de boeken die hij las over oorlogvoering; de literatuur wees juist op het belang van strategie en persoonlijkheden. Biddle stelt dat de kern van de oplossing voor het probleem van het militaire optreden op het letale gevechtsveld vooral ligt in de doctrine en tactieken en niet zozeer in technologie of numeriek overwicht.

In de moderne landoorlog is de vuurkracht dermate dodelijk dat openlijke troepenbewegingen suïcidaal zijn

FOTO MCD, AARON ZWAAL

In Oekraïne, op ruim 2500 kilometer van het hoofdkwartier van het Commando Landstrijdkrachten in Utrecht, woedt al meer dan twee jaar een oorlog die duidelijk maakt wat er gebeurt als twee moderne krijgsmachten de strijd aangaan. Dit levert regelmatig verschrikkelijke beelden uit het conflictgebied op, maar de landoorlog biedt professionals ook de mogelijkheid om ervan te leren. Dit kan op velerlei manieren. Eén daarvan is om te onderzoeken of onze denkbeelden over het toekomstige landoptreden stroken met de huidige werkelijkheid door krijgswetenschappelijke theorieën te toetsen aan militaire operaties in Oekraïne. In dit artikel toets ik de theorie van Stephen Biddle over het moderne systeem van militair optreden. Biddle zocht een antwoord op de vraag of het op het hedendaagse gevechtsveld nog mogelijk is om een betekenisvolle landoperatie uit te voeren. Als casuïstiek analyseer ik de twee offensieven door het Oekraïense leger bij Charkov en Cherson in het eerste oorlogsjaar. Tevens geef ik aan welke conclusies Biddle zelf trekt uit de gevechten in Oekraïne in recent gepubliceerde artikelen. Vervolgens worden op basis van de toetsing van de theorie van Biddle enkele conclusies getrokken.

De theorie van Biddle

Stephen Biddle (1959) is een 'product' van de Amerikaanse onderzoekstraditie die met een kwantitatieve onderbouwing oorlogvoering wil verklaren. Biddle is politiek-analist en historicus. Momenteel is hij als hoogleraar verbonden aan Columbia University en senior fellow voor defensiepolitiek bij de Amerikaanse denktank Council on Foreign Relations. Zijn publicaties behandelen een breed spectrum aan onderwerpen over de recente Amerikaanse defensiepolitiek en militaire inzet. De Amerikaanse inbreng in Irak en Afghanistan kreeg Biddle uit eerste hand mee door zijn deelname in de assessmentteams van generaal David Petraeus in Bagdad in 2007 en generaal Stanley McChrystal in Kabul in 2009.

Biddle vond zijn motivatie om onderzoek te doen in het debat over de Revolution in Military Affairs in de jaren 80, dat onder meer draaide om het belang van technologie voor de uitkomst van oorlogen. Biddle ervoer een discrepantie tussen zijn werk als analist in het Pentagon, met een focus op de hardware van oorlogvoering, en de boeken die hij las over oorlogvoering; de literatuur wees juist op het belang van strategie en persoonlijkheden, oftewel de software van oorlogen. Aangezien de Amerikaanse samenleving geobsedeerd is door technologie, is er altijd de verwachting dat een nieuw *gadget* een grote verandering in oorlogvoeren zal betekenen. Biddle concludeert echter dat techniek belangrijk is, maar dat tactieken en doctrine uiteindelijk de uitkomst van militaire oorlogvoering bepalen.

In zijn bekroonde boek *Military Power* uit 2004, waarin hij zijn theorie van het *modern system* introduceert, onderzoekt Biddle de invloed van numerieke overmacht, techniek en inzetstrategieën op het landoptreden.[1] Met behulp van formules en grafieken toont hij de onderlinge verbanden tussen de afhankelijke variabelen (campagneduur, terreinwinst en slachtoffers) als functie van de onafhankelijke variabelen (numeriek overwicht, technologie en inzet van eenheden) in 56 militaire operaties in de twintigste eeuw. Zijn conclusie is dat een modern systeem van militair optreden de gevolgen van technologische verandering dempt en bescherming biedt tegen de enorme vernietigingskracht en letaliteit van de vijandelijke wapensystemen. Het moderne systeem is een bepaald patroon van militaire inzet van 'cover, concealment, dispersion, suppression, small-unit independent maneuver, and combined arms at the tactical level, and depth, reserves, and differential concentration at the operational level of war'. Tezamen reduceren deze technieken van inzet de kwetsbaarheid voor de sensor- en wapentechnologie.[2]

* Carel Sellmeijer is sinds 2013 verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie. Met dank aan Han Bouwmeester, Peter Pijpers en Willem Verweij voor de feedback op eerdere versies van dit artikel.

1 Stephen Biddle, *Military Power. Explaining Victory and Defeat in Modern Battle* (Princeton, Princeton University Press, 2004).

2 Idem, 3. Hoofdstuk 3 is gewijd aan de uitleg over het moderne systeem.

Het probleem dat door de technologische ontwikkelingen in de moderne landoorlog moet worden opgelost, is dat de vuurkracht dermate dodelijk is dat openlijke troepenbewegingen suïcidaal zijn. De drie voornaamste effecten van technologische veranderingen na 1900 zijn: verbetering van het bereik, de vuuruitwerking en de precisie van wapens; grotere mobiliteit over grotere afstanden; en vergroting van de mogelijkheden tot observatie, surveillance, communicatie en verwerking van informatie. De optelsom van deze drie effecten betekent een toenemende letaliteit op het moderne gevechtsveld. Om nog betekenisvolle militaire operaties te kunnen uitvoeren in deze zogeheten *storm of steel* is het volgens Biddle vooral zaak om de blootstelling te reduceren door het toepassen van het moderne systeem. Het schermt de verdediger en de aanvaller af van de ergste effecten van wapens en van detectie door sensoren, maar implementatie van het moderne systeem kost veel tijd en capaciteit.[3]

De strategieën voor de strijdende partijen die Biddle heeft onderzocht zijn combinaties van de diepte in de verdediging, de inzet van de reserve-eenheden, de snelheid van de strijdende partijen,[4] en het verschil in technologische ontwikkeling. Als bijvoorbeeld de verdediger de snelheid van de reserve-eenheden naar beneden bijstelt, dan vermindert dat de kwetsbaarheid tijdens de verplaatsingen en resulteert dit in beperkte terreinwinst voor de aanvallende partij. Op basis van dit soort verbanden concludeert Biddle dat een verdediger die het moderne systeem hanteert in staat is om een doorbraak van een numeriek sterkere en technologisch superieure aanvaller te weerstaan.[5]

Het toepassen van het moderne systeem om de gevolgen van de hedendaagse wapentechnologie te verminderen is onderdeel van een palet aan *trade-offs*.[6] Moderne wapens dwingen beide partijen te vertragen en dekking te zoeken om te overleven. Als beide partijen het moderne systeem implementeren, dan hebben technologische veranderingen volgens Biddles onderzoek minder effect op het militair vermogen: er is dan weinig verandering in de dimensies terreinwinst en aantallen slachtoffers, behalve de campagneduur. Maar fouten van de partij die het moderne systeem niet toepast worden harder afgestraft. Een voorbeeld is de vernietiging aan het begin van de invasie in februari 2022 van Russische konvooien, die door een gebrek aan infanterie en flankbeveiliging kwetsbaar waren voor Oekraïense precisievuren en kleine, mobiele aanvalsteams bewapend met moderne antitankwapens. Technologie versterkt in zulke gevallen de gevolgen van (gewelds)inzet en werkt als katalysator.[7]

FOTO COUNCIL ON FOREIGN RELATIONS

Volgens Stephen Biddle zal de toenemende complexiteit van wapensystemen een kloof veroorzaken tussen krijgsmachten die daar wel of niet mee kunnen omgaan

3 Idem, 53-66.
4 Met snelheid wordt bedoeld de nettosnelheid die eenheden nodig hebben om hun doel te bereiken, inclusief planning, commandovoering, verkenning, *rehearsals*, vuurvoorbereiding en dergelijke.
5 Biddle, *Military Power*, 220-239.
6 De belangrijkste trade-offs zijn: aanval en verdediging; manoeuvre en attritie; spreiding en concentratie; diepte en voorwaartse ontplooiing; centralisatie en decentralisatie. Christopher Tuck, 'Land Warfare', in: David Jordan e.a., *Understanding Modern Warfare* (Cambridge, Cambridge University Press, 2009) 75-80.
7 Biddle, *Military Power*, 73-77.

De maatregelen om blootstelling tegen de moderne wapensystemen te reduceren zijn vaak lastig te implementeren door de toenemende verfijning en complexiteit van deze systemen. Er zal volgens Biddle een kloof ontstaan tussen militaire organisaties die wel of niet met deze complexiteit kunnen omgaan.[8] Als een krijgsmacht niet in staat is om het moderne systeem te implementeren neemt de kwetsbaarheid voor de toegenomen vuurkracht exponentieel toe.

Kortom, volgens het onderzoek van Biddle ligt de oplossing van het probleem omtrent de toegenomen letaliteit meer in de wijze van inzet van de krijgsmacht dan in technologie of numeriek overwicht. Door het toepassen van het moderne systeem reduceert een krijgsmacht de blootstelling aan de moderne wapentechnologie. Met het voortschrijden van de (wapen)techniek wordt het gevechtsveld dodelijker en wordt steeds een balans gezocht tussen de conflicterende eisen van overleven en snelheid in het optreden. De focus op hightech-oplossingen alleen is volgens Biddles onderzoek geen garantie voor succes in de moderne oorlogvoering. De factor materieel als onderdeel van het militair vermogen is sinds 1900 geen betrouwbare voorspeller van de uiteindelijke militaire resultaten in oorlogvoering gebleken.[9]

Tot slot geeft Biddle aan dat de aangetoonde stabiele aard van de relaties tussen technologie, numeriek overwicht, doctrine en tactieken sinds 1900 geen eeuwigheidswaarde heeft. Het moderne systeem was een antwoord op een specifiek geheel van technologische veranderingen in de tweede helft van de 19e eeuw. Dit kan door vergelijkbare ingrijpende technologische veranderingen in de 21e eeuw veranderen. Met betrekking tot de landoorlog wijzigt het verband tussen techniek, numeriek overwicht en inzet als het terrein transparant wordt, doordat alle bewegingen kunnen worden waargenomen en bestreden met precisievuur. Het gebruik van het terrein als onderdeel van het vechten op land wordt dan minder relevant, de huidige wijze van inzet van landeenheden verliest haar waarde en de superieure techniek wordt dominant voor oorlogvoering op het land.[10]

Wat gebeurt er als de casuïstiek van de Oekraïne-oorlog, met specifiek de twee offensieven bij Charkov en Cherson in de tweede helft van 2022, langs het hiervoor beschreven theoretische raamwerk van Biddle wordt gelegd?[11]

Tegenoffensief Oekraïne bij Charkov (6 september-2 oktober 2022)

In de zomer van 2022 werd een Oekraïens tegenoffensief gepland in de *oblast* Charkov. Het Oekraïense leger wilde namelijk gebruik maken van inlichtingen over de uitgedunde Russische verdediging in deze regio. Het voornaamste Russische militaire probleem was niet de schade in het achtergebied door de voorafgaande bombardementen met precisiewapens, maar kwantitatief en kwalitatief onvoldoende frontbezetting, onvoldoende reserve-eenheden, en een gebrek aan capaciteit om de uitgeputte eenheden te roteren. De voorafgaande maandenlange slijtageslag sinds de Russische inval, gecombineerd met de berichten over verwachte Oekraïense aanvallen in het zuiden bij Cherson, dwong de Russische legerleiding om te kiezen tussen het versterken van de regio Charkov en het verdedigen van Cherson.[12] Hoewel de Oekraïense troepenopbouw in de omgeving van

8 Stephen Biddle, 'The past as prologue. Assessing theories of future warfare', *Security Studies*, Vol. 8, No. 1 (1998) 12.

9 In het denkmodel over militair vermogen wordt de fysieke component gecomplementeerd door de conceptuele en mentale component. Zie: *Nederlandse Defensiedoctrine* (Den Haag, ministerie van Defensie, 2019) 66-73.

10 Admiraal buiten dienst Owen gaf in 1995 aan dat we op een kantelpunt waren aangekomen in de moderne oorlogvoering. Biddle verwacht deze paradigmaverschuiving niet in de komende decennia doordat bijvoorbeeld nieuwe sensortypes nog volop in ontwikkeling zijn, door problemen met interferentie en nevenschade in verstedelijkt gebied, en door de ontwikkelingen van tegenmaatregelen bij de grootschalige inzet van drones. Zie: Biddle, *Military Power*, 72-73.

11 De informatie over de twee offensieven komt voornamelijk van de website van het *Institute for the Study of War* (https://www.understandingwar.org) en het artikel van Isabelle Khurshudyan e.a, 'Inside the Ukraine counteroffensive that shocked Putin and reshaped the war', *Washington Post* (29 december 2022). Zie: https://www.washingtonpost.com/world/2022/12/29/ukraine-offensive-kharkiv-kherson-donetsk/.

12 Franz-Stefan Gady en Michael Kofman, 'Ukraine's Strategy of Attrition', *Survival*, Vol. 65, No. 2 (2023) 10.

Charkov in juli en augustus kon worden waargenomen, werden de betere Russische grondeenheden verplaatst naar de regio's Cherson en Zaporizja. Dit betekende een succes voor de Oekraïense misleidingsstrategie, een voortzetting van de Sovjet-*maskirovka*-doctrine in het Oekraïense militaire denken, waarbij generaal Oleksandr Syrsky Cherson wilde gebruiken als gedeeltelijke afleidingsmanoeuvre voor een tegenoffensief in de omgeving van Charkov.[13]

Een Oekraïense aanvalsmacht overschreed de frontlinie op 6 september. Er was gekozen voor twee aanvalsrichtingen om de Russische troepen te splitsen: een aanvalsmacht in noordelijke richting naar Koepiansk en in zuidelijke richting naar Izijoem. Het lukte met een troepenconcentratie nabij Prisjib op 9 september een doorbraak op een smal front te forceren. Daarop volgde een snelle opmars waarbij gebruik werd gemaakt van de dekkingsmogelijkheden in het terrein. Kleine zelfstandig optredende Oekraïense eenheden slaagden erin de Russische stellingen te omtrekken en door te stoten in de diepte van de Russische verdediging. Oekraïense brigades zetten drones in, zodat zij zelf nauwkeurig doelen konden bepalen en bestrijden en de opmarssnelheid behouden. Voor de Oekraïense aanvalsmacht was snelheid essentieel om te voorkomen dat Russische reserve-eenheden vanuit de omgeving Belgorod in Rusland konden worden ingezet.[14]

De Russische verdediging in de omgeving Charkov was ondiep, de inzet van reserves was niet goed afgestemd en de benodigde vuursteun bleef uit. In de doorbraaksector was een onsamenhangende mix van Russische eenheden en gemobiliseerde separatistische proxy's uit Loegansk aanwezig. Door het Oekraïense optreden brak er paniek uit in de Russische verdediging. Zij hadden moeite om samenhang in de verdediging te handhaven, boden weinig weerstand en verlieten uiteindelijk het gebied met achterlating van grote hoeveelheden materieel: 'The Russian troops had everything they needed for a serious defense, except the will to fight and, apparently, enough men', aldus Isabelle Khurshudyan.[15]

De voortschrijdende (wapen)techniek maakt het gevechtsveld dodelijker en noodzaakt tot het zoeken van een balans tussen de conflicterende eisen van overleven en snelheid in optreden

De verandering in de wijze van inzet keerde het tij. Een nieuwe Russische operationele commandant herstelde de controle over de eenheden, voerde een vertragend gevecht met de aanwezige Russische eenheden en liet verder naar het oosten nieuwe verdedigende linies langs de rivieren Oskil en Krasna voorbereiden. Vooral het gebrek aan Russische reserve-eenheden in het gebied leidde ertoe dat hij niet op tijd de verdediging kon versterken en tegenaanvallen uit kon voeren om de doorbraak te beperken.

Na enkele weken liep de Oekraïense opmars vast in massale Russische vuursteun en de Oekraïense bereidheid om verder te vechten nam af. Het Oekraïense tegenoffensief culmineerde in de herovering van de stad Lyman op 1 oktober. In nauwelijks een maand tijd was een aanvalsdiepte bereikt van ongeveer 90 kilometer. De *force-to-space* ratio aan Russische zijde in de omgeving van Charkov met uitgeputte, gesleten en ad-hoc samengestelde eenheden waar samenhang ontbrak, verhinderde dat de Russische eenheden een effectieve verdediging volgens het moderne systeem konden voeren en gaven de Oekraïense eenheden gelegenheid een succesvolle offensieve manoeuvre uit te voeren.

13 Viktoriya Fedorchak, *The Russia-Ukraine War. Towards Resilient Fighting Power* (Londen, Routledge, 2024) 87-88.
14 Idem, 88-89.
15 Khurshudyan, 'Inside the Ukraine counteroffensive'.

De snelle Oekraïense opmars en de falende Russische verdediging in de omgeving van Charkov bevestigen de theorie van Biddle. Het Oekraïense optreden was gericht op kleine, zelfstandig opererende eenheden, uitgerust met middelen voor de integratie van land- en luchtcapaciteiten. Na de doorbraak slaagden zij erin om hoge snelheden te ontwikkelen door verkenning en vuurvoorbereiding tijdens de opmars te coördineren in combinatie met drones, satellietbeelden en precisievuren. Snelheden van honderd kilometer per dag vereisen van de aanvaller volledige blootstelling zonder vuurvoorbereiding en met minimale verkenning. Maar deze blootstelling compenseerde Oekraïne door gebruik te maken van dekkingsmogelijkheden in het terrein, de integratie van communicatiesystemen, precisie-artillerie en bijna onafgebroken surveillance van het gevechtsveld door de grootschalige inzet van drones. Het Oekraïense offensief werd geholpen doordat er paniek uitbrak en Russische eenheden op de vlucht sloegen. Dit zorgde ervoor dat Oekraïense eenheden in deze sector 60.000 vierkante kilometer terreinwinst konden boeken.

Tegenoffensief Oekraïne nabij Cherson (29 augustus-11 november 2022)

Hoe anders verliep het Oekraïense tegenoffensief in de omgeving van Cherson dat in hetzelfde najaar van 2022 plaatsvond. Het Oekraïense leger zette in op een beperkte campagne met de focus op de stad Cherson. Vanaf eind augustus rukten Oekraïense eenheden langs drie assen op om Russische eenheden te omtrekken. De initiële penetratie kwam door felle tegenstand al snel tot stilstand. Het terrein bood door de open velden weinig dekkingsmogelijkheden voor de aanvallende troepen. Daarnaast vormden de vele irrigatiekanalen een aaneenschakeling van natuurlijke hindernissen. De gecoördineerde Russische tegenstand vanuit de verschillende verdedigingslinies leidde ertoe dat de Oekraïense eenheden nauwelijks voortgang boekten en enorme verliezen opliepen. Hoewel de stad Cherson en de bruggen over de rivier binnen het bereik van de Oekraïense artillerie kwamen, slaagden Russische eenheden erin de beschadigde bruggen onder vuur te vervangen en gecombineerd met veerdiensten de herbevoorrading in stand te houden, waardoor zij de verdediging konden blijven voeren.[16]

Begin oktober stabiliseerde de situatie zich. De Oekraïense politieke leiding was echter ongeduldig: de Oekraïense commandant werd vervangen en het offensief hervat. Om elke meter grond werd hard gevochten. De door het Westen geleverde geleide wapens en langeafstandraketwerpers, het voordeel van de kennis van de lokale omstandigheden en informatie van het netwerk van informanten achter de linies over Russische activiteiten, konden het Oekraïense offensief echter niet omzetten in een snelle opmars. De Russen verrasten uiteindelijk met een georganiseerde terugtrekking ondanks de intensieve Oekraïense surveillance. Elke terugtrekroute werd verdedigd tegen Oekraïense aanvallen door gecoördineerd optreden van het Russische gevecht van verbonden wapens. Het lukte de Oekraïense troepen niet de 35.000 terugtrekkende Russische militairen te achtervolgen en de ineenstorting van de Russische verdediging te forceren.[17] Zonder intensieve stadsgevechten werd Cherson op 14 november heroverd en eindigde dit Oekraïense tegenoffensief.[18]

Conform de technieken van het moderne systeem voerden de Russische eenheden een coherente verdediging vanuit voorbereide linies met afgestemde manoeuvre-, vuur- en geniesteun, met goede dekkingsmogelijkheden en afscherming tegen observatie, en met kwalitatief goede eenheden, waaronder het goed getrainde 1 Garde Tankleger, later aangevuld met reservisten en gemobiliseerd personeel. Ook de haperende logistiek brak de Russen uiteindelijk niet op. Door de confrontatie met een goed georganiseerde Russische verdediging, het ontbreken van dekkingsmogelijkheden in het terrein en de aanwezigheid van talloze vertragende hindernissen, namen de Oekraïense

16 Fedorchak, *The Russia-Ukraine War*, 89-90.

17 Barry Posen, 'Russia's Rebound', *Foreign Affairs*, 5 januari 2023. Zie: https://cis.mit.edu/publications/analysis-opinion/2023/russias-rebound.

18 Gady en Kofman, 'Ukraine's Strategy of Attrition', 12-13.

Oekraïense militairen in Koepiansk, 20 september 2022: na enkele weken liep de Oekraïense opmars vast in massale Russische vuursteun

FOTO ANP/ THE NEW YORK TIMES, NICOLE TUNG

verliezen snel toe en kon er weinig terreinwinst worden geboekt. De Russische verdediging slaagde erin het Oekraïense offensief in te dammen.

Wat zegt de meester zelf?

Volgens Biddle wordt de oorlog in Oekraïne gevoerd met nieuwe geavanceerde technologieën, maar zijn er ook soldaten te voet die zich een weg banen door modderige loopgraven in scènes die meer lijken op beelden uit de Eerste Wereldoorlog dan uit Star Wars, zoals velen hadden verwacht. De huidige oorlog is niet veel anders dan andere oorlogen omdat de gevolgen van de nieuwe technologieën veelal hetzelfde zijn. De aantallen slachtoffers of verliezen van tanks zijn niet ongewoon hoog vergeleken met historische cijfers. Er is ook geen patroon van een defensieve patstelling door de inzet van nieuwe technieken. Beide partijen passen zich aan door een combinatie van tegenmaatregelen en het steeds verder doorvoeren van de methoden van het moderne systeem die de blootstelling aan vijandelijk vuur reduceren door meer spreiding, bescherming, afscherming, diepte in de verdediging en grootschalige inzet van onderdrukkingsvuur.[19]

De verliezen zijn nog steeds groot, maar het betekent niet dat landeenheden geen terreinwinst kunnen boeken, zoals bij Charkov en Cherson. Succes in de aanval vereist een combinatie van offensieve vaardigheden en defensieve fouten. Het is voor beide partijen moeilijk om snel voortgang te boeken of doorbraken te forceren tegen een diepe, goed voorbereide verdediging ondersteund door reserves en een functionerende bevoorrading, met een patstelling als gevolg. Daarentegen konden beide partijen snel voortgang boeken tegen ondiepe verdedigingen zonder goede reserves achter hen, en vooral als het de verdedigers ontbrak aan inzet om te vechten en de benodigde bevoorrading niet in stand kon worden gehouden. Volgens Biddle is dit het gevolg van al lang bestaande trends en verbanden tussen technologie en een voortdurende, wederzijdse aanpassing waarbij de strijdende partijen te allen tijde willen voorkomen dat de tegenstander een beslissende voorsprong krijgt.[20]

19 Stephen Biddle, 'Back in the Trenches. Why New Technology Hasn't Revolutionized Warfare in Ukraine', *Foreign Affairs*, 10 augustus 2023. Zie: https://www.foreignaffairs.com/ukraine/back-trenches-technology-warfare.

20 Biddle, 'Back in the Trenches'; Stephen Biddle, 'Ukraine and the future of offensive maneuver', *War on the Rocks*, 22 november 2022. Zie: https://warontherocks.com/2022/11/ukraine-and-the-future-of-offensive-maneuver/.

ANP/THE NEW YORK TIMES, JIM HUYLEBROEK

Aan Oekraïense zijde van het front bij Cherson op 15 september 2022: conform de technieken van het moderne systeem voerden de Russen hier een coherente verdediging vanuit voorbereide linies

Conclusie

De conclusies die kunnen worden getrokken, te midden van de voortdurende gevechten in Oekraïne, zijn voorlopig. Maar percepties ontstaan snel dus is het zaak om deze zo nauwkeurig mogelijk vorm te geven, ook terwijl de oorlogvoering zich dagelijks ontvouwt. Aan beide zijden van de frontlinie wordt geleerd en worden aanpassingen gedaan, waarbij zij ook nieuwe technieken toepassen. Toetsing van de theorie van Biddle aan de gevechten in Oekraïne biedt een ander perspectief op deze oorlog.

De theorie van Biddle stelt dat de kern van de oplossing voor het probleem van het militaire optreden op het letale gevechtsveld vooral ligt in de doctrine en tactieken en niet zozeer in technologie of numeriek overwicht. Door het stringent toepassen van het moderne systeem reduceert een krijgsmacht de blootstelling aan de moderne wapentechnologie. De moderne technologie beperkt beweging op het gevechtsveld in het landdomein. De enorme vuurkracht en de grootschaligere inzet van bijvoorbeeld drones houdt eenheden (te) lang in dekking, waardoor de snelheid van de aanval verdwijnt. Met de voortschrijdende ontwikkeling van de (wapen)techniek wordt het gevechtsveld dodelijker en blijft het zoeken naar een balans tussen overleven en snelheid in het optreden.

De studie van Biddle geeft aan dat toepassing van het moderne systeem, ofwel het reduceren van de blootstelling, gevolgen heeft voor het aantal slachtoffers, de mogelijke terreinwinst en de duur van de oorlog. Dat gebeurt in Oekraïne en is in de uitgewerkte casuïstiek aangetoond. Zoals bij Charkov, als Rusland verzuimt voldoende reserve-eenheden in te zetten en geen coherente verdediging voert en daarvoor hard gestraft wordt in aantallen slachtoffers en verlies aan terrein. Of zoals bij Cherson, waar beide strijdende partijen het moderne systeem proberen toe te passen door het gevecht van verbonden wapens te voeren, diepte in het

gevecht aan te brengen en massaal gebruik te maken van onderdrukkingsvuren, waardoor het Oekraïense offensief traag verloopt en er aan beide zijden veel slachtoffers vallen.

Om in de toekomst betekenisvolle landoperaties uit te kunnen voeren in een storm of steel is het aan te bevelen de geïdentificeerde lessen van de Oekraïne-oorlog te gebruiken en Biddles advies te volgen om niet achter technische gadgets aan te jagen, maar meer geld en tijd te investeren in het opleiden en trainen van de landeenheden in het moderne systeem. Techniek blijft een *enabler* in de zeer ingewikkelde menselijke activiteit van oorlogvoeren. Nieuwe technologieën zullen eerst in relevante operationele concepten moeten worden vertaald voordat ze effectief kunnen worden toegepast.

Tot slot zou een aanbeveling kunnen zijn de huidige 'bezuinigingsorganisatie' snel om te bouwen naar een krijgsmacht die kan vechten volgens het moderne systeem met zelfstandige brigades. Die brigades moeten in wisselende samenstellingen met een diversiteit aan capaciteiten kunnen optreden, zoals de Oekraïense *small assault tactical teams* dat momenteel doen, of teruggrijpen naar de eigen Nederlandse ervaring in de Koude Oorlog, met de karakteristieken van de toenmalige verkenningsbataljons en zelfstandige verkenningseskadrons (ZVE). Kortom, de krijgsmacht gaat *forward with the past* en de precieze uitwerking van de lessen uit de Oekraïne-oorlog vergt nog veel denkwerk van theoretici. ■

Om betekenisvolle landoperaties uit te kunnen voeren in een storm of steel is het aan te bevelen om de geïdentificeerde lessen van de Oekraïne-oorlog te gebruiken en Biddles adviezen te volgen

FOTO MCD, HILLE HILLINGA

Straffen of leren?

Het negatieve effect van een retributieve houding op lerend vermogen

Kolonel dr. L. Boskeljon-Horst, dr. E.M. van Baarle en dr. A. Snoek*

Leren van incidenten is van belang voor een organisatie om de sociale en fysieke veiligheid,[1] en daarmee de effectiviteit van de organisatie, te verbeteren. Hiervoor is informatie over incidenten cruciaal. Echter, de mate waarin medewerkers bereid zijn die informatie te delen, hangt af van hoe een organisatie reageert op een incident. Als er straffend wordt gereageerd op een incident is er minder bereidheid om informatie te delen, maar welke houding stimuleert het delen van informatie dan wel? Dit artikel is deel 2 van het tweeluik 'Just culture en het effect op leren en herstel.'[2]

Straffen of leren? Volgens onderzoek kan een organisatie met een restauratieve just culture leren van incidenten en tegelijkertijd passende straffen toepassen

FOTO MCD, MIKE DE GRAAF

* Leonie Boskeljon-Horst is universitair hoofddocent Human Factors, Just Culture en Sociale Veiligheid en tevens Programmaleider Academische Werkplaats Just Culture, Sociale Veiligheid en Ethische Reflectie aan de Faculteit Militaire Wetenschappen. Eva van Baarle is universitair hoofddocent Sociale Veiligheid, Just Culture en Ethiek, projectleider van het Just Culture project en Programmaleider Academische Werkplaats Just Culture, Sociale Veiligheid en Ethische Reflectie. Anke Snoek is post-doctoraal onderzoeker binnen de Academische Werkplaats Just Culture, Sociale Veiligheid en Ethische Reflectie.

1 J. Reason, *Managing the Risks of Organizational Accidents* (Ashgate, 1997); S.W.A. Dekker, *The Field Guide to Understanding Human Error* (Ashgate, 2006); D.D. Woods, S.W.A. Dekker, R. Cook, L. Johannesen, N.Sarter, *Behind human error* (Ashgate, 2010).

2 Zie voor deel 1: L. Boskeljon-Horst, E.M. van Baarle en A. Snoek, 'Helden zonder schurken. Een op herstel gerichte just culture in de praktijk', *Militaire Spectator* 193 (2024) (4).

Een manier om te investeren in de gewenste informatiestroom is door het implementeren en koesteren van een zogenaamde just culture.[3] Just culture betreft een compromis tussen enerzijds de behoefte aan het afleggen van verantwoording voor daden en anderzijds de bereidheid van medewerkers om vrijwillig incidenten te melden zonder daarvoor te worden gestraft.[4] Het gaat om een klimaat van vertrouwen waarin gebeurtenissen worden gemeld en gedeeld[5] en waarin duidelijkheid wordt geboden over wat wel en niet wordt geaccepteerd van medewerkers.[6]

Een eerste uitwerking van het just culture concept is wat we noemen een retributieve (straffend/vergeldend) just culture. In een retributieve just culture wordt de oorzaak van een incident gelegd bij een individu dat een overtreding van de regels heeft begaan. Het rechtvaardigheidsprincipe ('just') is vooral gericht op de vraag hoe de ontstane schade wordt gecompenseerd met een consequentie die, als een vorm van straf, de prijs is die betrokken individuen moeten betalen. Vragen die hierbij worden gesteld zijn: Welke regel is overtreden? Wie heeft dat gedaan? Hoe erg is de overtreding? Welke sanctie hoort daarbij?[7] Het resultaat is dat betrokken personen verantwoording afleggen over wat zij hebben gedaan. Het idee

FOTO MCD, PHIL NIJHUIS

achter deze benadering is dat een duidelijke grens getrokken kan worden tussen acceptabel en onacceptabel gedrag. Het kenbaar maken van deze grens zorgt er voor dat mensen weten waar ze aan toe zijn. Als mensen deze grens overschrijden, dan is van tevoren duidelijk dat daar consequenties aan zijn verbonden.[8]

Echter, acceptabel en niet-acceptabel gedrag zijn geen in beton gegoten categorieën, maar worden bepaald door de tijd, context en persoon die hierover een beslissing neemt.[9] Als maatregelen als onrechtvaardig worden gezien, zullen mensen hun fouten proberen te verbergen om

3 D. Heraghty, S.W.A. Dekker, A. Rae, 'Modifying an accident process and its justice system – From single narratives and retribution to multiple stories and restoration', *Safety Science 139* (April 2020).

4 S.W.A. Dekker, H. Breakey, '"Just culture:" Improving safety by achieving substantive, procedural and restorative justice', *Safety Science 85* (2016) 187–193; International Civil Aviation Organization, 'Fostering just culture in operators and service providers', 28 mei-1juni 2018. Zie: https://www.icao.int/APAC/Meetings/2018%20APRAST12/APRAST12%20WP-11%20AI_5%20-%20%5BNokScoot_AEROTHAI_CANSO%5D%20Just%20Culture.pdf.

5 M. Kováčová, A. Licu, J. Bálint, 'Just Culture - Eleven Steps Implementation Methodology for organisations in civil aviation - "jC 11"', *Transportation Research Procedia* 43 (2019) 104–112.

6 EUROCONTROL, 'Establishment of "Just Culture" Principles in ATM Safety Data Reporting and Assessment - EAM2/GUI 6', 31 maart 2006.

7 S.W.A. Dekker, *Just Culture. Balancing Safety and Accountability* (Ashgate, 2007).

8 S.W.A. Dekker, 'Just culture: who gets to draw the line?', *Cognition, Technology and Work* 11 (2009) (3) 177-185.

9 S.W.A. Dekker, 'When human error becomes a crime', *Human Factors and Aerospace Safety* 3 (2003) (1) 83–92; M.D. Alicke, J. Buckingham, E. Zell, T. Davis, 'Culpable control and counterfactual reasoning in the psychology of blame', *Personality and Social Psychology Bulletin* 34 (2008) (10) 1371–1381; Dekker, 'Just culture: Who gets to draw the line?', 177–185.

De KMA in Breda. In dit artikel staat de praktijkcasus centraal waarbij cadetten op de KMA foto's deelden in een WhatsApp-groep die tot ophef leidden

zo negatieve consequenties te voorkomen[10] en de bereidheid om te melden zal afnemen. Beide gevolgen hebben een negatief effect op de open cultuur die men probeert te bewerkstelligen.[11] Zo bezien sluiten de twee doelen, retributie/straffen en leren, elkaar uit.[12]

Om deze negatieve effecten van retributie tegen te gaan is een tweede uitwerking van just culture ontstaan, getiteld restauratieve (herstelgerichte) just culture. In een restauratieve just culture ligt de focus niet zozeer op het beoordelen van gedrag maar meer op leren en herstel.[13] Het gaat hier om vragen als: Wie

10 Dekker, *Just Culture. Balancing Safety and Accountability*.

11 Reason, *Managing the Risks of Organizational Accidents*; L.E. Lipira, T.H. Gallagher, 'Disclosure of adverse events and errors in surgical care: Challenges and strategies for improvement', *World Journal of Surgery* 38 (2014) (7) 1614–1621; A.J. Lawrenson, G.R. Braithwaite, 'Regulation or criminalisation: What determines legal standards of safety culture in commercial aviation?', *Safety Science* 102 (July 2016), 251–262; O. Brborović, H. Brborović, I.A Nola, M. Milošević, 'Culture of blame—an ongoing burden for doctors and patient safety', *International Journal of Environmental Research and Public Health* 16 (2019) (23).

12 Dekker, 'When human error becomes a crime', 83–92; D. Heraghty, A.J. Rae, S.W.A. Dekker, 'Managing accidents using retributive justice mechanisms: When the just culture policy gets done to you', *Safety Science* 126 (May 2019).

13 S.W.A. Dekker, *Just culture: Restoring Trust and Accountability* (CRC Press Taylor & Francis Group, 2016); Dekker, Breakey, '"Just culture:" Improving safety by achieving substantive, procedural and restorative justice', 187–193.

heeft er schade geleden? Wat hebben zij nodig? Wie is verantwoordelijk om daaraan tegemoet te komen? Welke rol spelen de organisatie en de omgeving bij het herstel en bij het leren van deze situatie? Binnen deze benadering vinden gesprekken plaats tussen alle betrokkenen die door het incident zijn geraakt, met als doel te begrijpen wat er is gebeurd, inzicht te verkrijgen in de context waarin het incident heeft plaatsgevonden en antwoord te geven op de vraag wat vervolgens te doen.[14] Eventuele noodzakelijk gevonden maatregelen en herstelacties vloeien hieruit voort. Deze acties worden breed gedragen doordat dit een groepsinspanning is, niet voorbehouden aan een tot straffen bevoegde meerdere. Het afleggen van verantwoording neemt ook bij de restauratieve just culture een grote plaats in, de wijze waarop dit gebeurt verschilt echter van de retributieve benadering.

De literatuur laat positieve effecten zien van een restauratieve just culture, zoals een toename in onderling vertrouwen, gedeelde verantwoordelijkheid en leren.[15] Een focus op herstel en leren resulteert in kwantitatief en kwalitatief betere informatie waardoor de werkplek veiliger wordt.[16] Een restauratieve benadering leidt bovendien tot minder disciplinaire maatregelen, een afname in ziekteverzuim en toegenomen openheid.[17]

De afgelopen jaren hebben wij, samen met collega-onderzoekers, onderzoek gedaan naar sociale veiligheid bij Defensie vanuit een just culture perspectief[18]. In een tweeluik presenteren we de resultaten van ons onderzoek naar de effecten van zowel een retributieve als die van een restauratieve benadering op incidenten. In het eerste deel, gepubliceerd in de *Militaire Spectator* van april 2024, is aan de hand van een praktijkcasus 'safety standdown' weergegeven wat de effecten zijn van een restauratieve benadering op openheid en leren. Dit tweede deel biedt, eveneens aan de hand van een praktijkcasus ('WhatsApp'), inzicht in de effecten van een reactie op een incident die vooral retributief is op het uiteindelijke leren in de organisatie. In beide cases gaat het over situaties die niet onder het strafrecht vallen, waar een retributieve reactie te verwachten valt.

Casus: WhatsApp-foto's

De casus gaat om een WhatsApp-groep van cadetten waarin ze, in hun beleving, op humoristische wijze hun frustratie uiten over lessen, tentamens, cijfers en docenten. Op een gegeven moment heeft een aantal cadetten hierbij met Photoshop foto's van zichzelf en docenten ingevoegd in beeldmateriaal uit de Tweede Wereldoorlog. Een advocaat, betrokken bij een niet-gerelateerd juridisch proces, deelt een aantal screenshots uit de WhatsApp-groep met een functionaris binnen de organisatie. De boodschap hierbij is dat de advocaat een gesprek wil in de organisatie, anders zal hij de screenshots delen met (tv)media. De screenshots worden vervolgens onder de aandacht gebracht van het topbestuur van Defensie, dat de informatie op zijn beurt weer deelt met relevante directeuren binnen de Bestuursstaf en het betrokken onderdeelsmanagement. Naast de interne reactie vindt tevens een strafrechtelijke toetsing plaats: omdat het hier om een besloten WhatsApp-groep gaat is dergelijke content niet strafbaar.

Bevindingen

In 2021 en 2022 hebben we (LB en EVB) 30 direct en indirect betrokkenen bij de casus WhatsApp-groep geïnterviewd over hun ervaringen, onder

14 J. Parkinson, D. Roche, 'Restorative justice: Deliberative democracy in action?', *Australian Journal of Political Science* 39 (2004) (3) 505–518.

15 K. Turner, N.J.C. Stapelberg, J. Sveticic, S.W.A. Dekker, 'Inconvenient truths in suicide prevention: Why a Restorative Just Culture should be implemented alongside a Zero Suicide Framework', *Australian and New Zealand Journal of Psychiatry* 54 (2020) (6), 571–581.

16 Dekker, Breakey, '"Just culture:" Improving safety by achieving substantive, procedural and restorative justice', 187–193; S.K. Bell, T. Delbanco, L. Anderson-Shaw, T.B. McDonald, T.H. Gallagher, 'Accountability for medical error: Moving beyond blame to advocacy', *Chest* 140 (2011) (2), 519–526.

17 M. Kaur, R.J. De Boer, A. Oates, J. Rafferty, S.W.A. Dekker, 'Restorative Just Culture: a Study of the Practical and Economic Effects of Implementing Restorative Justice in an NHS Trust', MATEC Web of Conferences 273 (April 2018).

18 Zie bijvoorbeeld: L. Boskeljon-Horst, A. Snoek en E. van Baarle, 'Learning from the complexities of fostering a restorative just culture in practice within the Royal Netherlands Air Force', *Safety Science* 161 (2023); A. Snoek, T. Eikenaar, V.E.T. Dörenberg en E. van Baarle, 'Vormen voor sociale veiligheid: ruimte voor alle perspectieven?', *Officiersvorming in klare taal* (Nederlandse Defensie Academie/ Leiden University Press, 2023) 49-71; A. Spijkers, A. Snoek en E. van Baarle, 'De uitdagingen van (meer) vrouwen bij Defensie', *Militaire Spectator* 192 (2023) (1) 4-17.

wie cadetten, beleidsmedewerkers en commandanten, inclusief het topmanagement van Defensie. Uit de analyse van de WhatsApp-casus komen vijf thema's naar voren die hieronder worden uitgewerkt.

Context onbekend

Uit de data blijkt dat de bewuste WhatsApp-groep is ontstaan om snel roosters en andere informatie over de studie aan de KMA te kunnen delen. Al snel groeide dit uit tot een sociaal platform waarop, uit verveling, frustraties en commentaren op de lessen werden gedeeld. Naast het chatten werden ook afbeeldingen gedeeld. Deze afbeeldingen hadden een relatie met de lessen die op dat moment werden gevolgd. Vlak voor het in opspraak raken van deze WhatsApp-groep werd in deze klas de Tweede Wereldoorlog behandeld. Dit thema kwam dan ook terug in de boodschappen die over en weer werden gedeeld. In de maanden voorafgaand aan deze periode hadden de berichten binnen de WhatsApp-groep een ander thema, wat overeen kwam met wat op dat moment werd gedoceerd.

De motivatie achter het sturen van deze afbeeldingen was het op, zij het rauwe, humoristische wijze delen van de eigen ongenoegens of slechte prestaties of het elkaar op de hak nemen. De stroom aan berichten en afbeeldingen werden gezien als één lange grap. De intentie was niet een bevolkingsgroep te schofferen. Deze intentie wordt volgens de Centrale Organisatie Integriteit Defensie (COID) onderbouwd door het onderzoeksrapport.[19] Een voorbeeld: 'Binnen krijgswetenschappen behandel je genocide na genocide en [X] was de enige die een onvoldoende had gehaald voor een paper, nou, daar hadden ze een [afbeelding van een] SS-er die iemand executeerde en daar hadden ze [X] op gefotoshopt zeg maar. […] mensen vonden het grappig van haha, dit is de gast die een onvoldoende heeft gehaald en zijn docent geeft hem op zijn flikker. Dat was de humor. […]. Als ze bij wijze van de Boerenoorlog hadden gekozen dan was het een Afrikaan die iemand anders neerschoot zeg maar. Alleen omdat we nu als studieobject nazi-Duitsland hadden was het nazi-Duitsland. Maar dat had niks te maken met het verheerlijken van nazi's.'

Ondanks dat de inhoud van de WhatsApp-groep voor de cadetten ging om het humoristische element en het omgaan met verveling en frustratie, wordt vanuit de organisatie het gedrag gelabeld als rechts-extremistisch, racistisch, grensoverschrijdend, kwetsend, beledigend en verwijzend naar nazi-Duitsland. Tegelijkertijd laat Defensie in de media weten dat er 'geen beeld […] van inhoudelijke betrokkenheid bij of affiniteit met nationaal socialistisch gedachtengoed' naar voren komt.[20] En ook uit de interviewdata komt naar voren dat men niet de indruk heeft dat antisemitisme heerste en dat de foto's, gezien de context en beslotenheid van de groep, minder schokkend zijn dan ze in eerste instantie lijken. Ondanks deze nuancering hebben betrokkenen toch het idee dat ze worden weggezet als nazi-sympathisanten en antisemieten. Voor de cadetten is het plaatsen van content in de WhatsApp-groep een manier om met de aan hen voorgeschotelde informatie om te gaan: '80 procent van onze studie gaat over verschrikkelijkheden. Humor is dan ook een copingstrategie, met een luchtige grap is de spanning eraf. […] We gingen dehumaniseren, harde humor, je wordt erin meegesleurd.'

Op het moment van bekend worden van de content van deze WhatsApp-groep is de context – die van verveling en frustratie, intense lesstof en een groep cadetten die niet wezenlijk verschillen van civiele studenten – niet direct helder voor de ambtelijke top. Enkel het eindresultaat, de bewerkte foto's, wordt hun getoond. Ook later in het proces, zodra het onderzoek is gestart, lijkt er weinig ruimte voor de context waarin de WhatsApp-situatie is ontstaan: 'Het voelde als een politieverhoor. […] de vragen die werden gesteld die waren heel erg gericht op het achterhalen van mensen die wat gedaan hadden. En als je zaken aanhaalde over de cultuur op de academie […] die er heerst, dan

19 Dit onderzoeksrapport is niet openbaar en maakt ook geen deel uit van het onderzoek naar deze casus.

20 Nieuwsbericht ministerie van Defensie eind december.

werd dat gelijk afgekapt. […] Ja, de waaromvraag zeg maar, die werd niet gesteld.'

Zonder zicht te hebben op de context, de omstandigheden en de maandenlang durende glijdende schaal waarin de humor steeds rauwer wordt en scherpere kantjes krijgt, is het eindresultaat bijzonder schokkend. Als outsider van een groepsproces is het op dat moment niet te begrijpen hoe dit heeft kunnen ontstaan. En juist vanuit die eigen schok, zonder zicht op de context en maandenlange groepsdynamiek, volgt een, vanuit het perspectief van topmanagement, begrijpelijke en stevige reactie.

Politieke druk tot retributief optreden

De WhatsApp-foto's leiden tot een negatieve reactie vanuit de politiek. De suggestie dat er sprake zou (kunnen) zijn van rechts-extremistisch gedachtegoed kan niet terzijde worden gelegd. Wat opvalt in de geanalyseerde casus is dat het topmanagement, begrijpelijkerwijs, probeert hier proactief op in te spelen en niet te wachten tot Defensie verzocht wordt om tekst en uitleg te geven en hiermee in de verdediging wordt gedrukt. Communicatie vanuit Defensie in de media en richting de Tweede Kamer laat dan ook zien dat de eerste focus van het topmanagement ligt bij het treffen van maatregelen. De interviewdata laten zien dat in de perceptie van de geïnterviewden de focus ligt bij het daadkrachtig overkomen richting de politiek, een duidelijke boodschap dat Defensie dergelijk gedrag onacceptabel acht en hier hard tegen zal optreden: 'het was natuurlijk gelijk politiek gevoelig, […] we moeten wel laten zien dat het ons ernst is. […] het kan niet zo zijn dat op het moment dat we zeggen, let op, hier zijn we mee aan de slag, dat er dan direct daarna weer [iets] in de krant staat. Dan ben je al je geloofwaardigheid gelijk kwijt. […] Dit had een dossier kunnen zijn waarop het kabinet gevallen was.'

Op het moment dat de WhatsApp-content bekend wordt bij het topmanagement speelt er een aantal andere gevoelige dossiers bij Defensie. Zo is twee maanden voor de WhatsApp-situatie het rapport Giebels inzake misstanden en sociale veiligheid uitgekomen en is men binnen de Bestuursstaf op het moment van berichtgeving over de WhatsApp-content bezig met het schrijven van een beleidsreactie aangezien dit rapport en de reactie een krappe week later in het Algemeen Overleg Veiligheid van de Tweede Kamer worden besproken. Daarnaast speelde een situatie, eveneens op de KMA, waarbij een instructeur intieme relaties onderhield met meerdere cadetten. 'Nou ja, vlek op vlek als het ware. Dus ik denk dat daar de reactie vandaan komt, dat [...] gelijk eigenaarschap naar zich toetrok.'

De politieke gevoeligheid wordt door alle betrokkenen gevoeld. 'Ik vond het echt een overkill en vanaf toen zat echt het sentiment erin van dit is gewoon puur politieke spierballen, dit heeft niks te maken met de toedracht, dit heeft niks te maken met "hoe gaan we dit voorkomen, wat is er gebeurd", het is gewoon puur het hoofd van de minister ligt op het hakblok, het is tijd dat er een paar koppen gaan rollen en dan wordt het weer bestempeld als een incident.' En: 'Ik denk als er verder helemaal niets aan de hand was geweest, als er geen andere incidenten waren geweest dan denk ik dat de reacties op de WhatsApp-groep wellicht iets minder waren geweest.'

Op het moment van communiceren heeft echter nog geen onderzoek plaatsgevonden. De precieze oorzaak, context en intentie van de WhatsApp-foto's is nog niet onderzocht en niet bekend. Op voorhand is echter besloten dat ontslag van betrokkenen, die op dat moment evenmin bekend zijn, passend is. Hoewel de COID waarschuwt niet enkel te kijken naar politieke en publicitaire belangen omdat dit de situatie geen recht doet, moet een balans gevonden worden tussen feitelijk gedrag en (rechtspositionele) maatregelen. 'Als het aan het ministerie had gelegen dan was iedereen die schuldig was bevonden ontslagen omdat ze daarmee een statement konden maken richting de buitenwereld dat Defensie er wat aan gedaan heeft.'

Gezien het aftreden van de minister van Defensie en de commandant der strijdkrachten, in reactie op het onderzoeksrapport naar het voorval in Mali in 2017, is het ongemak, mogelijk zelfs angst, met betrekking tot een

De WhatsApp-casus leidde tot een felle retributieve reactie, terwijl de context van de casus onbekend was FOTO OPENBAAR MINISTERIE

politieke reactie begrijpelijk. Deze angst leidt echter intern tot wantrouwen en verwijdering in de hiërarchische lijn. In plaats van dat de geconstateerde situatie wordt afgedaan op commandantenniveau, wordt de handelswijze op het hoogste niveau besloten. Dit staat haaks op de uitspraak 'commandant in zijn kracht'. Reden voor deze strategie is volgens geïnterviewden dat er geen vertrouwen bestond in een 'juiste' afdoening door de commandanten. Voor hen bestond geen speelruimte, alle besluiten worden in Den Haag genomen. 'De eerste insteek van […] en dat heeft hem ook niet geholpen denk ik, was "nou ik schrijf wel een briefje naar alle NLDA-leden dat dit niet kan en dat we het gaan onderzoeken zeg maar." […]. Nou, dat was echt te mager. Dus de roep om laten zien dat het je ernst is in daden zeg maar, die was wel vrij groot.'

Kosten en baten van retributie

De casus laat zien dat er in de beleving van de betrokkenen geen ruimte was voor nuancering, begrip en zeker niet voor de optie niet te straffen. Het onderzoek heeft dan ook daadwerkelijk geresulteerd in disciplinaire maatregelen – voortijdig vertrek van twee commandanten, ambtsberichten voor een aantal cadetten – die door geïnterviewden als onrechtvaardig worden beschouwd. 'Een negatief ambtsbericht is de zwaarste straf die je iemand kan opleggen behalve ontslaan. […] En vooral ook omdat het zoiets normaals is zeg maar, dat er gewoon hele harde humor is, vooral binnen Defensie en dat tegelijkertijd die ontzettende zwartegalgencultuur op de KMA niet wordt aangepakt dat voelde gewoon heel krom en dat voelde heel onterecht.' En: 'Het was geen strafrechtelijk vergrijp dus werd het bestuursrechtelijk afgedaan. Zeg maar de organisatie heeft er echt wel moeite in gestopt om ons echt zo hard mogelijk te pakken.'

Eerder onderzoek laat zien dat straffen dermate onderdeel is van de defensiecultuur, dat het niet straffen en focussen op leren en herstel morele moed vraagt. Niet straffen, maar een restauratieve houding aannemen heeft in veel gevallen een negatieve invloed op je carrière. Sommigen suggereren dat een restauratieve houding momenteel enkel is weggelegd voor leidinggevenden die geen bevorderingsperspectief meer hebben.[21] Ook in dit onderzoek wordt opgemerkt dat het niet vanzelfsprekend is om te

21 L. Boskeljon-Horst, A. Snoek, en E.M. van Baarle, 'Learning from the Complexities of Fostering a Restorative Just Culture in Practice within the Royal Netherlands Air Force', *Safety Science* 161 (September 2022) 1060–74. Zie: https://doi.org/10.1016/j.ssci.2023.106074.

steunen in plaats van te straffen: ‘Toen bekend was dat wij het waren heeft [onze commandant] en dat vond ik heel dapper van hem, die heeft gezegd “jongens, mij wordt afgeraden om jullie te adviseren […] want er gaan koppen rollen […]” Hij heeft wel gewoon, het was echt 15 seconden even snel gewoon ja, vanuit de organisatie het meest de hand in het vuur gestoken voor ons dat ik tot nu toe heb gezien, naast […].’

Een cultuur gericht op retributief reageren leidt tot schade bovenop de schade die door een incident wordt veroorzaakt, zo laat de Whats-App-casus zien. Het gaat in dit geval met name om emotionele schade als gevolg van een gepercipieerde onrechtvaardige behandeling. Cadetten herkenden zich bijvoorbeeld niet in de over hen gedane beeldvorming met betrekking tot de WhatsApp-content. Het ervaren gebrek aan nuancering heeft geleid tot gevoelens van onmacht en angst. Het gebrek aan (juridische) begeleiding heeft hierin een mediërende rol gehad. ‘Ik heb zelf als cadet nooit kunnen plaatsen wat de zwaarte van een ambtsbericht is en wat het betekent en dat was ook een stuk juridische begeleiding die ik miste van wat betekent het waar ik in verzeild ben geraakt […] heb ik zwijgrecht?’

De wijze waarop de cadetten zijn benaderd en behandeld heeft volgens de geïnterviewden er toe geleid dat twee van hen een burn-out hebben gekregen. ‘In een aantal individuele gevallen is door het hele optreden zeker schade ontstaan; een aantal cadetten met psychische problemen, […] De [organisatie] dendert door maar dan liggen er nog wat slachtoffers langs de kant van de weg.’

Als onderzoekers worden we zelf ook geconfronteerd met de emotionele schade als ons wordt verteld dat een aantal betrokkenen er nooit meer over wil praten en dus ook, drie jaar na de kwestie, ons onder geen enkele voorwaarde wil spreken. ‘Van eentje of twee lopen nog processen en procedures, waarmee ik bedoel te zeggen: die waren toch wel zodanig geraakt door de hele problematiek dat het lang duurde voordat ze weer op de rails stonden […]. Maar als je ziet wat voor schade daardoor aangericht is door onjuiste bejegening.’

De feitelijke consequenties zoals ambtsberichten werden pas na anderhalf jaar duidelijk. De cadetten waren de kwestie op dat moment zo zat dat niemand overwogen heeft bezwaar aan te tekenen. Ze waren letterlijk moe gestreden en wilden enkel nog rust op dit vlak. De sporen zijn echter onuitwisbaar, zo is de indruk. In de interviews wordt gesproken over gevoelens van frustratie, verminderd zelfvertrouwen en verdriet. ‘Het is gewoon echt een wezenlijk onderdeel van mijn militaire identiteit geworden dat je onderhevig bent aan een systeem dat zo met personeel om gaat. Zo voelt het echt.’

Anderzijds bleven ook degene die wilden straffen onbevredigd achter, zij vinden de straffen veelal te mild, en zijn gefrustreerd dat niet duidelijk is geworden wat er precies is gebeurd. Als gekeken wordt naar de emotionele impact op alle betrokkenen dan kan de vraag worden gesteld of de schade die door de organisatie is toegebracht niet groter is dan de schade voor de organisatie als gevolg van de openbaarmaking. De ervaring leert dat in de media, en zelfs met Kamervragen, na een aantal weken het spreekwoordelijke stof weer neder-daalt. De WhatsApp-casus laat zien dat dit niet geldt voor betrokkenen. Uiteindelijk wordt het straffen door alle partijen als onrechtvaardig ervaren; niemand heeft het idee dat er recht is gedaan aan de situatie.

Het effect op leervermogen

Vanaf het moment dat wordt aangekondigd dat Defensie zich zal richten op passende maat-regelen, door de geïnterviewden gepercipieerd als vooringenomenheid, wordt eveneens intern door de top aangegeven dat de organisatie hiervan wil leren. In de Vaste NLDA-Order Integriteitskwesties staat echter de stelregel: ‘leren als het kan en alleen handhaven als het nodig is’. Ook de COID waarschuwt voor de effecten van het combineren van straffen en leren. ‘Cadetten en adelborsten worden opgeleid tot leidinggevenden en hetgeen zij leren en ervaren tijdens de opleiding vormt hun beeld en handelingsperspectief als toekomstig leiding-gevenden. Indien zij de afhandeling van deze kwestie als onrechtvaardig ervaren, ontstaat het

reële risico dat zij in hun toekomstige functies niet adequaat reageren op integriteitskwesties. Dit erodeert een integere krijgsmacht.'

Op het niveau van de cadetten bestaat niet de indruk dat Defensie daadwerkelijk gericht was op leren van de situatie. Hoewel het topmanagement van mening is dat leiderschap in deze situatie heeft gefaald, zijn er met betrokken lijncommandanten geen reflectie- of ontwikkelingsgesprekken gevoerd om hen op geconstateerde punten te ondersteunen en/of te verbeteren. Dit zou wel passend zijn als leren een doel is.

Bij de niet-cadet geïnterviewden heerst twijfel of er is geleerd van de situatie. Men heeft daar geen beeld bij. Op de vraag of voor cadetten nu helder is wat wel en niet acceptabele humor is, is het antwoord dat men dat niet weet. Sommigen zijn iets stelliger en antwoorden dat er waarschijnlijk niet zo veel is geleerd. De verklaring hiervoor wordt gevonden in de afhandeling van de situatie en in de wijze waarop verbetermaatregelen worden ingericht en opgepakt: 'Ik weet wel dat cadetten, de nieuwe generaties dezelfde humor hebben.'

Om te kunnen leren van een situatie is het noodzakelijk om te weten wat er precies heeft gespeeld. Zonder deze informatie loopt een organisatie het risico dat eventuele maatregelen maar een beperkte relatie hebben met een voorval en derhalve ook een beperkt effect sorteren. Het verkrijgen van deze relevante informatie is lastig als betrokkenen de dreiging van een straf boven het hoofd hangt. 'Mijn kant van het verhaal, zonder dat het gelijk leidt tot een veroordeling, heb ik nooit kunnen doen.'

Sinds 2019 zijn er meerdere WhatsApp-groepen in het nieuws geweest waarvan de content als niet-passend werd beschouwd. Dit laat zien dat de situatie op de KMA geen op zichzelf staande casus is geweest. De conclusie lijkt dan ook dat er van deze situatie niet veel is geleerd. De vraag is in hoeverre de retributieve houding hier een rol in heeft gespeeld.

Mogelijke reactie volgens betrokkenen

Uit de interviews komen ook alternatieve handelingsopties naar voren, die een sterk restauratief karakter hebben. Met name de mogelijkheid om fouten te kunnen/mogen maken, feedback te krijgen op wat wel en niet past en te kunnen leren van fouten zijn volgens geïnterviewden van belang. 'Als cadet ben je je niet bewust van de zwaarte van het ambt. Je bent immers gewoon student in uniform. […] En nu als officier twee jaar bezig snap ik dat bepaalde dingen niet kunnen omdat ik, puur om het simpele feit dat ik officier ben. En dat is nog steeds zoeken wat wel en niet kan. Want […] het enige wat je op de KMA moet doen is een beetje gehoorzamen aan de chef du protocol met die koorregels en ja, hoepeltje springen.' En: 'Je moet dus wel hè, als commandant kunnen aangeven dat het een grens is en dat je achter de grens staat, maar dat je niet per se iemand verkettert op het moment dat die dreigt om die grens over te gaan.' 'Als je zorgt dat je zorgvuldig en rechtvaardig bent, dat mensen vinden dat het ook klopt wat eruit komt […]. Dan bevorder je zelfreflectie.'

Door de straffende houding die boven het incident hing, werd het gewone gesprek bemoeilijkt, en gingen mensen zich apathisch of afwerend opstellen, in plaats van dat er een gezamenlijke discussie ontstond over de cultuur op de KMA. Juist een dergelijke discussie lijkt van belang voor het leereffect. 'Je wil juist dat mensen gaan discussiëren over hetgeen wat er gebeurd is en dat meenemen in hun rugzakje van kan wel/kan niet. Hoe zou je daarmee om moeten gaan? Hoe zou je met degene die dat doen moeten omgaan? En nu was het echt een lijn event zeg maar hè. De baas die bepaalde wat de straf werd en die dook erbovenop. (...) Vanuit een opleidingsperspectief zijn dat prachtige kansen die je kan benutten om te praten over waarden, normen, moreel en dat soort dingen. Die werden hiermee niet zo benut zeg maar. Dat werd hier niet bereikt.' En: 'Dan zou je eens moeten gaan kijken wat je kan inbouwen in het systeem KMA om ervoor te zorgen dat deze ongewenste neveneffecten niet plaatsvinden of gemitigeerd worden.'

Straffen en leren sluiten elkaar uit

De resultaten laten zien dat de defensietop verschillende doelen heeft in de aanpak van het WhatsApp-incident. Ten eerste wil men de schuldigen straffen. Vanuit politiek perspectief is deze reactie voorstelbaar. Berichtgeving over rechtsextremisme en relatie met nazisme leidt begrijpelijkerwijs tot alarmbellen. Straffen oogt rechtvaardig en het doel is om zo een duidelijk signaal af te geven dat dit gedrag ontoelaatbaar is. Bovendien is 'damage control' van belang omdat dit politieke risico's beperkt. Ten tweede wil men leren van het incident én dergelijke incidenten in de toekomst voorkomen, deels door een voorbeeld te stellen (doel 1), deels door te investeren in een plan van aanpak voor de toekomst. Om deze doelen mogelijk te maken is het noodzakelijk een gedegen onderzoek uit te voeren.

De vraag is in hoeverre deze doelen zijn bereikt en of straffen (doel 1) en leren (doel 2) verenigbaar zijn geweest in deze casuïstiek. De resultaten laten zien dat door de dreigende straf mensen niet geneigd waren informatie te delen; de informatiestroom stopte en er is nooit een dialoog geweest. Door de dreigende straf hebben veel cadetten hun WhatsApp-geschiedenis gewist en voelden ze niet de ruimte om open met de onderzoekers te praten. De nuances met betrekking tot de ontstane situatie zijn niet boven tafel gekomen. Het onderzoek ging alleen over het vinden van de schuldigen en niet over de achterliggende oorzaken van het incident en de bredere cultuur. De uiteindelijke straffen werden als onrechtvaardig en buitenproportioneel ervaren, vooral omdat de bredere cultuur geen onderwerp van gesprek is geweest. De straffen hebben averechts gewerkt: uit de gesprekken blijkt dat de kloof tussen de werkvloer en de top van de organisatie groter is geworden, dat men zich politieke pionnen voelt, dat er sprake is van onderling wantrouwen, gevoel van onmacht, willekeur en onrecht, dat het vertrouwen in de organisatie is verdwenen, en dat de zorgvuldig opgebouwde jaarband uit elkaar is gevallen door een splijting in de groep. Het incident kent eigenlijk alleen maar slachtoffers: naast de reputatieschade voor Defensie zijn als gevolg van de maatregelen nieuwe slachtoffers ontstaan zoals de leidinggevenden die het voor de cadetten hebben opgenomen en daarmee zelf consequenties (voortijdig van functie afgehaald) hebben ondergaan, de cadetten uit de WhatsApp-groep die publiekelijk zijn veroordeeld nog voordat het onderzoek was afgerond en de cadetten die, via een advocaat, de screenshots naar buiten hebben gebracht en daarmee buiten de groep vallen. Maar ook degenen die daadkrachtig op wilden treden tegen dit incident blijven onbevredigd achter: zij hebben niet boven tafel kunnen krijgen wat er precies gedaan is door wie, waardoor ze beperkt bleven in hun straffen. Uiteindelijk is er weinig geleerd van het incident. Het gedrag vindt nog steeds plaats, zo blijkt uit het onderzoek, maar wordt beter verborgen gehouden. Bovendien is nog steeds onduidelijk wat nu wel en niet mag. Hoewel er gestreefd werd naar rechtvaardigheid en leren, werd dit door de dreigende straf juist moeilijker. De uiteindelijke retributieve reactie heeft het leren in de weg gezeten en maakt een restauratieve just culture bijna onmogelijk. De casus onderbouwt hiermee de literatuur die stelt dat straffen en leren niet samen gaan.

De vraag die dit oproept is wat dan wel een goede reactie zou zijn? Onterecht wordt vaak gedacht dat een restauratieve benadering betekent dat mensen geen verantwoordelijkheid hoeven te accepteren voor hun daden, dat er geen consequenties volgen. Terwijl juist de restauratieve benadering de behoefte om zowel te leren als te reageren verenigt.

Deel 1 van het tweeluik, het artikel 'Helden zonder schurken', noemt vier factoren die van groot belang lijken te zijn om een restauratieve reactie te kunnen realiseren: 1) de bereidheid van betrokkenen om zich kwetsbaar op te stellen; 2) de wens om te leren van de situatie in plaats van enkel ervoor te straffen; 3) morele moed van leidinggevenden; en 4) een betrokken management dat commandanten niet straft voor restauratief (herstelgericht) reageren.[22]

Als deze factoren op de WhatsApp-casus worden toegepast dan zou een alternatieve handelingsoptie er als volgt uit kunnen zien. Bij het bekend

De retributieve straffen in de WhatsApp-casus werkten averechts: er is onder meer sprake van onderling wantrouwen en splijting binnen de groep

worden van de WhatsApp-content laat het topmanagement aan politiek en media weten dat het op de hoogte is gebracht van dit incident, dat dit zorgvuldig zal worden onderzocht en de uitkomsten van dit onderzoek zo snel mogelijk zullen worden gedeeld. Het onderzoek naar het incident wordt uitgevoerd door een commissie van interne en externe onderzoekers, bekend met het fenomeen social media en die zich richten op zowel het 'wat' (wat is er gebeurd) als het 'hoe' (hoe heeft dit kunnen ontstaan). Oftewel: systeemgericht in plaats van individugericht. Met de resultaten van dit onderzoek kunnen groepsgesprekken worden gevoerd met de cadetten en kader. Focus van deze gesprekken ligt op het reflecteren op het eigen handelen (factor 1) en het beantwoorden van de vraag welke schade dit heeft opgeleverd en wat er nodig is om die te herstellen (factor 2). Het is goed voorstelbaar dat uit dergelijke gesprekken blijkt dat een consequentie voor de cadetten passend is. Als dit de uitkomst is van deze groepsgesprekken, waarin de stem van de cadetten en hun leidinggevenden is gehoord, zal deze consequentie als passend en rechtvaardig worden beschouwd. Een eventuele consequentie maakt deel uit van het herstel- en leerproces en is geen doel op zich. Dit maakt dat het soort consequentie breder is dan wat uit het bestuursrechtelijke palet wordt aangeboden (factor 3). De leidinggevende hiërarchie krijgt de ruimte om conform het principe 'commandant in zijn kracht' de situatie zelf aan te pakken (factor 4).

Met een dergelijke handelingsoptie wordt het voor Defensie mogelijk om straffen en leren te combineren en een boodschap af te geven aan politiek en media dat zij dergelijk gedrag niet tolereert en heeft ingestoken op het voorkomen in de toekomst. ■

22 Boskeljon-Horst, Van Baarle en Snoek, 'Helden zonder schurken. Een op herstel gerichte just culture in de praktijk'.

Nederlandse militairen maken zich gereed om met hun Patriots naar Slowakije te gaan. In april 2022 werd een Nederlandse-Duitse Air and Missile Defence Task Force ingezet in dat land om het luchtruim te beschermen. Het DACCC levert Command&Control voor dit soort operaties

‘Nederland, pak een leidende rol in de NAVO’

Interview met generaal-majoor Denny Traas, commandant-DACCC

Leonie Boskeljon-Horst, Freek Groen en Maarten Katsman

Kort nadat generaal-majoor Denny Traas startte als commandant van het Deployable Air Command and Control Centre (DACCC) van de NAVO begon Rusland de grootschalige invasie van Oekraïne. Traas, die in een voor hem nieuwe wereld van Command&Control op operationeel niveau werd geplaatst, kwam daardoor terecht in een omgeving die zelf ook compleet anders werd. Wat is en doet het DACCC, hoe paste het zich aan de nieuwe situatie aan, en hoe kan Nederland de ervaring van commandant Traas op deze positie gebruiken? ‘Ik begon deze functie met een heel ander beeld dan wat het uiteindelijk is geworden. Ik reken me rijk dat ik elke dag kan meedenken over militair optreden’, zegt Traas. ‘Ik ben nauw betrokken bij de planvorming op operationeel en strategisch niveau, zeg maar de oorlogsplannen van de NAVO. In Nederland kom je niet toe aan de concepten en plannen op dat hoogste militaire niveau.’

Het Deployable Air Command and Control Centre is gevestigd in Poggio Renatico in Noord-Italië. Het commando rouleert elke drie jaar tussen Italië en Nederland, met sinds januari 2022 dus de beurt aan de Nederlandse generaal-majoor Denny Traas. Traas begon bij de krijgsmacht als marinier en maakte later de overstap naar de luchtmacht, waar hij jachtvlieger werd. Met uitzendingen op de Balkan en in Afghanistan, commandofuncties op vliegbases en als directeur Operaties bij de luchtmacht heeft hij de juiste ervaring als commandant DACCC. ‘Bij de NAVO is de landenpolitiek duidelijk zichtbaar, elk land probeert toch zijn eigen belangen na te streven en dat maakt het vinden van compromissen noodzakelijk. Die dynamiek is wel enigszins te vergelijken met hoe ik het in mijn Haagse functies heb ervaren. De blootstelling aan beleid- en planvorming tijdens mijn carrière en mijn achtergrond in operaties bieden een goede basis voor deze functie, hoewel ik er niet specifiek voor ben opgeleid’, legt Traas uit.

FOTO NAVO

Standby-taak

DACCC is in feite ontstaan na de reorganisatie binnen de NAVO in 2013. Van de zeven bestaande CAOC’s (Combined Air Operations Centres) bleven er drie over, waarvan één deployable: DACCC. Het DACCC bestaat uit vier divisies, twee operationele en twee ondersteunende.[1] Ten eerste DARS, een afkorting waarachter mogelijk de langste naam voor een eenheid schuilgaat: het staat voor Deployable Air Control Centre,

1 Zie voor meer informatie over het DACCC: https://ac.nato.int/about/daccc.

Recognized Air Picture Production Centre and Sensor Fusion Post. DARS is verantwoordelijk voor de aansturing van luchtoperaties op tactisch niveau, bijvoorbeeld door air surveillance en het opstellen van luchtbeelden. Het oefent regelmatig zijn vaardigheid in snelle inzetbaarheid en flexibele integratie in de bestaande Air C2-structuur van de NAVO.

De tweede operationele divisie is het Deployable Air Operations Centre (DAOC). Dat levert onder andere C2-experts als de Joint Force Air Component (JFAC) wordt opgezet op het NAVO-hoofdkwartier voor luchtoperaties in Ramstein (Allied Air Command). Met de Training & Exercise Division en de Combat Service Support Division heeft DACCC twee ondersteunende eenheden in huis, bijvoorbeeld om luchtmachtpersoneel op te leiden en logistieke ondersteuning te verzorgen.

Binnen de NAVO hebben CAOC Uedem (Duitsland) en CAOC Torrejon (Spanje) een staande taak vanuit hun eigen locatie, zij zijn dagelijks belast met de air policing boven NAVO-grondgebied. ‘Wij (DACCC, red.) komen in beeld wanneer de spanning oploopt’, zegt Traas. ‘Wij staan gereed om snel inzetbaar te zijn op diverse fronten. Meteen na de Russische invasie in Oekraïne begin 2022 is de JFAC opgezet. Wij leverden daar direct mensen voor. Tegelijkertijd werd DACCC belast met het leveren van een team bij Joint Force Command Naples om de coördinatie met AIRCOM te versterken. Daarmee is de staande taak van DACCC eigenlijk het leveren van Air C2-capaciteit waar en wanneer dat nodig is.’ Naast de bemensing van de JFAC is er nog een concreet voorbeeld van de ondersteunende inzet door DACCC als gevolg van de Russische invasie van Oekraïne. DACCC leverde op verzoek sensors aan NAVO-bondgenoten aan de oostflank die zelf die capaciteit niet hebben, maar die daar wel behoefte aan hadden door de invasie. Er is bijvoorbeeld datalink-apparatuur ingezet om extra verbindingen mogelijk te maken. ‘Hiermee zijn gaten in de luchtverdediging gedicht langs de oostflank, wat laat zien dat het bondgenootschap werkt zoals het is bedoeld’, aldus Traas.

Netwerk NAVO

Zoals gezegd wisselen Italië en Nederland het commando over DACCC af. Er bestaat wel een subtiel verschil tussen hoe de twee landen dat invullen: Traas is voor honderd procent NAVO-functionaris. Zijn Italiaanse voorgangers en opvolgers hebben een dubbele pet op. Zij vullen de functie voor twintig procent als NAVO-generaal, en besteden daarnaast tachtig procent van hun tijd aan nationale taken.

Toch had ook generaal Traas een dubbele pet op. Direct na de invasie in Oekraïne werd hij door de commandant van het Allied Air Command (COMAIRCOM, momenteel USAF-generaal James B. Hecker) aangewezen als vertegenwoordiger (‘Deputy Commander Air’) bij het Joint Force

FOTO DACCC

Generaal-majoor Denny Traas is commandant van het Deployable Air Command and Control Centre (DACCC) van de NAVO

Command (JFC) in Napels.[2] 'Omdat je COMAIRCOM direct vertegenwoordigt zijn onderling vertrouwen en een goede kennis van de intenties van de commandant belangrijk. Uiteindelijk praat je in zijn naam met de leiding van het JFC.'

De JFC's (behalve Napels is er één in het Nederlandse Brunssum en één in Norfolk in de VS) en het Supreme Headquarters Allied Powers Europe (SHAPE, het NAVO-hoofdkwartier onder leiding van SACEUR) zijn zwaar onderbemand wat betreft air-expertise. 'De JFC-commandant heeft daarom veel baat bij een generaal in zijn team die advies kan geven over air-operaties, een rol die ik als Deputy Commander Air goed heb kunnen vervullen', zegt Traas. 'In de praktijk ben je dan veel bezig met relaties opbouwen om het wederzijdse vertrouwen te vergroten: met de commandant zelf, maar ook met zijn plaatsvervanger, de chief of staff, et cetera.'

Behalve op het gebied van persoonlijke relaties is het NAVO-bondgenootschap op meerdere vlakken een netwerkorganisatie. Zo heeft AIRCOM in Ramstein geen eigen middelen. Vliegtuigen en luchtverdedigingscapaciteiten moeten allemaal door de landen zelf geleverd worden. De NAVO beheert alleen de commandostructuur, bijvoorbeeld in de vorm van het DACCC. Met een grootschalige oorlog in Europa levert dat bepaalde uitdagingen op. Traas: 'Vroeger, in de Koude Oorlog, trainden we op snel overschakelen van een vredes- naar een oorlogssituatie. Sinds de invasie in 2022 zitten we meer in een langdurige crisis, je kunt die een tussenfase of grey zone noemen. Die tussenfase kan blijkbaar lang duren, en legde de afgelopen jaren het gebrek aan middelen bij de landen pijnlijk bloot. Hoewel de NAVO-landen genoeg "air assets" bij elkaar konden schrapen voor een respons op de invasie in Oekraïne, is de capaciteit voor een gewapend conflict met Rusland onvoldoende.'

DACCC zelf is een netwerk van vijftien deelnemende landen, hoewel niet ieder land even sterk vertegenwoordigd is. 'Er bestaat een wisselwerking tussen de kennis van de NAVO en individuele landen', legt Traas uit. 'Vanuit de landen komt soms heel specifieke expertise binnen, die ertoe leidt dat DACCC zijn eigen kennis ook vergroot. Sowieso zorgen onze mensen met allerlei verschillende achtergronden voor een smeltkroes die een schat aan kennis mogelijk maakt.' Vervolgens zorgt de opleidingstaak van DACCC voor een extra kwaliteitsimpuls: 'We zijn verantwoordelijk voor de initiële opleiding en training voor al het personeel dat een (oorlogs)taak heeft in de JFAC. Dat dwingt ons natuurlijk om zelf boven de stof te staan. In de praktijk zijn we dan ook een expertisecentrum op het gebied van Air Command and Control', stelt Traas.

'De capaciteit voor een gewapend conflict met Rusland is onvoldoende'

'Nederland, pak een leidende rol'

Op het moment dat DACCC werd opgericht had Nederland vrij weinig generaals op NAVO-posities. Deze openstaande commandofunctie bood dus een kans, die Nederland succesvol heeft gegrepen. Maar wat is nu effectief het resultaat, welke baat heeft Nederland bij het invullen van dergelijke functies? 'Vanuit mijn positie ben ik sinds enkele jaren nauw betrokken bij de operationele plannen en de ontwikkeling

2 In juni 2023 droeg Traas de rol van Deputy Commander Air Naples over aan de Commandant CAOC Torrejon.

Militairen scannen de omgeving tijdens oefening Ramstein Legacy, die zich richt op Integrated Air and Missile Defence (IAMD). Volgens Traas zou Nederland zonder extra investeringen een stevigere rol op zich kunnen nemen binnen de NAVO, bijvoorbeeld door de leiding te nemen op het gebied van IAMD

van het daarvoor benodigde militaire vermogen', legt Traas uit. Vanuit deze positie briefte hij een aantal keer de Krijgsmachtraad over de Regional Plans. 'Dat is absoluut een meerwaarde van dit soort NAVO-posities, dat je dicht op het vuur zit en de mogelijke kansen voor Nederland kunt identificeren en kunt vertalen naar de Nederlandse context.'

Een ander voorbeeld heeft te maken met de prioriteiten van AIRCOM in Ramstein. Met een specifiek daarvoor geformeerd team werkt Traas aan de ontwikkeling van plannen op het gebied van offensieve en defensieve luchtoperaties en de bijbehorende C2-structuur. Een onderdeel daarvan is het counteren van Russische A2/AD-capaciteiten (anti-access/area denial). 'Die vormen een groot strategisch probleem', aldus Traas, 'omdat sommige gebieden die Rusland kan bestrijken met A2/AD op Europees NAVO-grondgebied liggen. Wat wij hieraan kunnen

FOTO NAVO

bijdragen met een klein aantal Nederlanders in het team maakt echt verschil. Dat verbetert de Nederlandse positie binnen het bondgenootschap en de Nederlandse defensie heeft daar indirect baat bij.'

In een eerder interview met de *Militaire Spectator* stelde luitenant-generaal Elanor Boekholt-O'Sullivan dat het soms nodig is 'stenen in de vijver' te gooien. Die stenen veroorzaken rumoer dat tot wezenlijke verandering kan leiden

'Nederland kan veel meer dan naar rato bijdragen aan de NAVO'

binnen Defensie.[3] Niet wetend wie de vraag zou krijgen, was haar vraag voor een volgend interview: 'welke steen is de volgende?' Generaal Traas betoogt dat die steen gaat om het afwerpen van bescheidenheid: 'met de kennis en kunde die de Nederlandse krijgsmacht heeft kunnen we in mijn ogen veel meer dan naar rato bijdragen. Door de leiding te nemen in en op specifieke gebieden en sleutelmissies, bijvoorbeeld op het gebied van counter A2/AD en integrale lucht- en raketverdediging (wat overigens joint missies pur sang zijn), kan met dezelfde investering een stevigere rol worden genomen. Vervolgens ontstaat een sterkere positie en daarmee invloed binnen de NAVO. Dit vereist natuurlijk wel een bredere strategie binnen het Nederlands Defensie- en Veiligheidsbeleid.'

Het onderwerp strategie leidt ten slotte tot de vraag die generaal Traas wil stellen in een volgend interview in de *Militaire Spectator*: 'Moet Nederland een *Grand Strategy* opstellen, en zo ja, waaruit bestaat die?' ■

3 L. Boskeljon-Horst en M. Katsman, 'Rechtop en trots in een pak dat past. Interview met Elanor Boekholt-O'Sullivan', *Militaire Spectator* 193 (2024) (4). Zie: https://militairespectator.nl/artikelen/rechtop-en-trots-een-pak-dat-past.

‘Kritiek is goed, dat houdt je scherp’

Historicus Rémy Limpach blikt terug op zijn tijd in Nederland

Door Alex Claver en Frans van Nijnatten

De Indonesische onafhankelijkheids- of dekolonisatieoorlog is met pieken onderwerp van debat in Nederland.[1] Met zijn proefschrift *De brandende kampongs van Generaal Spoor* gooide historicus dr. Rémy Limpach in 2016 een steen in de discussievijver. Het boek leidde tot Kamervragen en er kwam een nieuw historisch onderzoek naar de oorlog van 1945-1949. Limpach werkte mee aan dat wetenschappelijk onderzoek en vorig jaar verscheen zijn deelstudie *Tasten in het duister*. Nu hij na tien jaar het Nederlands Instituut voor Militaire Historie om privéredenen verlaat om terug te gaan naar Zwitserland kijkt hij in een interview met de *Militaire Spectator* terug op zijn tijd in Nederland, de kritiek op het grote Indonesië-onderzoek en de rol van de media.

De Zwitsers-Nederlandse historicus Rémy Limpach (1974) is senior wetenschappelijk medewerker bij het Nederlands Instituut voor Militaire Historie. Hij promoveerde in 2015 aan de Universiteit van Bern op het proefschrift *Die brennenden Dörfer des General Spoor. Niederländische Massengewalt im indonesischen Unabhängigkeitskrieg 1945-1949*. Momenteel werkt hij aan een boek over de oorlog in Nieuw-Guinea, dat volgend jaar verschijnt.

In februari 2022 presenteerden de drie onderzoeksinstituten KITLV, NIMH en NIOD de resultaten van het onafhankelijk uitgevoerde onderzoeksprogramma Onafhankelijkheid, Dekolonisatie, Geweld en Oorlog in Indonesië, 1945-1950 (ODGOI). In 2012 had de regering een verzoek om financiering van een dergelijk onderzoek nog afgewezen. Mede aanleiding dat er uiteindelijk wel geld beschikbaar kwam voor zo’n onderzoek was het verschijnen van *De brandende kampongs van Generaal Spoor* van Rémy Limpach in 2016, een bewerking en vertaling van zijn proefschrift.[2] ‘Ik begon aan mijn promotieonderzoek omdat ik een lacune zag in de historiografie over de geweldpleging in de onafhankelijkheidsoorlog in Indonesië’, licht hij toe. Hij werd gedreven door zijn interesse in koloniale geschiedenis en aangemoedigd door zijn Duitse promotor aan de Universiteit van Bern, prof. dr. Stig Förster. ‘Förster is een specialist op het gebied van internationale geweldsstudies. Hij is militair historicus en ‘van alle oorlogen thuis’. Förster stimuleert zijn promovendi om door verhulling en eufemismen heen te prikken, man en paard te noemen en juist ook kritisch te staan tegenover de eigen nationaliteit, organisatie en groep.’ Het viel Limpach op dat er vooral over wat hij de ‘schaduwkanten’ van de oorlog in Indonesië noemt weinig was gepubliceerd. ‘Ik las *Ontsporing van geweld* van Van Doorn en Hendrix, een goede historisch-sociologische studie uit 1970

1 Zie voor een toelichting op de terminologie Gert Oostindie, ‘Achtergrond, uitgangspunten en werkwijze’, in: Gert Oostindie, Ben Schoenmaker en Frank van Vree (red.), *Over de grens. Nederlands extreem geweld in de Indonesische Onafhankelijkheidsoorlog, 1945-1949* (Amsterdam, Amsterdam University Press, 2022) 29.

2 Tweede Kamer, ‘Brief van de ministers van Buitenlandse Zaken, van Defensie en staatssecretaris van Volksgezondheid, Welzijn en Sport’ (2 december 2016) 26 049, nr. 82.

Rémy Limpach over zijn positie als onderzoeker:
'Bij het NIMH heeft niemand mijn pen vastgehouden'

FOTO MILITAIRE SPECTATOR

waar ik veel respect voor heb.[3] Sindsdien bleek er echter niet veel nieuw wetenschappelijk werk over het extreme geweld ten tijde van de Indonesische onafhankelijkheidsoorlog gepubliceerd te zijn. Ik besloot onderzoek te gaan doen naar extreem militair geweld en toen ik als promovendus de financiering rond had en me grondig had ingelezen ben ik in 2011 naar Nederland gegaan.'

Bijna 15 maanden lang bivakkeerde Limpach dagelijks in het Nationaal Archief in Den Haag, waar hij talloze bronnen las en netwerkte om op de hoogte te komen van de stand van het onderzoek in Nederland. 'Ik kreeg van collega-historici waardevolle adviezen over relevante contacten, literatuur en archieven. Terwijl ik in het archief zat las ik in de media met de nodige belangstelling ook over de rechtszaken die toen speelden, onder meer rond het bloedbad van Rawagede in december 1947.' In september 2011 honoreerde de rechtbank in Den Haag claims van een overlevende en zeven weduwen van slachtoffers van wederrechtelijke executies in dat dorp en veroordeelde de Nederlandse Staat tot het betalen van een schadevergoeding.[4] Een jaar later werd in Enschede in een vuilcontainer een fotoalbum gevonden waarin foto's van executies tijdens de oorlog in Indonesië zaten. Ook dit nieuws haalde de voorpagina, in dit geval van *de Volkskrant*.[5] 'Langzaam ging ik beseffen dat er voor mijn onderzoek weleens aandacht zou kunnen ontstaan in Nederland. Tot dan was ik ervan uitgegaan dat ik, net als de meeste andere historici, blij moest zijn als ik überhaupt een uitgever zou vinden en dat het dan een Duitstalige publicatie zou worden waar verder geen haan naar zou kraaien.'

Na het vonnis van 2011, dat Limpach 'baanbrekend' noemt, kwamen er meer claims van nabestaanden van slachtoffers van extreem Nederlands geweld in Indonesië. Het NIMH deed daar historisch verificatieonderzoek naar. In 2013, midden in de schrijffase van zijn proefschrift, kreeg Limpach, die inmiddels naar Zwitserland was teruggekeerd, het aanbod om claimonderzoeker op het NIMH te worden, maar hij koos ervoor eerst zijn dissertatie zover mogelijk af te maken. In de zomer van 2014 trad hij alsnog in dienst, maar vooralsnog vooral om de omvangrijke dagboekencollectie van het NIMH te bestuderen en te ontsluiten. Rond die tijd publiceerde hij ook een samenvattend artikel over zijn promotieonderzoek in een internationaal vaktijdschrift.[6] 'Anne-Lot Hoek, historica en *NRC*-journalist, las in 2015 mijn artikel en stelde vast dat mijn conclusies haaks stonden op de tot dan toe geldige officiële lezing dat er in Indonesië slechts incidentele excessen hadden plaatsgevonden, wat zij nieuwswaardig achtte.[7] Ze verzocht me om een interview, maar ik vroeg haar daarmee te wachten tot mijn boek af was. Zij wilde echter zo snel mogelijk publiceren. Op 15 augustus 2015, precies 70 jaar na de Japanse capitulatie in de Tweede Wereldoorlog, publiceerde *NRC* op de voorpagina over mijn onderzoek. De krant leek daarmee Nederlands daderschap te benadrukken, terwijl de koning en de premier op die dag bij het Indisch Monument in Den Haag stonden om Nederlandse slachtoffers van Japanse gruwelen te herdenken. De citaten die Hoek in haar stuk gebruikte kwamen overigens uit mijn artikel. Daarna kwamen talrijke journalisten met vragen en verzoeken bij mij op het net, maar ik hield de boot af: ik wilde eerst klaar zijn met mijn dissertatie.'

Limpach verdedigde zijn proefschrift in september 2015 aan de Universiteit van Bern. 'Het daaropvolgende vertaalproces – want de markt voor dit boek was in Nederland – duurde een jaar.' Op 29 september 2016 presenteerde hij *De brandende kampongs van Generaal Spoor* in Nieuwspoort in Den Haag. Limpach waardeerde dat hij bij een organisatie als Defensie alle ruimte kreeg om kritisch en onafhankelijk wetenschappelijk onderzoek uit te voeren. 'Bij het NIMH heeft

3 J.A.A. van Doorn en W.J. Hendrix, *Ontsporing van geweld. Het Nederlands-Indonesisch conflict* (heruitgave) (Zutphen, Walburg Pers, 2019).

4 Zie: Rechtspraak.nl, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBSGR:2011:BS8793.

5 Laura de Jong en Marjan van den Berg, 'Opgedoken executiefoto's: 'Het was dus echt oorlog'', *de Volkskrant*, 10 juli 2012.

6 Rémy Limpach, 'Business as usual. Dutch mass violence in the Indonesian War of Independence', in: Bart Luttikhuis en Dirk Moses (red.), *Colonial counterinsurgency and mass violence. The Dutch empire in Indonesia* (Londen, Routledge, 2014).

7 Anne-Lot Hoek, 'Op de vlucht neergeschoten', *NRC*, 15 augustus 2015.

Kick-off onder grote publieke belangstelling van het grote Indië-onderzoek in Pakhuis De Zwijger in Amsterdam, 2017 FOTO MARCEL ISRAEL

niemand mijn pen vastgehouden.' Na de hernieuwde ophef kwamen Kamervragen over Limpachs boek en begin december 2016 stelde de regering wel financiële middelen beschikbaar voor een breed historisch onderzoek door het NIOD Instituut voor Oorlogs-, Holocaust- en Genocidestudies, het Koninklijk Instituut voor Taal-, Land- en Volkenkunde en het Nederlands Instituut voor Militaire Historie. 'Soms wordt het zo geframed dat mijn boek daarvoor de directe aanleiding vormde, maar het eerste onderzoeksverzoek van de instituten lag er dus al in 2012', verduidelijkt Limpach, die bovendien benadrukt dat juist ook de claims doorslaggevend waren. In mindere mate gold dat ook voor journalistiek werk en ander historisch onderzoek, zoals het in 2015 gepubliceerde boek *Soldaat in Indonesië* van Gert Oostindie, waarin hij en zijn medeauteurs, net als eerder Limpach, stelden dat Nederlandse militairen in Indonesië structureel extreem geweld pleegden.

Limpach verrichtte voor zijn dissertatie omvangrijk en divers empirisch onderzoek. Zo toetste hij door direct betrokkenen geschreven bronnen aan overheidsarchieven, collecties van particulieren en hield hij interviews met veteranen. 'Oral history en egodocumenten staan in mijn onderzoek overigens nooit op zichzelf; het zijn waardevolle aanvullingen op de officiële bronnen. Een historicus moet uiteenlopende bronnen immers altijd complementair gebruiken.' Egodocumenten als dagboeken en soldatenbrieven kunnen volgens Limpach sporen opleveren naar bij een breed publiek onbekende incidenten die onderzoekers vervolgens aan

'Vooral de dagboeken laten zien wat een afstompend of verruwend effect een grimmige en langdurige guerrillastrijd tegen een 'onzichtbare' en 'ongrijpbare' tegenstander op een militair kan hebben'

officiële rapportages kunnen spiegelen. Maar ook die aanpak kent de nodige valkuilen, waarschuwt hij. 'Geschiedschrijving is geen exacte wetenschap. Iedere bron, zoals een patrouillerapport, bestuurlijk verslag of dagboek, is immers door een mens opgesteld en per definitie subjectief. Iedere bron heeft ook een bepaalde intentie, meestal om genomen besluiten achteraf te rechtvaardigen. Daar moeten historici met zorgvuldige bronnenkritiek doorheen kunnen prikken.' Verder moet een historicus bereid zijn, juist als hij patronen wil opsporen, grote hoeveelheden uiteenlopende bronnen te verzamelen en te analyseren. Zodoende ging Limpach 'met een breed sleepnet' door de archieven, 'ook omdat ik er toen nog van uit ging dat er de komende 20-30 jaar misschien niemand nog serieus naar zou gaan kijken'.

Kritiek en veteranen

Oostindie kreeg in 2015 de wind van voren van veteranen en hun organisaties, hoewel hij in één van zijn hoofdstukken benadrukte dat de meeste militairen die naar Indonesië werden gestuurd niets wisten van oorlogsmisdrijven en zeker geen daders waren.[8] Rond de publicatie in 2016 van *De brandende kampongs van Generaal Spoor* schreef Limpach: 'Dat de harde conclusie 'structureel extreem geweld' veel veteranen kwetst die daaraan part noch deel hadden is begrijpelijk. De vaststelling dat Nederlandse militairen structureel extreem geweld toepasten wil echter niet zeggen dat *de* Nederlandse militairen oorlogsmisdadigers waren. De meerderheid hield namelijk schone handen'.[9] In de Kamerbrief waarin in december 2016 een 'breed opgezet' onderzoek werd aangekondigd naar 'de context van het geweldsgebruik en de periode van dekolonisatie' in Indonesië schreef het kabinet dat alle oud-militairen die in opdracht van de Nederlandse regering naar conflictgebieden zijn uitgezonden waardering verdienen en dat een 'belangrijke conclusie' van Limpach luidde dat 'het merendeel van de Nederlandse militairen niet betrokken was bij extreme gewelddaden'.[10] 'Er waren inderdaad ook veel militairen met een intact moreel kompas', is nog steeds zijn overtuiging. Bovendien lag de hoofdverantwoordelijkheid bij de regering en de legerleiding, benadrukt hij. 'Dat betekent echter niet dat de individuele militair die over de schreef ging moet worden ontzien.'

Ondanks de vaststelling van meerdere onderzoekers en het kabinet dat de meeste naar Indonesië uitgezonden militairen niet direct bij buitensporig geweld betrokken waren, hagelde het tijdens het grote Indonesië-onderzoek kritiek van veteranen en hun organisaties. Tijdens het ODGOI-onderzoek kwamen veteranenvoormannen onder meer met het verwijt dat de onderzoekers oordelen naar de morele en juridische maatstaven van nu. 'Wij zeggen dan: nee, het martelen en vermoorden van gevangenen was toen ook al verboden', aldus Limpach, 'maar ze bleven het verwijt stug herhalen.' Ook zouden de onderzoekers de veteranen collectief veroordelen en Indonesisch geweld negeren. Limpach noemt dergelijke beweringen een 'kwalijke framing van het onderzoek door veteranenkopstukken, waardoor sommige veteranen de ODGOI-boeken niet zullen lezen omdat zij denken bij voorbaat als oorlogsmisdadiger te worden weggezet'. In een reactie op de presentatie van de resultaten van het ODGOI-onderzoek liet directeur-bestuurder Paul Hoefsloot van het Nederlands Veteraneninstituut weten geschrokken te zijn 'van sommige nogal

8 Willem Bouwman, 'Nederlandse oorlogsmisdadigers in Indië', *Nederlands Dagblad*, 30 oktober 2015.

9 Rémy Limpach, 'Extreem Nederlands militair geweld tijdens de Indonesische onafhankelijkheidsoorlog 1945-1949. 'Brengun erover en zo gauw mogelijk terug naar Holland'', *Militaire Spectator* 185 (2016) (10) 418-419.

10 Tweede Kamer, 'Brief van de ministers van Buitenlandse Zaken, van Defensie en staatssecretaris van Volksgezondheid, Welzijn en Sport' (2 december 2016) 26 049, nr. 82, 3, 5.

generaliserende conclusies over het toegepaste extreme geweld'. Het VI noemde het onderzoek eenzijdig, maar Martin Elands, als militair historicus aan hetzelfde instituut verbonden, noemde het 'grote winst dat het onderzoek op overtuigende wijze aantoont dat politici, bestuurders, ambtenaren en rechters net zo zeer verantwoordelijk waren door geweld te tolereren, te rechtvaardigen en onbestraft te laten. Voor het eerst wordt de trap van bovenaf schoon geveegd!'[11]

De conclusie van het ODGOI-onderzoek dat het hoogste Nederlandse dek hoofdverantwoordelijk was voor het structureel extreme geweld in Indonesië laat zien dat het debat over de dekolonisatie-oorlog nog steeds een ontwikkeling doormaakt. In 1969 kreeg de discussie een soortgelijke impuls toen Indonesiëveteraan Joop Hueting in *Achter het nieuws* bij de VARA vertelde dat hij als dienstplichtig militair in Indonesië bij martelingen en executies aanwezig was geweest. Na Kamervragen liet de regering destijds een haastige archiefinventarisatie uitvoeren. Bij het aanbieden in juni van wat de *Excessennota* zou gaan heten noemde premier Piet de Jong het rapport onevenwichtig, omdat het slechts 'negatieve feiten' bevatte. De Jong schreef verder dat het 'niet nieuw' was om te constateren dat Nederlandse militairen 'wandaden' hadden gepleegd in Indonesië. De regering handhaafde evenwel haar inmiddels achterhaalde opvatting 'dat de krijgsmacht als geheel zich in Indonesië correct heeft gedragen'.[12] Door de ophef publiceerden de Indiëveteranen Van Doorn en Hendrix hun verslagen over extreem geweld, die zij na de oorlog hadden laten liggen, in 1970 alsnog.

Net als historica Stef Scagliola in 2002[13] spitte Limpach voor zijn proefschrift alle 885 brieven door die de VARA in 1969 kreeg na de onthullingen van Joop Hueting. 'Ik stelde vast dat ongeveer 60 procent van de inzenders Hueting een landverrader, nestbevuiler of leugenaar noemde, terwijl 40 procent zijn ervaringen deelde en meende dat het eindelijk eens goed zou zijn een nationaal debat over de Nederlands-Indonesische oorlog en de in die tijd gepleegde misdaden te voeren.'

'Ondanks mijn harde conclusies over structureel extreem geweld wil ik duidelijk stellen dat ik veteranen enorm waardeer', zegt Limpach. 'Juist doordat ik zoveel dagboeken heb gelezen en interviewcollecties geraadpleegd heb, heb ik ook veel begrip voor Indonesiëveteranen. Als onderzoeker denk je ook: hoe zou ik me hebben gedragen in zo'n situatie? Ik kan niet uitsluiten dat ik in die specifieke context ook niet over de schreef gegaan zou zijn. Vooral de dagboeken laten zien wat een afstompend of verruwend effect een grimmige en langdurige guerrillastrijd tegen een 'onzichtbare' en 'ongrijpbare' tegenstander op een militair kan hebben. Als onderzoeksgroep hebben we dan ook aandacht besteed aan de meer structurele oorzaken van extreem geweld, zoals een chronisch troepentekort, straffeloosheid, slechte opleiding, gebrek aan taal- en cultuurkennis, een ondoordachte strategie, onvoldoende leiderschap en ook misleidende propaganda met een oriëntalistisch-racistische kijk op de Indonesiërs en hun antikoloniale vrijheidsstrijd.'

Limpach constateert dat het debat rond zijn boek en het ODGOI-onderzoek uiterst gepolariseerd was, waarbij veelal op de persoon werd gespeeld zodat hij en zijn collega's een dikke huid moesten ontwikkelen. Volgens hem past dit 'bij de internationale tendens van het verdacht maken van kritische wetenschappers, zoals die ook te zien is in andere disciplines als de klimaatwetenschap. Als collectieve onderzoeksgroep hebben we van extreem-links en -rechts heel veel naar ons hoofd gekregen, van 'NSB-historici', 'woke historici', 'nestbevuilers', 'geschiedsvervalsers', 'moraalridders', tot 'koloniale witwassers' en 'racisten'. Ik kreeg ook herhaaldelijk te maken met persoonlijke aanvallen, die in feite smaad waren en doelden op mijn integriteit. Zo werd mijn doctortitel door een luidruchtig groepje reactionaire en

11 'Nederlands Veteraneninstituut steekt Indiëveteranen hart onder de riem' (Doorn, Veteraneninstituut, 17 februari 2022).

12 Jan Bank (inleiding), *De Excessennota. Nota betreffende het archiefonderzoek naar de gegevens omtrent excessen in Indonesië begaan door Nederlandse militairen in de periode 1945-1950* (Den Haag, Sdu Uitgeverij, 1995) 31-32.

13 Stef Scagliola, *Last van de oorlog. De Nederlandse oorlogsmisdaden in Indonesië en hun verwerking* (Amsterdam, Uitgeverij Balans, 2002).

Aankomst van het troepentransportschip Sloterdijk in Tandjong Priok, 1946: 'Als ik veteranen persoonlijk sprak kwamen er meer dan eens verhalen los over wat ze aan nare zaken meegemaakt hadden, zoals een marteling of het platbranden van een kampong'

dilettantische amateurhistorici in twijfel getrokken. Volgens hun tenenkrommende complottheorieën had mijn copromotor Peter Romijn van het NIOD mij destijds in Zwitserland al aangezet tot mijn onderzoek om zo ooit miljoenen los te kunnen weken van de Nederlandse Staat voor het ODGOI-project. Ik zou dan een willoze pion in het hele verhaal geweest zijn. Wat een onzin'. De afgelopen jaren heeft Limpach ook met veteranen kunnen spreken. 'Sommigen waren kritisch, maar als dat onderbouwd was dan is dat nuttig om als historicus scherp te blijven. Kritiek, ook van bijvoorbeeld links-activistische kant, heeft in die zin zeker iets positiefs. Als ik veteranen persoonlijk sprak kwamen er trouwens meer dan eens verhalen los over wat ze aan nare zaken meegemaakt hadden, zoals een marteling of het platbranden van een kampong.' Eén van de veteranen die veel indruk op Limpach maakte en ook een waardevolle getuige voor zijn onderzoek vormde is Bert Carper, inlichtingenofficier tijdens de oorlog in Indonesië. 'Maar eigenlijk vond ik ieder gesprek met veteranen verrijkend, want ze waren immers ooggetuigen en kwamen meestal met interessante anekdotes over hun wel en wee over de brug.'

De Indonesische kant

In de Kamerbrief waarin het kabinet de financiering aankondigde stond dat het onderzoek veelomvattend zou moeten zijn en de regering liet het verder aan de drie instituten over om dat inhoudelijk in te vullen.[14] In het samenvattende

14 'Een dergelijk onderzoek dient zich niet te beperken tot de geweldspleging door alle partijen waar veel deelstudies zich op richten, doch nadrukkelijk in te gaan op de brede context van de naoorlogse dekolonisatie (inclusief samenleving) en het politiek, bestuurlijk, justitieel en militair optreden in 1945–1949 in voormalig Nederlands-Indië/Indonesië, zowel vanuit Haags als vanuit lokaal perspectief. Het is belangrijk dat een vervolgonderzoek een integrale benadering hanteert en dieper ingaat op zaken die aan bod zijn gekomen in de studie van dr. Limpach. De geweldsspiraal tijdens de zogenaamde 'Bersiap' zal in een onderzoek worden betrokken. Ook de politieke besluitvorming in Den Haag over de dekolonisatie, de brede steun in Nederland voor het behoud van de relatie met Nederlands-Indië/Indonesië en de uitzending en het optreden van de Nederlandse militairen, de beperkte informatievoorziening, als ook de nasleep na 1949 en de veteranenzorg, verdienen nader onderzoek. Waar mogelijk wordt samenwerking gezocht met partners in het buitenland, zoals Indonesië, het Verenigd Koninkrijk, Japan, Australië en de Verenigde Staten. Verder moeten belanghebbenden de gelegenheid krijgen informatie aan te reiken, waar gewenst in de vorm van interviews met betrokkenen die dat wensen, inclusief veteranen, en via het ter beschikking stellen van brondocumenten'. Zie: Tweede Kamer, 'Brief van de ministers van Buitenlandse Zaken, van Defensie en staatssecretaris van Volksgezondheid, Welzijn en Sport' (2 december 2016) 26 049, nr. 82, 4-5.

slotwerk *Over de grens* staat dat het onderzoek door sommige Indonesische media werd bekritiseerd als een poging van Nederland het eigen blazoen op te poetsen. Indonesische diplomaten lieten zowel de regering in Den Haag als de onderzoeksinstituten weten 'ernstige reserves te koesteren met het oog op een mogelijke belasting van de bilaterale relaties'. Daardoor kwamen er 'minder Indonesische bronnen over de geweldsdynamiek naar boven' dan gehoopt, terwijl Indonesische historici die aan het onderzoek meewerkten hun eigen prioriteiten stelden. Het ODGOI-onderzoek is daardoor 'in een beperkt aantal opzichten niet uitgevoerd zoals voorzien'.[15] Willem Bouwman van het *Nederlands Dagblad* schreef in 2015 al dat het boek van Gert Oostindie de Indonesische kant van de zaak onderbelicht liet, 'omdat de Indonesiërs geen behoefte hebben aan onderzoek: de uitkomsten zouden het mythische verhaal van de heldhaftige vrijheidsstrijd tegen de Nederlandse onderdrukkers kunnen weerspreken'.[16]

Hoe kijkt Limpach daar tegenaan? 'Indonesische historici hebben absoluut hun nek uitgestoken om tijdens het afgelopen project hun kant van de Indonesische revolutie te onderzoeken', zegt hij. 'Zij hebben daarbij deels op eieren moeten lopen, maar historici als Bambang Purwanto en Abdul Wahid hebben hun eigen onderzoeksagenda kunnen bepalen. Gelukkig komt er in Indonesië ook steeds meer onafhankelijke geschiedschrijving op. Zo heeft Bambang Purwanto intussen in Indonesië al aardig wat studenten en promovendi opgeleid tot kritische historici. In Indonesië hebben hij en collega's het verwijt gekregen dat ze geld aannemen van 'belanda's', met de vraag: zijn jullie nog wel onafhankelijk? Bambangs tegenargumenten zijn dat hij in Indonesië zoveel geld niet krijgt om historisch onderzoek naar onderbelichte aspecten van de onafhankelijkheidsstrijd te doen en dat hij aan niemands leiband loopt. Vanuit Nederland is dan ook niet voorgekauwd wat zij zouden moeten onderzoeken. De samenwerking met de Indonesiërs was deels zeer intensief en wierp wederzijds vruchten af, bijvoorbeeld op het gebied van terminologie, invalshoeken en cultureel besef. De Nederlandse onderzoekers hebben dan ook veel belangrijke inzichten, contacten en toegang tot Indonesische bronnen aan deze coöperatie te danken, denk aan gezamenlijke workshops aan Indonesische universiteiten of met Indonesische hulp uitgevoerd veldonderzoek. Maar omgekeerd zijn voor Indonesiërs nu ook veel relevante feiten bekend die voor het ODGOI-onderzoek in Nederlandse archieven begraven lagen.' De aan het begin van het project geuite kritiek van bepaalde critici uit de links-activistische hoek dat de Indonesische collega-onderzoekers 'white faces with brown masks' zouden zijn noemt Limpach 'absurd'.

Tasten in het duister

In zijn proefschrift besteedde Limpach al aandacht aan 'systematisch martelende inlichtingendiensten' en hij werkte dat thema voor het ODGOI-onderzoek uit tot het boek *Tasten in het duister*. 'Dat was voor mij een kans om inhoudelijk nieuw terrein te betreden, omdat ik altijd zeer geïnteresseerd ben geweest in het inlichtingenveld. Ik raakte ook geïntrigeerd door een vaststelling van militair historicus Jaap de Moor, die schreef dat elke koloniale expeditie en zelfs elke Nederlandse patrouille in Indonesië afhankelijk was van autochtone spionnen of informanten. Maar juist over die informanten, door de Indonesiërs als verraders beschouwd, was tot dusver niets bekend. Daarom ga ik in *Tasten in het duister* uitvoerig in op hun selectie, motieven, bescherming, achtergrond en aansturing.' Naar de Nederlandse inlichtingendiensten kijken zonder ook de tegenstander goed onder de loep te nemen was volgens Limpach ook niet mogelijk; een tegenstander die in de inlichtingenstrijd eveneens structureel extreem geweld toepaste. 'Ik ga in het boek nadrukkelijk in op Indonesisch extreem geweld, hoewel sommige critici zeggen dat mijn collega's en ik dat zouden negeren.' In Limpachs proefschrift kwam Indonesisch massageweld overigens ook al ruimschoots aan bod. 'Het bloed spat bij wijze van spreken van

15 Gert Oostindie, 'Achtergrond, uitgangspunten en werkwijze', in: Oostindie, Schoenmaker en Van Vree (red.), *Over de grens*, 22.

16 Willem Bouwman, 'Nederlandse oorlogsmisdadigers in Indië', *Nederlands Dagblad*, 30 oktober 2015

Het opbrengen van een Indonesische para die in de buurt van Merauke in Nieuw-Guinea gevangen is genomen: Limpach noemt de continuïteiten met de oorlog van 1945-1949 'frappant'

die pagina's af. Of het geweld in naam van de vrijheidsstrijd, het kolonialisme of rust en orde plaatsvindt, moord blijft moord en doodslag blijft doodslag. Dat Indonesië misschien aan de 'goede kant' van de geschiedenis staat, betekent niet dat historici Indonesisch geweld tijdens de onafhankelijkheidsoorlog moeten negeren, want dat zijn immers ook belangrijke feiten die onder meer directe gevolgen voor de bereidheid tot geweldpleging door sommige Nederlanders kunnen hebben gehad. Het is de taak van historici om te zoeken naar verklaringen, niet om zelf te veroordelen.'

Ontwikkeling als historicus

'Bij het NIMH heb ik een ontwikkeling naar militair historicus doorgemaakt en de Defensie-organisatie beter leren kennen. Ik heb met name door het lezen van dagboeken, soldatenbrieven en memoires meer begrip voor militairen en hun veelal lastige positie in het veld gekregen; een onderzoeker aan een universiteit staat daar vaak verder vanaf. Daardoor werken ze wellicht met aannames die niet altijd kloppen of zoeken ze te veel achter bepaalde militaire termen als 'zuiveringen' of 'vernietigen', termen die in de militaire context een specifieke betekenis hebben. Te veel begrip voor militairen hebben en hun stellingen klakkeloos overnemen is uiteraard ook niet goed, des te meer omdat de krijgsmacht een lerende organisatie wil zijn en men juist het meest van eigen fouten en van moeilijke periodes kan leren.' Limpach wijst op voorgangers bij het instituut die kritische wetenschappers bleken, zoals Petra Groen en Jaap de Moor. Dat is volgens hem bijzonder,

FOTO NATIONAAL ARCHIEF

‘want er zijn nog genoeg landen waar de militair-historische dienst niets meer is dan een zuiver propaganda-instituut’.

In zijn NIMH-tijd voerde Limpach nog meer werkzaamheden uit dan het ODGOI-project en was hij onder meer betrokken bij het onderzoek dat in mei 2024 tot de postume rehabilitatie leidde van de drie mariniers Joop de Hoog, Louis Stokking en Martinus Smit. Dit trio had op 11 augustus 1947 het bevel geweigerd een kampong bij Pakisaji op Oost-Java in brand te steken. Zij hadden ernstige morele en godsdienstige bezwaren, maar werden destijds tot lange gevangenisstraffen veroordeeld in verhouding tot de milde straffen of vrijspraken die Nederlandse militairen normaliter kregen die ernstige misdaden hadden gepleegd – als er überhaupt al strafrechtelijk onderzoek plaatsvond. ‘Het was fijn om dit onderzoek te doen, het ging immers om militairen die juist niet over de schreef wensten te gaan en hun geweten volgden.’

Tot Limpachs verbazing is er nog bijna niets gepubliceerd over ‘onoorbare praktijken’ van Nederlandse militairen in de strijd tegen Indonesische infiltranten en weerbarstige papoea-clans in Nieuw-Guinea

Limpach begon recent aan een onderzoek naar Nieuw-Guinea, dat na de onafhankelijkheidsoorlog Nederlands was gebleven en ‘waar nog veel geweld is toegepast’ voordat het gebied na 1962 alsnog bij Indonesië werd gevoegd. ‘Frappant zijn de continuïteiten met de oorlog van 1945-1949’, vertelt hij. ‘In sommige gevallen gewoon weer kampongs in de as leggen, alle schandalen in de doofpot stoppen, KNIL-voorschriften weer te voorschijn halen. Vergeleken met de eerdere oorlog in Indonesië waren de onoorbare praktijken weliswaar minder omvangrijk, met zo’n 30.000 uitgezonden Nederlandse militairen in plaats van 220.000. Ze moesten het opnemen tegen in totaal zo’n 2.000 Indonesische infiltranten en enkele opstanden van weerbarstige Papoeaclans de kop indrukken. Daarbij is wel het nodige gebeurd, waar tot mijn verbazing nog vrijwel niets over gepubliceerd is. Het ligt in het archief voor het oprapen en ik vind het vreemd dat nog geen enkele historicus dat voor een onderzoek gebruikt heeft.’ Als voorbeeld waar het mis ging noemt Limpach de Slag bij Vlakke Hoek in januari 1962, waar de Nederlandse marine een Indonesisch schip tot zinken bracht. ‘De Nederlanders haalden vijftig drenkelingen uit het water en brachten die naar het vasteland. Nederland stond niet toe dat die gevangenen bezocht werden door een vertegenwoordiging van de Indonesische regering, maar ging wel akkoord met een bezoek van een Zwitserse afgevaardigde van het Internationale Rode Kruis. Die afgevaardigde kreeg van negen gevangenen te horen dat de Nederlanders hen hadden mishandeld. Daarop stelde de legerleiding een onderzoekscommissie in, die dat inderdaad bewezen achtte. Maar uiteindelijk liep het niet zo’n vaart: er werden twee of drie militairen overgeplaatst en daarmee was de kous af. Na hun vrijlating vertelden de negen gevangenen in Jakarta voor de media dat zij waren mishandeld. Defensie deed dat af als Indonesische propaganda, ondanks de bevindingen van de onderzoekscommissie.’

Limpach heeft zijn focus lang op Indonesië gelegd, met Nieuw-Guinea als een soort *encore*. Er zijn echter nog veel andere onderwerpen die hem interesseren. ‘Ik zou niet met alle macht meer terug willen naar de Indonesische revolutie, maar liever verder de geschiedenis in,

bijvoorbeeld het interbellum of de Atjehoorlog, of juist vooruit, naar de Korea-Oorlog. Een internationaal vergelijkend onderzoek sluit ik ook niet uit. Maar ook wat betreft de Indonesische onafhankelijkheidsoorlog ligt er nog veel werk, zoals onderzoek naar specifieke eenheden, acties en regio's. Ook zijn er geen biografieën van belangrijke kopstukken als procureur-generaal Felderhof of Buurman van Vreeden, de plaatsvervanger van bevelhebber Spoor.' Of hij volgend jaar in Zwitserland als wetenschapper blijft werken weet Limpach nog niet: 'Het zou ook leraar of journalist kunnen worden. Het is ongewis'.

Hoe laat Limpach het debat achter?

In een eerste reactie in 2022 zei de regering dat het ODGOI-onderzoek duidelijk heeft gemaakt dat Nederlandse militairen destijds door politieke besluitvorming moesten 'deelnemen aan wat – in retrospectief – een onmogelijke missie was'.[17] Dat er een proces gaande is om niet meer weg te kijken van het verleden bewijst ook de in 2005 gemaakte vaststelling van toenmalig minister van Buitenlandse Zaken Ben Bot dat Nederland 'aan de verkeerde kant van de geschiedenis' heeft gestaan, terwijl koning Willem-Alexander Indonesië in 2020 aanbood voor Nederlandse 'geweldsontsporingen' en opdracht heeft gegeven tot een onafhankelijk onderzoek naar de rol van het Huis Oranje-Nassau in de koloniale geschiedenis.[18]

Bevindt het debat zich momenteel op een hoge curve, die waarschijnlijk weer zal afvlakken? Limpach: 'Ik vermoed van wel. In veel landen, ook in Nederland, gaat het historisch besef niet diep. Veel mensen weten niet wat de van 1945 tot 1949 gevoerde koloniale oorlog inhield of wat er verder gebeurd is in Indonesië en gebruiken nog steeds de propagandaterm 'politionele acties'. Helaas sneeuwt het Indonesische perspectief in het Nederlandse debat ook vaak volledig onder. Niettemin denk ik dat er wel een bepaalde kentering heeft plaatsgevonden en dat in ieder geval het Nederlandse zelfbeeld nu wat minder rooskleurig is. In schoolboeken, musea en ook wel in de hoofden van mensen leven nu nieuwe feiten over de oorlog die mogelijk zullen beklijven. Ook in ander opzicht is inmiddels meer aandacht voor kolonialisme in het algemeen en voor belangrijke aspecten als slavernij in het bijzonder. Dat is een proces dat tijd vergt en ook beïnvloed wordt door het politieke klimaat.'

Limpach vindt dat het elke natie en elk instituut siert om kritisch en open naar het eigen verleden te durven kijken.[19] 'Er zullen helaas altijd mensen zijn die een hopeloos reactionair achterhoedegevecht voeren en de illusie koesteren dat Nederland in de periode 1945-1949 of eerder iets groots verrichtte in Indonesië. Natuurlijk praat geen enkel land graag over weinig verheffende gebeurtenissen uit het verleden waarbij extreem geweld is gebruikt, over daderschap. Veel geschiedenisboeken staan bol van nationalisme, pathos en trots. In veel landen is er een tendens om de zwarte pagina's in de geschiedenisboeken grijs te tinten of heel snel over te slaan, al komt daar gelukkig steeds meer verandering in. Ik denk trouwens dat militairen wel een slag mensen zijn die bovengemiddeld sterk op waardering en erkenning door de samenleving hameren. En dat begrijp ik ook wel, want ze steken hun nek uit op missies en dat is heel iets anders dan ergens veilig achter een bureau zitten, maar die vraag naar waardering mag kritisch onderzoek naar hun handelen niet in de weg staan.'

Volgens de historicus Jan Bank leidde het tv-interview met Joop Hueting in 1969 tot 'publieke beroering'.[20] Limpach ervoer zelf ook zoiets bij de publicatie van zijn proefschrift en tijdens het ODGOI-onderzoek, maar het ontmoedigt hem niet en de kritiek komt volgens hem vooral van uitersten: 'De grote massa laat zich niet horen, die kan er blijkbaar goed mee leven. Bovendien zijn het slotwerk en de

17 Tweede Kamer, 'Brief van de minister-president, minister Algemene Zaken en de ministers van Buitenlandse Zaken en van Defensie en de staatssecretaris van Volksgezondheid, Welzijn en Sport' (17 februari 2022) vergaderjaar 2021-2022, 26 049, nr. 92.

18 Zie: Oostindie, Schoenmaker en Van Vree (red.), *Over de grens,* 12-13; 'Onafhankelijk onderzoek naar het Huis Oranje-Nassau en de koloniale geschiedenis' (Den Haag, Rijksvoorlichtingsdienst, 6 december 2022).

19 Tweede Kamer, 'Verslag van een rondetafelgesprek' (23 mei 2022) vergaderjaar 2021-2022, 26 049 (nr. 94) 3.

20 Jan Bank (inleiding), *De Excessennota,* 9-10.

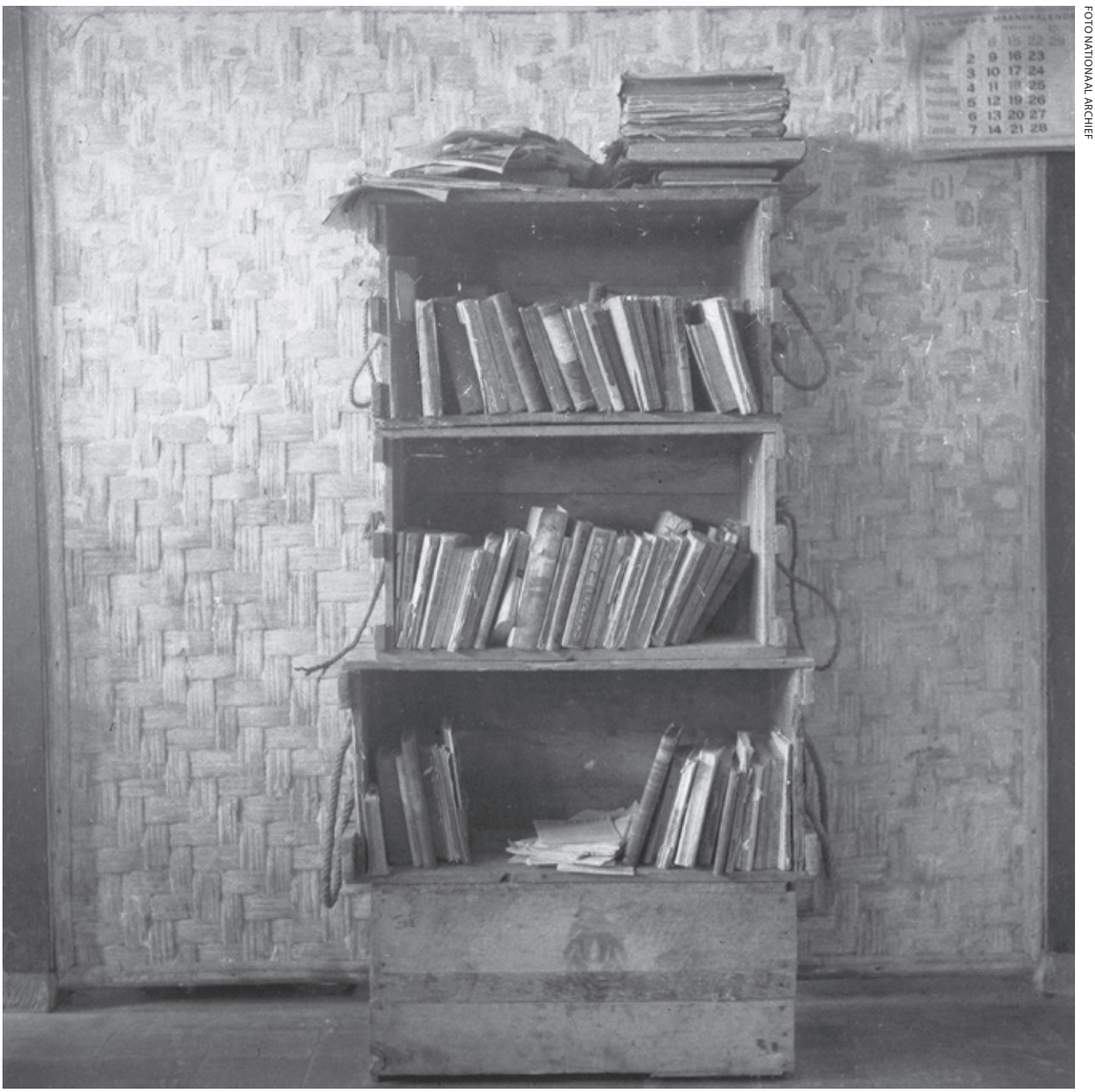


FOTO NATIONAAL ARCHIEF

Een boekenkast van gestapelde munitiekisten in een Nederlands militair verblijf in Indonesië, 1948: Limpach hoopt dat door het ODGOI-onderzoek nieuwe feiten over de oorlog in de hoofden van mensen zullen beklijven

deelstudies door de media en de wetenschap al met al goed ontvangen'. Verwacht Limpach opnieuw reuring als zijn boek over Nieuw-Guinea uitkomt? Hij zal het gesprek in ieder geval niet uit de weg gaan: 'Als ik mijn resultaten op tafel leg, dan kunnen we discussiëren. Maar dan wel graag eerst mijn boek lezen'. ■

Een noodzakelijk maritiem doekje voor het bloeden in de Rode Zee

Jaus Müller

Zelfs vier beveiligers konden weinig doen tegen de snel naderende speedboten op de Rode Zee op 21 augustus. Gewapende Houthi-rebellen overmeesterden die dag de 25-koppige bemanning van de gigantische Griekse olietanker MT Sounion, met ongeveer 150.000 ton petroleum aan boord. Tijdens de aanval raakte de besturing van het schip buiten werking. Kort daarna plaatsten de rebellen explosieven op het schip. In een spectaculair filmpje, gemaakt door de rebellen, is te zien hoe na een reeks explosies vlammen uit de luiken van het schip slaan. Vlak voor dit alles kon de EU-missie in de Rode Zee, Aspides, de bemanning op het nippertje evacueren.[1]

Drie weken later, bij het schrijven van deze column, begeleidt Aspides de berging van de tanker, die nog steeds in brand staat.[2] Een milieuramp van historische proporties is misschien net op tijd afgewend. Dit roept de vraag op hoe succesvol de EU-missie in de Rode Zee eigenlijk is. Ja, de bemanning werd gered, maar het stuurloze, brandende schip midden in de Rode Zee kan moeilijk als een teken van succes voor de EU worden gezien. Het is tijd om de missie eens goed te bekijken en na te gaan wat de kritische succesfactoren van deze operatie zijn.

Ik ben niet helemaal objectief ten aanzien van deze missie: begin februari kreeg ik een telefoontje van de Directie Operatiën van het ministerie van Defensie met de opdracht om mij een krappe week later te melden in Larissa, Griekenland. Samen met collega's uit 21 EU-landen mocht ik de basis leggen voor deze missie, als stafofficier namens Nederland op het EU Operations Headquarters (OHQ) voor een periode van vier maanden (vandaar ook mijn langere afwezigheid als columnist). Een aantal observaties vanuit deze unieke EU-missie wil ik graag delen.

Ik begin bij het unieke karakter van Aspides. Het is voor het eerst in de geschiedenis van de Europese Unie dat zij zo snel een militaire operatie heeft weten op te zetten, en dat in het hoogste geweldsspectrum. De aanleiding was een aanhoudende reeks Houthi-raketaanvallen op koopvaardijschepen in de Rode Zee eind 2023, waarmee de rebellen probeerden druk uit te oefenen op de EU om Israël te dwingen zich terug te trekken uit de Gazastrook. De EU liet echter juist zien dat zij buiten haar eigen verdragsgrenzen in staat is om zowel handels- als veiligheidsbelangen te waarborgen. Op 19 februari begon de missie, waarmee zij in elk geval politiek gezien al een succes was.

In navolging van mare liberum, het principe van Hugo de Groot (1583-1645) dat de open zee vrij bevaarbaar moet zijn, stuurde Nederland afgelopen halfjaar de Zr.Ms. Tromp en zelfs de Zr.Ms. Karel Doorman als vlaggenschip naar de missie, inclusief Aspides Force Commander commandeur George Pastoor. Nieuw was ook het hoogrisico-operatiegebied van de missie: ver buiten het verdragsgebied van de EU op een

levensgevaarlijk stuk zee. De vijand bleek sluwer dan verwacht. Op hun socialemediakanalen presenteerden de rebellen zich als de Robin Hoods op zee: ongeorganiseerd, met roestige Kalasjnikovs. In werkelijkheid hadden we te maken met door Iran gesteunde professionele strijders, die met hun hypermoderne ballistische antischeepsraketten akelig precies hun doelen raakten. Zo bezien stonden we tegenover een asymmetrische dreiging op zee. Tegen de achtergrond van een veel groter conflict in het Midden-Oosten werd hier een soort proxy-oorlog uitgevochten in de vorm van maritieme guerrillaoorlogvoering vanuit land op zee, met als doel de EU te raken waar het pijn doet: de handel.

Hoe effectief is Aspides? Na ruim een halfjaar hebben de deelnemende marines 230 koopvaardijschepen begeleid door de Rode Zee en de Golf van Aden. Daarbij zijn 19 drones neergehaald (waarvan twee 'waterdrones') en vier ballistische raketten onderschept.[3] Toch werd de situatie niet veiliger. Twee koopvaardijschepen zonken en grote rederijen als Maersk keerden niet terug naar de Rode Zee en kozen voor een enorme omweg via Kaap de Goede Hoop. Waar voor de Rode Zee-crisis per dag zo'n 80 tot 100 koopvaardijschepen de Bab-el-Mandebstraat ten zuiden van Jemen passeerden, is dit aantal begin dit jaar gedaald naar 20. Een aantal dat sindsdien onveranderd is gebleven, ondanks Aspides.

Betekent dit dat de missie niet werkt? In mijn ogen niet. Aspides betekent 'schild' en een schild is geen speer: Aspides heeft een louter defensief mandaat. De missie kan bedreigingen voor de scheepvaart dus enkel afweren, niet elimineren. Op tactisch niveau probeert een andere missie, geleid door de Verenigde Staten en het Verenigd Koninkrijk, de bron van de dreiging weg te nemen. Begin dit jaar vernietigde deze coalitie Houthi-radarstations en zo'n 40 lanceerlocaties. Toch nam het aantal raketaanvallen daarna alleen maar toe. Dit toont aan dat een oplossing voor dit conflict niet in het militaire domein ligt. Noch de Amerikaans-Britse missie, noch Aspides biedt een structurele oplossing voor het probleem.

Dit soort asymmetrische conflicten wordt zelden met militaire middelen gewonnen. De enige hoop lijkt het wegnemen van de politieke angel uit het conflict. In dit geval: het beëindigen van de oorlog in de Gazastrook. Dat is ook wat de EU graag wil, maar zij is geen actor in dit conflict. De politieke sleutel tot het beëindigen van die oorlog ligt niet in Brussel, maar ergens in Jeruzalem.

Toch ben ik ervan overtuigd dat de situatie in de Rode Zee zonder Aspides nog verder zou zijn verslechterd, met nog meer brandende en zinkende schepen als gevolg. Maar ik waarschuw voor te hoge verwachtingen van de missie, want met drie à vier EU-schepen, geconcentreerd in een hoogrisicogebied ter grootte van heel Italië, kun je niet anders dan de verwachtingen temperen. Terecht wijst de Griekse Operations Commander van Aspides erop dat het aantal marineschepen echt moet verdubbelen wil de missie meer effect kunnen sorteren.[4] Mocht een politieke oplossing voor Gaza op korte termijn uitblijven, dan zullen de marines van de Europese Unie toch echt meer luchtverdedigingscapaciteiten moeten aanbieden aan Aspides. Tot die tijd fungeert Aspides militair gezien nog niet als de beloofde hoeder van mare liberum, maar eerder als een maritiem doekje voor het bloeden. Maar wel een dat helaas hoogstnoodzakelijk is, vraag maar aan de geredde bemanning van de MT Sounion. ■

1 'Tanker MV Sounion Boarded by Houthi & Demolition Charges Set on Board in the Red Sea', zie: https://www.youtube.com/watch?v=CS5eWaZH5L8.
2 Nick Blenkey, 'Sounion salvage tow gets under way', *MarineLog*, 16 september 2024.
3 Instagram Aspides: https://www.instagram.com/operation_aspides.
4 Simon Marks, 'Fending Off Houthis Requires Double the Fleet, EU Force Says', *Bloomberg.com*, 21 juni 2024.

Nepnieuws en oorlog

Pien van der Hoeven

Met nepnieuws en oorlog houd ik mij al jaren bezig, of nauwkeuriger gezegd met de misleiding van de nieuwsconsument omwille van oorlogvoering. Tjonge, dat is een actueel onderwerp, reageren mensen dan tegenwoordig altijd. Veel meer dan pakweg tien jaar geleden worstelen mensen met het gevoel dat het nieuws niet te vertrouwen is. Cursisten en studenten en mensen op feesten en partijen hoor ik zeggen: 'Je kunt tegenwoordig niet meer op het nieuws aan.' Of: 'De waarheid doet er tegenwoordig niet meer toe, lijkt het wel.' Die onzekerheid wordt steevast gekoppeld aan de opkomst van sociale media.

Maar het ultieme voorbeeld van misleiding van de nieuwsconsument ten tijde van oorlog vind ik nog altijd de Golfoorlog, de kortstondige militaire operatie Desert Storm in 1991 om Saddam Hoessein uit Koeweit te verdrijven. En die was ver vóór het ontstaan van sociale media, toen zelfs het internet nog heel pril was. Ik was toen student. Ik herinner me onze opwinding: het was de eerste oorlog die *live* op de televisie was dankzij de destijds nieuwe kabel- en satelliettechnologie. We zaten gekluisterd aan de buis en we dachten dat we de oorlog echt meemaakten. Als televisiekijkers suisden we mee met op raketten gemonteerde videocamera's naar de doelwitten in Irak. We zagen spectaculaire beelden van brandende oliebronnen en 'vuurwerk' boven Bagdad. Ondertussen lazen we in de krant over de precisiewapens waarmee militaire doelen werden bestookt. Superieure westerse technologie zorgde voor een schone oorlog – een oorlog waarin geen bloed vloeide.

De Franse filosoof Jean Baudrillard stelde dat de Golfoorlog niet plaatsvond. En hij had gelijk, want wat wij zagen was één groot rookgordijn, waarachter een gruwelijke werkelijkheid zich voltrok: geen oorlog, maar een slachting. Tienduizenden Iraakse dienstplichtigen werden in de grootste geallieerde vuurzee ooit verkoold in de woestijn. Hiervan was hoegenaamd niets te zien op de tv. Desert Storm, gevierd als een groot militair succes, was vooral een staaltje public relations.

Met het ontstaan van internet en sociale media aan het begin van deze eeuw is de verspreiding van nepnieuws in een stroomversnelling geraakt. De mogelijkheden van buitenlandse inmenging via trollen en nepaccounts zijn ijzingwekkend – en dat in een tijd van grote geopolitieke onzekerheid. In onze geïndividualiseerde samenleving dringen berichten via sociale media zonder tussenkomst van leiders en deskundigen meteen door in de haarvaten van de maatschappij. Algoritmes bevestigen burgers steeds verder in dezelfde denkbeelden. Des te groter is de ontwrichtende werking van nepnieuws. Hoewel technologische ontwikkeling leidt tot discontinuïteit – sociale media zorgen immers voor schaalvergroting en versnelling in de verspreiding van nepnieuws – valt mij als onderzoeker inhoudelijk gezien juist de continuïteit in het nepnieuws op van vóór en na de opkomst van sociale media. Twee voorbeelden, een recent uit Oekraïne en een uit de Eerste Wereldoorlog, schetsen die continuïteit van nepnieuws.

Eerst het meest recente, het verhaal dat door het Rusland van Vladimir Poetin de wereld in is geholpen bij de invasie van Oekraïne, namelijk dat in Oekraïne in Amerikaanse biotechnologische laboratoria virussen worden ontwikkeld om de Russische bevolking uit te roeien. Dit nepnieuws is uitgezet via Telegram en grif opgepikt door westerse complot-

denkers, ook in Nederland. Belgische en Nederlandse journalisten hebben deze Russische nepnieuwscampagne in een gezamenlijk onderzoeksproject prachtig gereconstrueerd door 3 miljoen Telegramberichten te analyseren.[1]

Het verhaal over de biolabs deed mij sterk denken aan een ander geval van nepnieuws in oorlogstijd uit mijn eigen onderzoek: dat van de *Kadaververwertungsanstalten* oftewel de Duitse lijkenverwerkingsfabrieken. Dat speelde in 1917, op een moment in de Eerste Wereldoorlog dat het moreel laag was, zowel bij de geallieerden als bij de centralen. Soldaten bevonden zich in de uitzichtloze situatie van de loopgraven en na de slag om de Somme was in ieder Engels gezin wel een gesneuvelde zoon te betreuren. Om de oorlog voort te kunnen zetten moest de haat tegen de Duitsers worden aangewakkerd. Eén geval van nepnieuws was wat dit betreft bijzonder effectief, het verhaal dat de Duitsers bij het front in Reims fabrieken hadden waar ze hun gesneuvelden verwerkten tot nuttige producten als vet, veevoer en zeep.

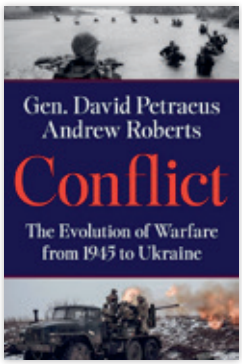
Dit verhaal is door Belgische emigrés in Nederland verzonnen, heb ik ontdekt.[2] Nederland was tijdens de Eerste Wereldoorlog het toevluchtsoord voor een miljoen Belgen, aangezien hun land door de Duitsers was bezet. Eerst probeerden de Belgische propagandisten het nepnieuws in te steken in Nederlandse kranten, maar het werd niet opgepikt; de *NRC* vond het ongeloofwaardig. In de Engelse kranten lukte het wel: en zo werd het nepnieuws via de *Times* wereldwijd verspreid – en alsnog opgenomen in de *NRC*.

Mij vielen de overeenkomsten op tussen dit geval van nepnieuws uit de Eerste Wereldoorlog en dat uit de huidige oorlog in Oekraïne – en trouwens alle gevallen van nepnieuws in oorlogstijd die ik heb onderzocht. Ten eerste, het inspelen op emoties, vooral op angst: Duitsers zouden een gevaarlijk volk zijn met primitieve normen en waarden, Hunnen. Zo ook de Amerikanen, die erop uit zouden zijn de Russen uit te roeien. Ten tweede, het aansluiten bij vooroordelen, bij de gangbare manier van denken. Duitsers bekleedden een vooraanstaande positie in de wetenschap en technologie. Net als de Amerikanen nu. Door die Duitse technologische superioriteit in combinatie met hun zogenaamde morele primitiviteit kon Duitsland als één groot Frankenstein worden gepresenteerd. Op hetzelfde sentiment wordt ingespeeld bij de Amerikaanse biolabs. Ten derde valt mij de kern van waarheid op. Nepnieuws is altijd een mengvorm van waar en onwaar, dus de leugen komt binnen aan hand van de waarheid: er *zijn* Amerikaanse laboratoria in Oekraïne, maar daar wordt geen virus ontwikkeld om de Russische mens uit te roeien; er *waren* fabrieken achter het westelijk front bij Reims. Daar werden echter niet de lijken van soldaten verwerkt, maar die van paarden.

Ondanks de schaalvergroting en versnelling in de verspreiding van nepnieuws is het de vraag of de misleiding van de nieuwsconsument tegenwoordig groter is. Ik vermoed dat niet zozeer het bedrog zelf, maar met name het *bewustzijn* van bedrog bij de nieuwsconsument is toegenomen. Dit heeft alles te maken met het afnemend vertrouwen van de burger in de democratische instituties. Toen de Amerikaanse regering aan de vooravond van de oorlog in Oekraïne waarschuwde voor de Russische inval en inlichtingen over troepenconcentraties openbaar maakte, werden deze door veel westerse media met wantrouwen bejegend. Journalisten dachten geleerd te hebben van het bedrog met inlichtingen in aanloop naar de Irakoorlog, waarmee zogenaamd werd bewezen dat Saddam massavernietigingswapens had en banden met al-Qaida. De paradox is dat in 2003 geloofd werd wat *niet* waar was en mede daardoor in 2022 gewantrouwd werd wat *wel* waar was. Wantrouwen is het nieuwe vooroordeel geworden. Maar kritisch denken vraagt om een werkelijk open blik. Niet alles is nepnieuws. ■

1 'Geheime biolabs in Oekraïne? Complotdenkers herkauwen Russische propaganda', *Pointer* (KRO/NCRV) 16 juli 2022, zie: https://pointer.kro-ncrv.nl/geheime-biolabs-in-oekraine-complotdenkers-herkauwen-russische-propaganda; Luc Van Bakel, Anton Olbrechts en Amra Dorjbayar, 'Hoe Rusland complottheorieën tot in de Vlaamse huiskamers krijgt: VRT NWS onderzocht 3 miljoen berichten op Telegram', *VRT NWS*, 16 juli 2022, zie: https://www.vrt.be/vrtnws/nl/2022/07/13/hoe-rusland-westerse-complotdenkers-voor-zijn-kar-spant-vrt-nws/; Rien Emmery, 'Wat Russische claims over 'Amerikaanse biolabs' in Oekraïne met corona te maken hebben', *Knack*, 15 maart 2022, zie: https://www.knack.be/nieuws/wereld/wat-russische-claims-over-amerikaanse-biolabs-in-oekraine-met-corona-te-maken-hebben/.

2 Pien van der Hoeven, 'Zeepfabriek: Britse propaganda in de Eerste Wereldoorlog', *Historisch Nieuwsblad*, jul/aug 2014, 44-51.



Conflict

The Evolution of Warfighting from 1945 to Ukraine
Door David Petraeus en Robert Andrews
New York (HarperCollins) 2023
544 blz.
ISBN 9780063293137
€ 37,-

Na jaren van nucleaire patstelling tijdens de Koude Oorlog en het consumeren van het vredesdividend na het vallen van de Berlijnse Muur zijn de geopolitieke verhoudingen danig uit balans. Het agressieve optreden van Rusland jegens Oekraïne, na jaren van economische, diplomatieke en digitale prikacties, en het gewapende conflict tussen Israël en Hamas roepen de vraag op hoe oorlogvoering evolueert en welke trends hieruit te halen zijn voor de toekomst. *Conflict* van David Petraeus en Robert Andrews behandelt precies dat. Generaal b.d. Petraeus kennen we van het counterinsurgency-gedachtegoed en de ontwikkeling hiervan is dan ook – weliswaar fragmentarisch – in het boek terug te vinden. Petraeus was commandant van de Amerikaanse troepen in Irak en later commandant van ISAF in Afghanistan. Na zijn diensttijd was hij kort actief als directeur van de CIA. De Britse professor Robert Andrews, sinds eind 2022 Baron Roberts of Belgravia, is als historicus vooral bekend van zijn biografieën over Napoleon en Churchill.

Leiderschapslessen

Conflict is een lezenswaardig boek met een toegankelijke stijl en geschreven voor een breed publiek. Op knappe wijze belicht het boek conflicten zowel vanuit een historisch als krijgswetenschappelijk perspectief. Het is echter geen compendium over de historie van oorlogvoering, want enkel de operaties die fundamentele veranderingen in oorlogvoering (vooral gericht op leiderschap) teweegbrengen zijn opgenomen. De auteurs zijn duidelijk voorstander van opdrachtgerichte commandovoering en de leiderschapslessen – de essentie van het boek – zijn dan ook helder, maar niet erg opzienbarend. Strategische leiders dienen een goed beeld te hebben van het grote plaatje; ze moeten hun opdrachten en oogmerk effectief communiceren met hun omgeving; ze zien toe op de implementatie van de gegeven opdrachten en ten slotte zijn ze in staat om gedurende een operatie, bij gewijzigde omstandigheden, bij te sturen. Voor militairen is dat een open deur en feitelijk een samenvatting van de leiderschaps- en commandovoeringsdoctrine, wat niet wil zeggen dat deze wijze van commandovoering altijd wordt gehanteerd.

Het interessantste deel van *Conflict* is waar de auteurs de geleerde lessen toepassen op de oorlog in Oekraïne en doorkijken naar de *wars of the future* (hoofdstukken 9 en 10). Andrews en Petraeus komen, begrijpelijkerwijs, niet met een toekomstbestendig raamwerk – 'trying to predict the future of warfare is notoriously difficult' (blz. 405) – maar geven wel aan dat de toekomstige oorlog niet een gemakzuchtige terugkeer is naar de Koude Oorlog. Dat is immers de fout die de Russische leider Poetin maakt. De auteurs stellen dat 'Putin had failed to grasp how warfare had evolved since the days of the Blitzkrieg' (blz. 353). De toekomstige oorlog is een combinatie van *hybrid warfare*, nucleair optreden, desinformatie, *cyberwarfare* en drones. Verder zijn alle componenten van militair vermogen van belang – goed materieel, expertise, kennis van de informatieomgeving, coalitievorming, en de mogelijkheid je aan te passen aan gewijzigde omstandigheden. Maar de nadruk ligt op de morele component. Meer nog dan de lessen in leiderschap of de aspecten van het toekomstige conflict zijn, volgens de auteurs, de kwaliteiten van militair leiderschap van belang: mensen kunnen inspireren, motiveren, het hebben van interpersoonlijke vaardigheden, empathie, uithoudings- en doorzettingsvermogen, en vooral 'the ability to be tough when needed, but compassionate when appropriate'.

'MacArthur-bashing'

Conflict is evenwel niet vrij van onvolkomenheden, wat de lezer niet verwacht bij dit schrijversduo. De auteurs nemen het optreden van de laatste actieve jaren van de Amerikaanse generaal Douglas MacArthur als voorbeeld van hoe het *niet* moet. MacArthur was, in zijn latere jaren als commandant van de eenheden in Korea, een toonbeeld van hoogmoed

en ijdelheid. Het knappe staaltje 'MacArthur-bashing' is illustratief voor de oneffenheden in *Conflict*. De auteurs nemen afstand van MacArthur, maar vergeten gemakshalve dat hij een product was van de Amerikaanse cultuur en het opleidingsmodel van die tijd. Tevens negeren zij dat niet alleen MacArthur behept was met hoogmoed, egoïsme en ijdelheid, maar dat dit op leiders van alle tijden van toepassing is. Daarnaast is de beschrijving van de conflicten – zoals Israël, Kashmir, Indo-China, Korea, Vietnam of de Golfoorlog – verre van strategisch, maar eerder anekdotisch. De lessen over strategisch leiderschap zijn weliswaar goed te plaatsen binnen die anekdotes, maar volgen er niet op een logische wijze uit.
Petraeus en Andrews hebben verder een vrij gekleurd of vooringenomen beeld van de werkelijkheid en de neiging om acties van niet-Anglo-Amerikaanse actoren te bagatelliseren of te ridiculiseren. De auteurs stellen dat het voor autoritaire staten gemakkelijk is om een verrassingsaanval uit te voeren, omdat ze geen rekening hoeven te houden met publieke opinie of een kritisch parlement. Denk daarbij aan de aanval van Saddam Hussein op Koeweit of de Arabische aanval op Israël tijdens Jom Kippoer in 1973. Ook hier worden D-Day of de Zesdaagse Oorlog in 1967, met de Israëlische pre-emptieve aanvallen op Syrisch grondgebied, weggelaten. De rationale van de auteurs is sowieso *off-target*, omdat verrassing een van de principes van oorlogvoering is. Het Russische optreden in Afghanistan zorgde, aldus de auteurs, voor een genocide onder de bevolking als gevolg van aantoonbaar slecht leiderschap, en de uiteindelijke Russische aftocht was 'humiliating' (blz. 154-155). Het Amerikaanse optreden in Vietnam, daarentegen, is verpakt als een ongelukkige samenloop van omstandigheden, waarbij goedbedoelende politici en een krijgsmacht belast met verouderde doctrines met elkaar moesten samenwerken. De terugtocht van de Amerikanen uit Vietnam, net als in Korea, was eervol ondanks de kwantitatieve *body count*-benadering van minister van Defensie Robert McNamara.[1] Tot slot bezien de auteurs – als een verplicht nummer – hoe China, bij een aanval op Taiwan, zou kunnen leren van de fouten die Rusland maakte bij de inval in Oekraïne. Een analogie die wellicht strookt met een Anglo-Amerikaans wereldbeeld, maar totaal voorbijgaat aan de verschillen in cultuur, doelstelling en strategisch denken tussen Rusland en China.

Realisme

Ondanks de wat eenzijdige blik is *Conflict* zeker de moeite waard om te lezen. Het is bovenal interessant als een product van zijn tijd. Na decennia waarin het liberalisme en de onderlinge afhankelijkheid tussen staten in internationale organisaties en economische fora hoogtij vierden is recentelijk het realisme als lens om de veiligheid in de wereld te beschouwen weer dominant geworden. Ook de voorzitter van het Militair Comité van de NAVO en de Nederlandse CDS maken gebruik van deze si vis pacem, para bellum-retoriek. *Conflict* is zeker geen oproep tot oorlog, sterker nog: die moet juist voorkomen worden door een adequate afschrikking, of zoals de slotzin stelt: 'The amount of money that needs to be spent might seem vast, but historically it has always proven to be a mere fraction of what it costs in blood and treasure when deterrence fails'. De *human toll of war* is immers voor alle strijdende partijen een hard gelag. ■

Kolonel mr. dr. Peter Pijpers, NLDA

1 Henk de Jong en Floribert Baudet, 'War by Numbers. A Technocratic Hubristic Fable,' in: Peter B.M.J. Pijpers, Mark Voskuijl, and Robert J.M. Beeres (red.), *Towards a Data Driven Military. A Multidisciplinary Perspective (Leiden, Leiden University Press, 2023).*

‘Gods eigen voertuig’

FOTO MCD, EVA KLIJN

1 Ministerie van Defensie, *Defensienota 2024. Sterk, Slim en Samen*. Zie: https://www.defensie.nl/onderwerpen/defensienota/downloads/beleidsnota-s/2024/09/05/defensienota-2024.
2 P.J.T.M. Hagenaars, ‘Geen einde van zware wapens!’, *Militaire Spectator* 182 (2013) (7/8). Zie: https://militairespectator.nl/artikelen/geen-einde-van-zware-wapens.
3 Niels Roelen, ‘Prinsjesdag’, *Atlantisch Perspectief* 39 (2015) (5). Zie: https://www.atlcom.nl/artikel-atlantisch-perspectief/prinsjesdag/.

In 2011 deed de Nederlandse regering de laatste tanks van de hand. Volgens de nieuwe *Defensienota* komen ze nu weer terug in de Nederlandse krijgsmacht: ‘Voor de zware infanteriebrigade schaft Nederland tanks aan om een volwaardig tankbataljon op te richten dat de gevechtskracht

FOTO MCD, EVERT-JAN DANIELS

Met hun mobiliteit, vuurkracht en bescherming 'dragen' tanks manoeuvre met verbonden wapens

levert die de NAVO van Nederland vraagt. Door deze investering gaat Nederland voor het eerst sinds 2011 weer operationele gevechtstanks bezitten en zo een bijdrage leveren aan het invullen van een belangrijke tekortkoming binnen de NAVO (NATO Priority Target).'[1]

De oplettende lezer van de *Militaire Spectator* weet natuurlijk al lang dat de tank een belangrijke, zo niet onmisbare schakel is voor het leveren van gevechtskracht. In 'Geen einde van zware wapens!' betoogde P.J.T.M. Hagenaars dat 'de rol van de tank in de afgelopen jaren niet wezenlijk is veranderd en dat deze, samen met andere zware gepantserde middelen, nog steeds een essentieel deel vormt van het huidige en toekomstige manoeuvreoptreden.'[2] Hagenaars noemt drie vermogens die manoeuvre in het landoptreden vormen: mobiliteit, vuurkracht en bescherming, en de tank heeft deze alle drie. Optreden met verbonden wapens wordt daarom 'gedragen door tanks', aldus Hagenaars.

Vergeet ook niet het psychologische effect van wat sommige ervaringsdeskundigen 'Gods eigen voertuig'[3] noemen. Hagenaars schrijft: 'Tanks dwingen respect af bij een tegenstander. Op het gevechtsveld zorgt de tank vaak voor een psychologisch schokeffect. Iraakse strijders sloegen herhaaldelijk op de vlucht wanneer tanks ter plaatse kwamen. Bij de eigen troepen verhogen tanks het moreel.'

Een aantal jaar eerder (in 2007) benoemde ook D.M. Brongers dit effect, want 'bij activiteiten in het lagere geweldsspectrum kan de tank vanwege zijn psychologische effect worden ingezet ter voorkoming van het escaleren van geweld en het deëscaleren van geweld door zijn escalatiedominantie.'[4] Destijds stond de tank al

4 D.M. Brongers, 'De toekomst van de tank. Vervangen, aanpassen, of afschrijven?', *Militaire Spectator* 176 (2007) (7/8). Zie: https://militairespectator.nl/sites/default/files/teksten/bestanden/MS%207-8%202007%20Brongers%20Toekomst%20van%20de%20Tank.pdf.

FOTO NAVO

Amerikaanse tanks tonen tijdens een NAVO-oefening hun vuurkracht en escalatiedominantie. Met de aanschaf van nieuwe tanks draagt Nederland bij aan het invullen van een 'NATO Priority Target'

ter discussie, en Brongers brak een lans voor 'Het traditionele boegbeeld van de landstrijdkrachten, zoals het fregat dat is voor de marine, of de straaljager voor de luchtmacht.'

Scepsis over het nut van de tank is er overigens altijd wel geweest. In 1918 stelde eerste luitenant der infanterie B. van Slobbe in 'De strijd in het polderland': 'Voor tanks behoeft de verdediger niet bevreesd te zijn. Zou een aanvaller deze machines op de accessen bezigen, dan nog zou geconcentreerd artillerievuur er spoedig mede afrekenen.'[5] Misschien had de verdediger in het polderland te weinig middelen, maar ruim dertig jaar later zou de Wehrmacht door effectief gebruik van verbonden wapens Van Slobbes ongelijk bewijzen.

Al met al toonde 'Gods eigen voertuig' in diverse conflicten zijn effectiviteit, zoals Hagenaars in een kort overzicht liet zien. Toch besloot de Nederlandse regering in 2011 het laatste restje tanks af te schaffen. De nasleep van de financiële crisis van 2008 dwong tot bezuinigen. Achteraf is het makkelijk praten, maar in dit geval is gebleken dat het wegbezuinigen van de tanks geen enkel nut heeft gediend. Sterker, het werkte averechts en er is geen cent bespaard. De Algemene Rekenkamer onderzocht een paar jaar geleden de doelmatigheid van de bezuinigingen van 2011. Op dat moment waren er plannen om toch weer 52 nieuwe tanks te kopen. Met de voorgenomen nieuwe aanschaf in het achterhoofd concludeerde de Rekenkamer: 'Tanks behouden was 7 tot 8 keer goedkoper geweest dan afstoten en nieuwe kopen.'[6] Politiek kortetermijndenken leidt soms helaas tot missers, maar voor het repareren van de Nederlandse gevechtskracht lijkt de *Defensienota 2024* raak te schieten. ■

5 B. van Slobbe, 'De strijd in het polderland', *Militaire Spectator* 87 (1918) (6). Zie: https://militairespectator.nl/sites/default/files/bestanden/uitgaven/1918-6.pdf.

6 Algemene Rekenkamer, *Uit het vizier* (2021). Zie: https://www.rekenkamer.nl/publicaties/rapporten/2021/04/13/uit-het-vizier; S.J. Keulen, 'Defensiebezuinigingen voor de toekomst', *Militaire Spectator* 190 (2021) (12). Zie: https://militairespectator.nl/artikelen/defensiebezuinigingen-voor-de-toekomst.

SIGNALERINGEN

100 Great War Movies

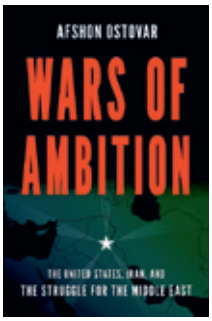
The Real History behind the Films
Door Robert J. Niemi
Londen (Bloomsbury) 2024
392 blz.
ISBN 9798765130995
€ 31,-

De historische feiten waren niet helemaal correct. Die conclusie trekken militair geïnteresseerden nog wel eens na het verlaten van de bioscoop. In zijn boek *100 Great War Movies* gaat Robert Niemi uitgebreid in op de achtergrond van tientallen oorlogsfilms. Niemi bekijkt films vanaf 1930 en de onderwerpen lopen in de tijd uiteen van de Schotse Onafhankelijkheidsoorlogen in de 13e eeuw (Braveheart) tot de strijd in Afghanisten begin deze eeuw (Lone Survivor). Het grootste deel van de films gaat over de Tweede Wereldoorlog. Niemi, die ook Soldaat van Oranje bespreekt, onderzoekt naast historische accuraatheid ook of de films negatieve of positieve recensies kregen.

The Very Long Game

25 Case Studies on the Global State of Defense AI
Door Heiko Borchert, Torben Schütz en Joseph Verbovszky (red.)
Berlijn (Springer) 2024
621 blz.
ISSN 2948-2283
Open access via: https://link.springer.com

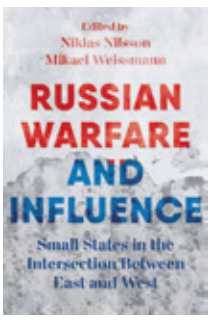
In *The Very Long Game* inventariseren deskundigen welke toepassingen van Artificial Intelligence westerse krijgsmachten verwachten te gaan gebruiken. De bundel bevat artikelen over onder meer de VS, het VK, Rusland, China en Iran. Marierose Heineken-van Dooren en Roy Lindelauf verwijzen in hun bijdrage over Nederland naar de *Defensievisie 2035*, waarin staat dat de krijgsmacht dan een 'vergaand gebruik' van AI verwacht, ook bij de planning en uitvoering van informatiegedreven militaire operaties. Net als de meeste andere westerse landen ziet Nederland, dat naast AI volop inzet op *data science*, kunstmatige intelligentie vooral als een *capability multiplier* die ethisch en juridisch strak ingekaderd moet zijn.



Wars of Ambition

The United States, Iran, and the Struggle for the Middle East
Door Afshon Ostovar
New York (Oxford University Press) 2024
360 blz.
ISBN 9780190940980
€ 27,-

Afshon Ostovar, universitair hoofddocent aan de Naval Postgraduate School in Monterey, omschrijft het Midden-Oosten in zijn boek *Wars of Ambition* als de microkosmos van een geopolitieke strijd waarin tegenstanders een einde willen maken aan de invloed van de VS in het gebied en het bestaan van Israël. Ostovar analyseert de ontwikkelingen sinds 9/11, waarna de Amerikaanse invasie in Irak tot een politieke chaos leidde die de positie van Iran versterkte, het tegendeel van wat Washington wilde bereiken. De auteur legt uit hoe Rusland en China de situatie hebben gebruikt om hun eigen belangen in het Midden-Oosten uit te breiden en te beschermen.



Russian Warfare and Influence

States in the Intersection Between East and West
Door Mikael Weissmann en Niklas Nilsson (red.)
Londen (Bloomsbury) 2024
208 blz.
ISBN 9781350335219
€ 23,-

Hoe gaan landen om met de hybride oorlog die Moskou tegen hen voert en welke middelen gebruiken de partijen daarbij? Dat is de centrale vraag in *Russian Warfare and Influence*. De auteurs in de bundel kijken voornamelijk naar landen die direct aan Rusland grenzen, waaronder Finland en Oekraïne, maar ook naar Servië en Kosovo. Zij concluderen dat conceptuele denkers over hybride oorlog vaak ten onrechte aannemen dat landen die Moskou in het vizier neemt passieve slachtoffers zijn die geen enkele tegenmaatregel kunnen nemen. Dat het anders is blijkt onder meer uit de reactie van de Baltische staten op Russische beïnvloedingsoperaties.