Jaargang 192 nummer 11 - 2023

MILITAIRESPECTATOR

CONCEPTUAL MANOEUVRING

- Speciale operaties in turbulente tijden
- Wiperware: een nieuw cyberwapen?
- Interview: Civil defence in Sweden
- Interview: Caecilia van Peski

FOTO BEELDBANK NIMH

Militaire Spectator 12-2023 is een themanummer over 275 jaar Regiment Genietroepen.

In zijn voorwoord staat commandant kolonel Bas van den Berg stil bij de kernwaarden van het Regiment Genietroepen: (technische) vakkundigheid, brede inzetbaarheid en kameraadschap. Jos Overman en Sven Maaskant gaan in op de geschiedenis van het Regiment, waarbij zij onder meer de technische ontwikkelingen van de 19e eeuw bespreken, die de oorlogvoering een ander aanzien gaven.

Ruud Moeskops, Hoofd Bureau Total Force Genie, wijst in zijn artikel op de genie als een goede ontwikkelomgeving voor civiel-militaire capaciteit vanwege het evidente raakvlak met civiele *counterparts* zoals Rijkswaterstaat en civiele aannemersbedrijven. Luitenant-kolonel Johan Kranenburg, Hoofd Kenniscentrum Genie, analyseert welke kant *military engineering* de komende jaren op kan gaan nu de nadruk bij de NAVO en Defensie weer bij de eerste hoofdtaak ligt. ■

Schrijft u een gastcolumn in de *Militaire Spectator*?

De redactie van de *Militaire Spectator* biedt lezers de mogelijkheid een gastcolumn te schrijven van maximaal duizend woorden. Het thema is vrij, maar moet passen in de formule van het tijdschrift. Een gastcolumn bevat een relevante boodschap voor de lezers, een gefundeerde eigen mening en juiste en verifieerbare feiten in een logisch opgebouwd betoog.

U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon) of aanbieden via de website. De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur

Digitaal voorwaarts: Mars in Cathedra

Sinds 1972 is de Koninklijke Vereniging ter Beoefening van de Krijgswetenschap (KVBK) uitgever van de *Militaire Spectator*, sinds 2015 digitaal. De KVBK bestaat al sinds 1865 en gaf sinds die tijd ook verschillende andere periodieken uit, meestal publicaties van verslagen van door de vereniging georganiseerde lezingen. Deze lezingen zijn inclusief de daarop volgende discussies met de aanwezigen geboekstaafd in het verenigingsarchief. Van 1969-1997 gaf de KVBK daartoe het kwartaalblad *Mars in Cathedra* uit. Alle 110 afleveringen van dat blad zijn nu gedigitaliseerd en via de archiefpagina op de website van de KVBK voor iedereen toegankelijk.[1] Daarmee is weer een belangrijk deel van het Nederlandse militair cultureel erfgoed ontsloten.

De verslagen in *Mars in Cathedra* geven een goed beeld van het militair denken in Nederland in die tijd en sommige artikelen zijn nog verrassend actueel. Zo blijkt uit de bijdrage van toenmalig brigade-generaal Berkhof uit 1984 dat het militaire gebruik van de ruimte al in dat jaar onderwerp van discussie was.[2] En wat te denken van een voordracht van commandant Dutchbat 2 uit februari 1995, nog onwetend van het komende drama? Geen enkel boek zal meer het leven van een Nederlands bataljon in de enclave zo oprecht kunnen beschrijven dan de voordracht van luitenant-kolonel Everts destijds.[3]

Een prachtig tijdsbeeld levert de bijdrage van generaal-majoor Von Meijenfeldt uit april 1979.[4] De opvattingen van de 'rode gouverneur van de KMA' moesten volgens de toenmalige redactie 'tenminste in de rubriek 'sterk controversieel' […] worden ondergebracht'. Het siert de KVBK dat deze generaal toch het woord kreeg en de lezer nu (weer) kennis kan nemen van het destijds hoogoplopende debat over de inzet van het kernwapen. De toenmalige redacteur gaf niettemin lucht aan zijn zorg dat 'de thans in opleiding zijnde cadetten van land- en luchtmacht zouden kunnen worden 'besmet' met zijn denkbeelden'. Quod non!
Tijdloos is het referaat 'Gedachten over de instelling van een 'hoogste vorming' voor (aanstaande) militaire topfunctionarissen' van de majoors der infanterie Van der Graaf en Tomasso uit 1972, die met deze vooruitziende blik op de noodzakelijke *permanent education* voor officieren de KVBK-prijsvraag wonnen.[5]

De gedachten van zulke voorgangers zijn het waard om herlezen te worden. Niet alleen vanuit historisch perspectief, maar ook omdat huidige officieren van hen kunnen en moeten leren. ■

1 Zie: https://kvbk.nl/artikelen-archief.
2 G.C. Berkhof, 'Het militaire gebruik van de ruimte', *Mars in Cathedra* 59 (januari 1984).
3 P.L.E.M. Everts, 'Ervaringen in 'de grootste openluchtgevangenis van Europa'', *Mars in Cathedra* 102 (februari 1995).
4 M.H. von Meijenfeldt, 'Nucleaire opvattingen binnen en buiten de landsgrenzen', *Mars in Cathedra* 41 (april 1979).
5 H.J. van der Graaf en E.P.B. Tomasso, 'Gedachten over de instelling van een 'hoogste vorming' voor (aanstaande) militaire topfunctionarissen', *Mars in Cathedra* 18 (april 1973).

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)
Sectie MOW
Ledenadministratie KVBK
Postbus 90002, 4800 PA Breda
E ledenadministratie@kvbk.nl

REDACTIE
lgen b.d. ir. R.G. Tieskens (hoofdredacteur)
drs. A. Alta
kol Marns drs. G.F. Booij EMSD
ltkol dr. L. Boskeljon-Horst
bgen prof. dr. A.J.H. Bouwmeester
dr. A. Claver
drs. P. Donker
cdre KLu b.d. F. Groen (plv. hoofdredacteur)
kap (R) L.J. Leeuwenburg-de Jong MA (e-outreach)
kol mr. dr. B.M.J. Pijpers
mr. drs. A. van Vark KMar
ktz drs. H. Warnar
dr. R. de Winter

BUREAUREDACTIE
M. Katsman MA
dr. F.J.C.M. van Nijnatten (eindredactie)
NIMH
Postbus 90701
2509 LS Den Haag
E redactie.militaire.spectator@mindef.nl
www.militairespectator.nl
facebook.com/militaire-spectator
twitter.com/milspectator
linkedin.com/company/militaire-spectator/

De Militaire Spectator is aangesloten bij de European Military Press Association

LIDMAATSCHAP

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

OPMAAK
Coco Bookmedia

DRUK
Wilco Meppel
ISSN 0026-3869
Nadruk verboden

Coverfoto: Introductie van nieuwe systemen op het Special Operation Forces Innovation Network Seminar in Bordeaux, 2019
Foto: MCD, Hille Hillinga

MILITAIRESPECTATOR

JAARGANG 192 NUMMER 11 – 2023

FOTO US AIR FORCE CHRIS HIBBEN

526

FOTO MCD, KEESNAN DOGGER

542

Speciale operaties in turbulente tijden

Martijn Kitzen

De huidige veiligheidssituatie vereist een nieuw perspectief op de rol van special forces, zeker voor kleine landen als Nederland en België.

Conceptual manoeuvring

Marije Timmer and Paul Ducheine

The conceptual foundations of Information Manoeuvre and the manner in which it is interpreted within the Netherlands Ministry of Defence need clarification.

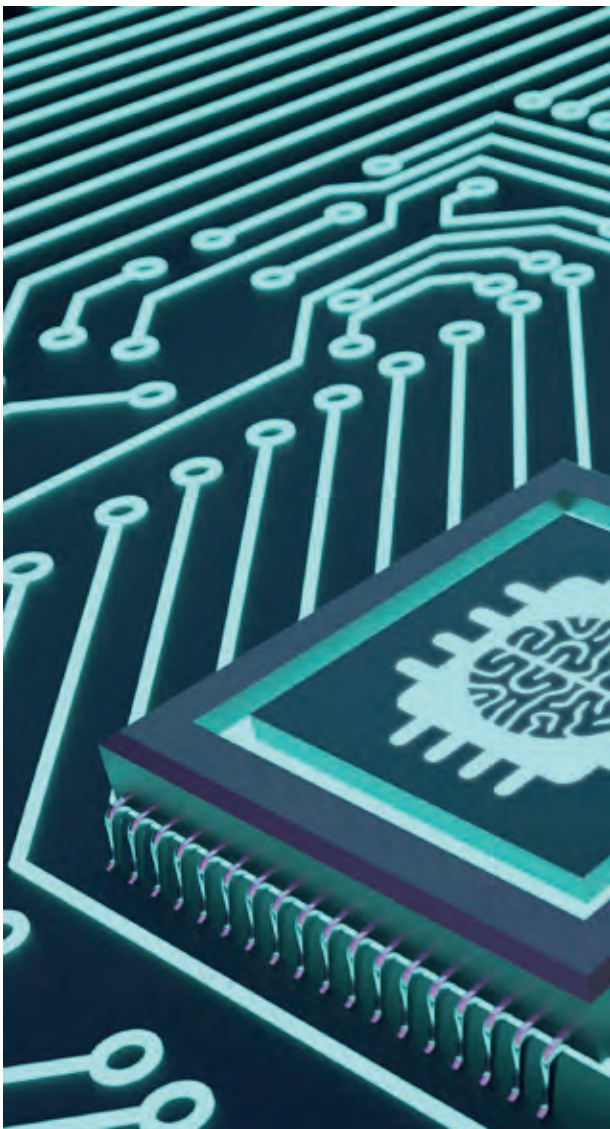
EN VERDER

Wiperware: een nieuw cyberwapen voor de militaire toolbox?

Luitenant-kolonel K.L. Arnold ESMD MSc en drs. S. van Dorst*

In het huidige Russisch-Oekraïense conflict vinden dagelijks cyberaanvallen plaats; niet alleen gericht tegen Rusland en Oekraïne, maar ook tegen derde landen. Het overgrote deel van die cyberaanvallen betreft relatief onschuldige *denial-of-service*-aanvallen, *defacements* of *hack-and-leak*-operaties met bescheiden militaire impact. Slechts een enkele cyberaanval staat uitgebreid in de belangstelling en heeft meer (militaire) betekenis. Daartussen bevindt zich een categorie cyberaanvallen met een destructief karakter; klein in aantal, maar met potentie om via digitale oorlogvoering daadwerkelijk tastbare schade aan te richten: zogeheten 'wiperware'. Maar wat is wiperware? Wat doet het en hoe werkt het? Wat is de militaire meerwaarde ervan? Past het in de gereedschapskist van onze eigen krijgsmacht? Dit artikel gaat in op de mogelijkheden van wiperware voor militaire doeleinden.

Wat is wiperware, en heeft het militaire toepassingen?
FOTO DARPA



Cyberaanvallen vinden tegenwoordig dagelijks plaats, maar alleen de meest opvallende worden geregistreerd en geanalyseerd en komen in het nieuws. Dit geldt ook voor de Russisch-Oekraïense cyberoorlogvoering. Er lijkt weinig te gebeuren in cyberspace, maar niets is minder waar. Sinds de invasie op 24 februari 2022 zijn 2.776 aan deze oorlog gerelateerde cyberaanvallen geregistreerd.[1]

Grofweg kun je cyberaanvallen indelen in drie categorieën.[2] Allereerst zijn er cyberaanvallen met een strategische impact. In de Russisch-Oekraïense oorlog is vooralsnog één cyberaanval

aan te wijzen die een dergelijke strategische impact had; of had kunnen hebben. Op de vooravond van de invasie vielen hackers modems aan van het Viasat satelliet-internet-communicatiesysteem. Met elektronische oorlogvoering (EOV) verminderden de Russen reeds de effectiviteit van drie van de vier hoofdvormen van draadloze communicatie[3] van de Oekraïense strijdkrachten. De uitschakeling van Viasat completeerde het verlies van militaire communicatie, met name in de regio van het destijds zwaar bedreigde Kyiv.[4] De Viasat-cyber-aanval maakte de Oekraïense troepen vrijwel blind voor de Russische troepen en hun bewegingen.[5] Met steun van Elon Musks Starlink satellietontvangers[6] en tienduizenden nieuwe Viasat-modems[7] kon de Oekraïense internet-communicatie echter snel worden hersteld,

* Kraesten Arnold is cyberonderzoeker en -docent aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie in Breda; Sander van Dorst is als medewerker verbonden aan het team Concepten & Doctrine van het Cyber Warfare & Training Centre.

1 CyberPeaceInstitute, status per 30 september 2023. Zie: https://cyberconflicts.cyberpeaceinstitute.org/impact.

2 Jon Lindsay en Erik Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited', in: K.M. Greenhill en P.J.P. Krause (red.), *The Power to Hurt: Coercion in Theory and in Practice* (Oxford, Oxford University Press, 2016) 179–203; B.M.J. Pijpers en Kraesten L. Arnold, 'Arms Control in Cyberspace?', *Altantisch Perspectief* 47 (2023) (2) 35–40.

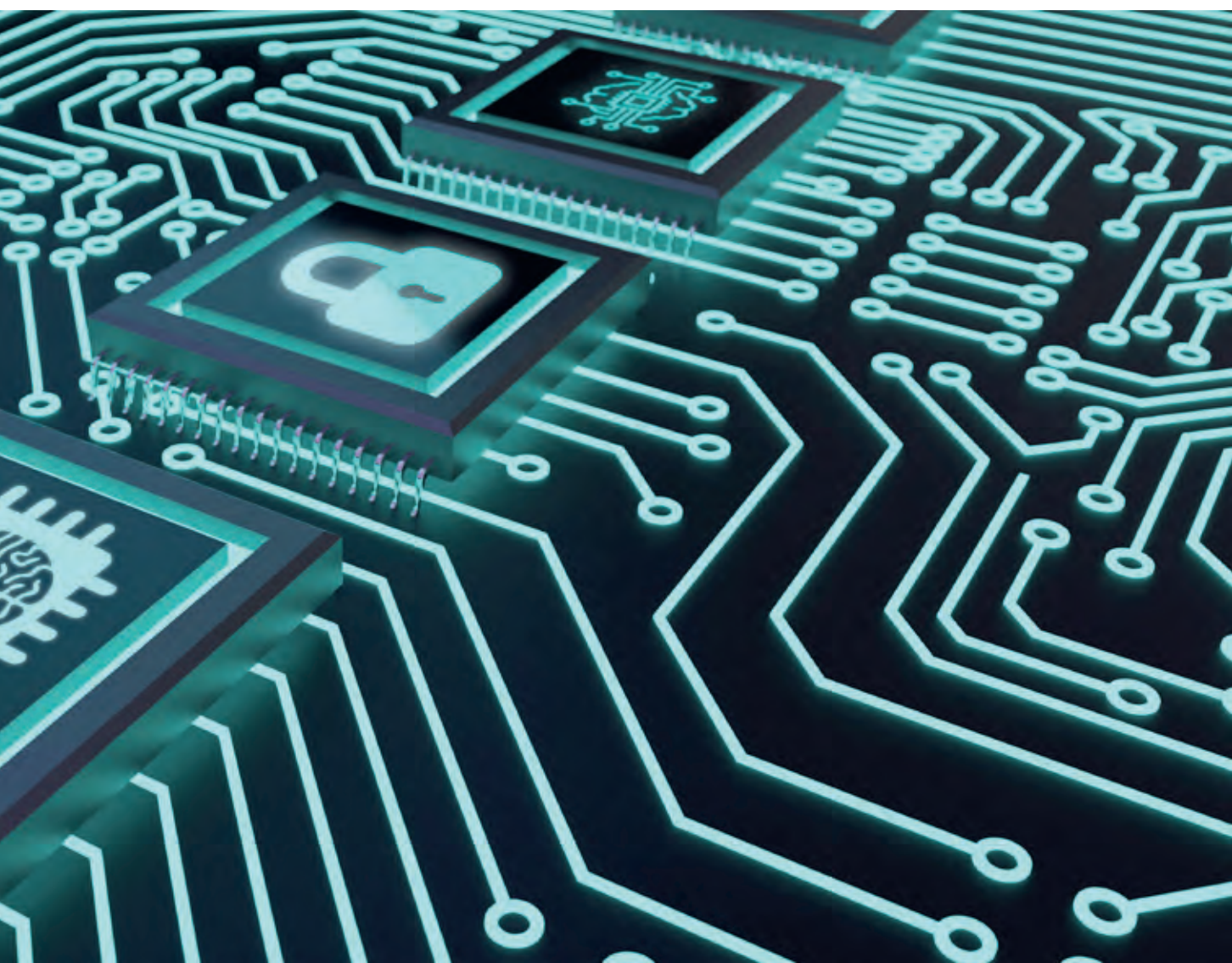
3 *Legacy* analoge radiosystemen; nieuwe, beveiligde digitale radiosystemen; LTE mobiele telefonie; satellietcommunicatie (SATCOM).

4 Dan Rice, 'The Untold Story of the Battle for Kyiv', *Small Wars Journal*, 31 mei 2022. Zie: https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.

5 Jason Blessing, 'Revisiting the Russian Viasat Hack: Four Lessons About Cyber on the Battlefield', *American Enterprise Institute*, 2 september 2022.

6 Hyunjoo Jin, 'Musk Says Starlink Active in Ukraine as Russian Invasion Disrupts Internet', *Reuters*, 2022.

7 Viasat Corporate News, 'KA-SAT Network cyber attack overview', 30 maart 2022. Zie: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.



Het gebruik van wiperware als cyberwapen is vermoedelijk te herleiden naar de VS FOTO DARPA

waardoor de negatieve gevolgen voor Oekraïne beperkt bleven.

Van een geheel andere orde zijn cyberaanvallen die weliswaar veelvuldig voorkomen, maar eerder vervelend dan schadelijk zijn. Die aanvallen veroorzaken geen dood en verderf, en dienen ogenschijnlijk geen militair doel, maar zijn desondanks wel hinderlijk. Het merendeel van de waargenomen en geregistreerde cyberaanvallen die zijn te relateren aan de Russisch-Oekraïense oorlog bestaat uit dat soort hinderlijke denial-of-service aanvallen,[8] website defacements,[9] phishing[10] en hack-and-leaks.[11]

De derde categorie betreft cyberaanvallen die op een operationeel niveau (in)direct militaire of diplomatieke campagnes ondersteunen. Rusland en Oekraïne verzamelen beide digitaal inlichtingen en beide landen voeren digitale verkenningsoperaties uit ter ondersteuning van hun militaire operaties. Maar er is nog een type cyberaanvallen dat in deze oorlog door pro-Russische actoren is ingezet tegen een scala aan Oekraïense entiteiten: aanvallen met ransomware en wiperware, ofwel kwaadaardige software bedoeld om respectievelijk data te versleutelen, of data én computers onherstelbaar te beschadigen.

Met dit artikel willen we inzicht verschaffen in de mogelijkheid wiperware in te zetten als operationeel cyberwapen ter ondersteuning van militaire operaties. We starten met een uitleg wat wiperware omvat: wat het is, wat het doet en

8 Bij een denial-of-service (DOS)-aanval wordt een computer of netwerk bestookt met dusdanig veel opdrachten of verzoeken dat de werking van die computer of dat netwerk ernstig wordt beperkt of zelfs onmogelijk gemaakt. Een distributed denial-of-service (DDoS) aanval gebruikt meerdere computers voor de cyberaanval.

9 Bij een website defacement verandert de aanvaller het 'uiterlijk' van een website door die te vullen met andere inhoud (tekstueel en visueel), zoals politieke, sociale of religieuze boodschappen.

10 Phishing is het 'hengelen' naar vertrouwelijke informatie zoals gebruikersnamen, wachtwoorden en creditcardgegevens.

11 Onder hack-and-leak wordt verstaan het inbreken in een computer, om vervolgens gevoelige informatie te stelen en naar buiten te brengen.

welke effecten je ermee kunt creëren. Dan kijken we naar de ontstaansgeschiedenis van deze vorm van malware, waarbij enkele roemruchte cyberaanvallen aan de orde komen. Vervolgens gaan we in op het specifieke gebruik van dit soort cyberwapens in het Russisch-Oekraïense conflict; welke doelwitten zijn bestookt; door welke actoren; in hoeverre diende dit een militair doel en; was het effectief? Hieruit volgt een analyse waarna we aangeven in hoeverre wiperware een praktisch bruikbaar cyberwapen kan zijn voor onze eigen krijgsmacht.

Wat is wiperware?

Als je in een gangbaar computer besturingssysteem[12] (*Operating System*, OS) een bestand verwijdert, dan gebruik je bijvoorbeeld *delete* (bij een Microsoft Windows OS) of *remove* (bij een Linux OS).[13] Met dat commando verwijder je evenwel alleen de verwijzing naar dat bestand zodat het besturingssysteem dat bestand niet meer 'ziet'. De inhoud van het bestand zelf wordt echter niet gewijzigd. Een bestand dat op die manier is 'verwijderd', kun je dan ook relatief eenvoudig weer terughalen.[14] Als je de inhoud van een bestand permanent wil verwijderen of onleesbaar maken, dan moet je die inhoud geheel of gedeeltelijk vervangen door andere, bijvoorbeeld willekeurig gegenereerde gegevens. Hoe vaker je dat proces herhaalt, des te lastiger het is om de originele informatie nog terug te halen. Op een bepaald moment is dat niet meer mogelijk.

De term 'wiper' in wiperware slaat op de primaire functie van dergelijke software, die is bedoeld om data definitief te wissen van het permanente computergeheugen.[15] In werkelijkheid worden specifieke computerbestanden,[16] of bepaalde gedeeltes van een harde schijf,[17] meerdere keren overschreven met andere data, maar soms ook met (politieke) boodschappen of foto's.[18] De originele informatie is dan onherstelbaar beschadigd ('gewist').

Behalve gegevensbestanden (*files*) permanent wissen, kan wiperware ook andere software beschadigen, zoals het programma dat nodig is om de computer op te starten (*bootloader*);[19] de software die zorgt voor de virtuele indeling ('partities') van het computergeheugen,[20] of andere *firmware*.[21] Een geheel andere methode is het onomkeerbaar cryptografisch versleutelen van specifieke databestanden, gedeeltes van de harde schijf, of essentiële systeembestanden die nodig zijn om een computersysteem op te starten. De gedachte erachter is hierbij hetzelfde. De computer, of het apparaat waar die computer in zit, werkt niet meer naar behoren of kan zelfs helemaal niet meer opstarten. De computer is dan niet meer te gebruiken.

Omdat voornoemde wipe-methodes elk hun specifieke voor- en nadelen hebben, bestaat wiperware vaak uit een combinatie van die methodes om een zo groot mogelijk destructief effect te creëren. De reden voor een wiper-aanval kan variëren, maar in tegenstelling tot ransomware ligt bij wiperware een financiële drijfveer

12 Een besturingssysteem zorgt ervoor dat, na het opstarten van de computer, de hardwarecomponenten met de verschillende softwareprogramma's kunnen communiceren.
13 Andere gangbare besturingssystemen zijn macOS, Unix, Android, BSD, VMkernel, IOS, Solaris.
14 Het verwijderen van een computerbestand en vervolgens de prullenbak legen is niet voldoende om gegevens op een computer of gegevensdrager (harde schijf, SDD USB, CD-rom, flash-geheugen) permanent te wissen. Zelfs het (eenmalig) formatteren van dat geheugen is daartoe niet afdoende. Met *data recovery software* zijn die gegevens namelijk weer te achterhalen.
15 Dit betreft zowel vast als verwisselbaar geheugen, zoals een hard disk, solid state drive of USB-stick.
16 *Data destruction*, zie: https://attack.mitre.org/techniques/T1485/.
17 *Disk content wipe*, zie: https://attack.mitre.org/techniques/T1561/001/.
18 De aanval met Shamoon wiperware in 2012 toonde een brandende Amerikaanse vlag. De Shamoon wiperware van 2016 toonde de foto van een gevlucht Syrisch kind; verdronken en aangespoeld op het strand. Sean Gallagher, 'Shamoon wiper malware returns with a vengeance', *Ars Technica*, 12 januari 2016. Zie: https://arstechnica.com/information-technology/2016/12/shamoon-wiper-malware-returns-with-a-vengeance/.
19 Een bootloader betreft software die na het opstarten van een computer bekijkt welke hardware aanwezig is en welke stuurprogramma's voor die hardware moeten worden geladen. Deze opstartsoftware is ook nodig om het besturingssysteem op te starten. Voorbeelden van opstartsoftware zijn de Unified Extensible Firmware Interface (UEFI) en het wat oudere Basic Input / Output System (BIOS).
20 Bij het partitioneren van het computergeheugen deel je de fysieke opslagruimte op de harde schijf op in gedeeltes. Zo kun je bijvoorbeeld één opstartbare partitie gebruiken voor het besturingssysteem, één partitie voor programma-toepassingen en één partitie om gegevens op te slaan. Een dergelijke indeling wordt gemaakt door de (oudere) Master Boot Record (MBR) of (nieuwere) GUID Partition Table (GPT).
21 Firmware is software die is ingebed in de hardware van een computer. Firmware zorgt ervoor dat een computer of computeronderdelen, of het apparaat waar die computer in zit, kunnen opstarten en vervolgens goed kunnen functioneren.

niet voor de hand.[22] Logischer is dat een aanvaller een wiper bijvoorbeeld gebruikt om sporen van andere activiteiten, zoals spionage, te wissen. Het kan uiteraard ook gewoon de bedoeling zijn om permanente schade aan te richten.

Ontstaansgeschiedenis

In 2012 vielen onbekende hackers Saudi Aramco aan; een Saoedisch staatsoliebedrijf en een van de grootste oliebedrijven ter wereld. De schade was ongekend. Van meer dan 35.000 Windows-computers werden alle gegevens gewist en de computers zelf werden vervolgens onherstelbaar beschadigd. Hoewel de olie*productie* onverminderd doorliep, was het *handelen* erin nagenoeg onmogelijk geworden.[23] Een groep die zichzelf Cutting Sword of Justice noemde, claimde de verantwoordelijkheid. De malware kreeg de naam 'Shamoon'. Het vermoeden bestond dat de cyberaanval het werk was van Iraanse statelijke actoren.[24] Het land reageerde met deze aanval waarschijnlijk op een soortgelijke aanval eerder dat jaar gericht tegen het Iraanse ministerie van olie en de nationale Iraanse Oliemaatschappij. In 2016,[25] 2017,[26] en 2018[27] keerde Shamoon nagenoeg ongewijzigd terug op het toneel en wederom waren computers van de oliesector in Saoedi-Arabië het doelwit.

Het Russische cybersecuritybedrijf Kaspersky onthulde in 2012 dat Shamoon gelijkenissen vertoonde met malware die eerder juist tegen Iran was gebruikt. Kaspersky's onderzoek leidde destijds tot de ontdekking van de zogeheten *Flame*-malware.[28] Op zich lijkt dat niet zo relevant, ware het niet dat die Flame-malware[29] op zijn beurt weer gelijkenissen vertoonde met het *Stuxnet*-virus,[30] de (vermeend) Amerikaans-Israëlische malware die schade aanrichtte bij de Iraanse uraniumverrijkingsinstallatie in Natanz.[31] Kaspersky vond aanwijzingen dat de makers van Stuxnet dezelfde waren als de zogeheten Equation Group en daarmee de Amerikaanse National Security Agency (NSA); of daarmee op zijn minst nauwe banden hadden.[32] Het initiële gebruik van wiperware als cyberwapen is daarmee vermoedelijk te herleiden naar de Verenigde Staten.

In 2013 maakte de, aan de Noord-Koreaanse staat gelieerde, hackergroep Dark Seoul gebruik van wiperware (*Trojan.Jokra*) tegen Zuid-Koreaanse doelwitten in de financiële en mediasector. Hoewel de malware 32.000 computers beschadigde van zes financiële en mediabedrijven,[33] bleek de gebruikte techniek vrij eenvoudig.[34] Enkele doorgaans door *Advanced Persistent Threats* (APT)[35] gebruikte technieken waren bijvoorbeeld niet benut. Deze wetenschap

22 Bij ransomware verstrekken hackers doorgaans tegen betaling de cryptografische sleutel waarmee het slachtoffer de versleutelde data zou kunnen terughalen. Bij wiperware is het doel data of computers vernietigen, niet om die data of computers na betaling weer te herstellen.

23 Jose Pagliery, 'The inside story of the biggest hack in history', *CNN Business*, 5 augustus 2015. Zie: https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

24 Council on Foreign Relations, Cyber Operations tracker, 'Compromise of Saudi Aramco and RasGas', 2012. Zie: https://www.cfr.org/cyber-operations/#Timeline.

25 Symantec Threat Hunter Team, 'Shamoon: Back from the dead and destructive as ever', 30 november 2016. Zie: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shamoon-back-destructive.

26 'Saudi Arabia warns on cyber defense as Shamoon resurfaces', *Reuters*, 23 januari 2017. Zie: https://www.reuters.com/article/us-saudi-cyber-idUSKBN1571ZR.

27 In 2018 was weliswaar een Italiaans bedrijf in de oliesector het doelwit, maar grootste klant van dat bedrijf was Saudi Aramco. Zie 'Saipem says Shamoon variant crippled hundreds of computers', *Reuters,* 12 december 2018, https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA.

28 Kaspersky Lab Expert, 'Shamoon the Wiper – Copycats at Work, 16 augustus 2012. Zie: https://web.archive.org/web/20120820041239/http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work.

29 Flame had overigens de mogelijkheid om alle sporen van de eigen aanwezigheid te wissen na ontvangst van een *kill*-commando. Dergelijke ingebouwde zelfdestructie (*self-kill logic inside*) heeft overeenkomsten met de technieken die zijn benodigd voor destructie van data of andere computerbestanden.

30 Boldizsár Bencsáth et al, 'The Cousins of Stuxnet: Duqu, Flame, and Gauss', *Future Internet* 4 (2012) (4) 971-1003. Zie: https://doi.org/10.3390/fi4040971.

31 Kim Zetter, *Countdown to Zero: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, 2015); James Long, 'Stuxnet : A Digital Staff Ride', Modern War Institute, 2019.

32 Kaspersky Lab, 'Equation Group Questions and Answers', februari 2015. Zie: https://web.archive.org/web/20150217023145/https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

33 Michael Pearson, K.J. Kwon, en Jethro Mullen, 'Hacking attack on South Korea traced to China, officials say', *CNN*, 20 maart 2013. Zie: https://edition.cnn.com/2013/03/20/world/asia/south-korea-computer-outage/index.html.

34 Jonathan A.P. Marpaung en HoonJae Lee, 'Cyber Attack: Could it be worse?', *CISAK 2012 – C1/O/8*. Zie: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/Dark_Seoul_Cyberattack.pdf.

35 Een *Advanced Persistent Threat* (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.

duidt op het gevaar dat ook hackers met minder geavanceerde kennis en kunde dit soort destructieve malware kunnen ontwikkelen en inzetten.

Op 27 juni 2017, de avond voorafgaand aan de dag waarop in Oekraïne de onafhankelijkheid van de Sovjetunie wordt gevierd, voerden Russische hackers cyberaanvallen uit op Oekraïne, waarbij onder meer de financiële, media- en energiesector werden getroffen.[36] Kort daarop verspreidde deze malware zich over andere delen van de wereld, waaronder de VS, Europa en Rusland. De malware werd berucht onder de naam *NotPetya*.[37] Het kreeg deze benaming omdat de gebruikte code grotendeels leek op de in 2016 opgedoken *Petya*-gijzelsoftware (ransomware), maar deels ook niet. Waar de Petya-malware echter een crimineel doel nastreefde (bestanden versleutelen en deze na betaling van losgeld vrijgeven), leek de NotPetya-malware zuiver bedoeld om zowel data als computers onherstelbaar te beschadigen.[38] Het vernuftige aan deze aanval was vooral de wijze waarop de malware bij de slachtoffers werd binnengeloodst. De aanval vond plaats via een *supply-chain attack*. De aanvallers hackten een Oekraïense leverancier van populaire boekhoudsoftware en besmetten vervolgens hun legitieme software met malware. De slachtoffers haalden vervolgens met een reguliere software-update automatisch de malware binnen. De schade die NotPetya wereldwijd aanrichtte, werd geschat op een miljard dollar.[39]

In 2018 verstoorden hackers de openingsceremonie van de Olympische Winterspelen in het Zuid-Koreaanse Pyeongchang. De technologisch geavanceerde wiperware *Olympic Destroyer* vernietigde een beperkte hoeveelheid databestanden en enkele computers, alle direct gerelateerd aan de Winterspelen. De malware dupliceerde en verspreidde zichzelf, waardoor wordt aangenomen dat het daadwerkelijke doelwit zich dieper in het netwerk bevond.[40] Opvallend aan deze aanval was dat de malware zodanig was geprogrammeerd, dat die niet zijn eigen sporen wiste. Het leek erop dat de aanvaller juist wilde dat de malware werd ontdekt. De forensische sporen in de malware duidden op meerdere mogelijke daders, waaronder Noord-Korea, Rusland en China. In een diepgaand onderzoek stuitten onderzoekers op meerdere *false flags*,[41] waaronder bewust aangebrachte 'digitale vingerafdrukken', waarschijnlijk bedoeld om daarmee de attributie van deze cyberaanval te bemoeilijken. Achter deze cyberaanval bleken uiteindelijk hackers van de Russische militaire inlichtingendienst (GRU) schuil te gaan.[42]

Naast voornoemde cyberaanvallen die internationaal de aandacht trokken, vonden in 2017 en 2019 aanvallen plaats met twee nagenoeg identieke wipers vermomd als ransomware, respectievelijk *Ordinypt*[43] en *GermanWiper*,[44] die hun pijlen alleen richtten op Duitstalige doelwitten. En in 2019 en 2020 was het Midden-Oosten wederom het toneel van wiperware-aanvallen. De *Dustman* en *ZeroCleare* malware vertoonden gelijkenissen met het eerder gebruikte Shamoon. De doelwitten bevonden zich wederom in de energiesector, met name de olie- en gasindustrie. Onderzoekers van IBM

36 U.S. Department of Justice, United States District Court Western District of Pennsylvania, Indictment No. 20-316, 15 oktober 020, 16. Zie: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiZkob246DvAhUM1hoKHX4WDJAQFjABegQIARAD&url=https%3A%2F%2Fwww.justice.gov%2Fopa%2Fpress-release%2Ffile%2F1328521%2Fdownload&usg=AOvVaw0vAt3KDfKocmOCkUj0gujJ.

37 Andere benamingen zijn: Nyetya, ExPetr, PetrWrap, Win32/Diskcoder.C.

38 Anton Cherepanov, 'TeleBots are back: Supply-chain attacks against Ukraine', ESET, 30 juni 2017. Zie: https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine/.

39 U.S. Department of Justice, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace', 19 oktober 2020. Zie: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

40 Andy Greenberg, '"Olympic Destroyer" Malware Hit Pyeongchang Ahead of Opening Ceremony', *Wired*, 12 februari 2018. Zie: https://www.wired.com/story/olympic-destroyer-malware-pyeongchang-opening-ceremony/.

41 *False flags* zijn bewust aangebrachte of gefalsificeerde 'bewijzen' die zijn bedoeld om het onderzoek naar de identiteit van een daadwerkelijke dader van een activiteit te bemoeilijken.

42 De GRU staat voor *Glavnoye Razvedyvatelnoye Upravlenie* (Hoofdbureau voor Inlichtingen), zie ook: U.S. Department of Justice, 'Six Russian GRU Officers Charged'.

43 Catalin Cimpanu, 'Ordinypt Ransomware Intentionally Destroys Files, Currently Targeting Germany', *BleepingComputer*, 9 november 2017. Zie: https://www.bleepingcomputer.com/news/security/ordinypt-ransomware-intentionally-destroys-files-currently-targeting-germany/.

44 Catalin Cimpanu, 'GermanWiper ransomware hits Germany hard, destroys files, asks for ransom', *ZDnet*, 2 augustus 2 2019. Zie: https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/.

wezen Iraanse statelijke actoren aan als vermoedelijke daders.[45]

Explosie aan wipers in Oekraïne

De huidige Russisch-Oekraïense oorlog is vooral een kinetisch gevecht waarbij de fysieke verwoesting alle andere activiteiten overschaduwt. Daardoor lijkt cyberoorlogvoering in dit conflict geen rol van betekenis te spelen. Desondanks woedt er wel degelijk ook een gevecht in cyberspace. In de aanloop naar de invasie op 24 februari 2022, en in de weken direct daarna, voerden pro-Russische hackers cyberaanvallen uit ter ondersteuning van, en afgestemd op, Russische kinetische militaire operaties.[46] Vooral het gebruik van wiperware als cyberwapen viel daarbij op. Uit de hierboven beschreven ontstaansgeschiedenis blijkt dat het afgelopen decennium slechts een bescheiden aantal wipers is ingezet om verscheidene redenen en tegen uiteenlopende doelwitten. Sinds de Russische invasie is het gebruik van wiperware voor militaire doeleinden significant gestegen. Mandiant telde in de eerste maanden van 2022 meer destructieve malware dan de afgelopen acht jaar.[47] En waar eerst voornamelijk de kantoorautomatisering of informatietechnologie (IT) het doelwit was, worden de pijlen inmiddels ook gericht op (de computers van) de operationele technologie (OT); ofwel de industriële controlesystemen (ICS) die zorgen voor het monitoren en aansturen van industriële processen en systemen van bijvoorbeeld kritieke infrastructuur, zoals de olie en gasindustrie, watervoorziening, telecommunicatie of energiecentrales.

Halverwege januari 2022 (dus nog voor de invasie) maakte Microsoft bekend dat het een malware-aanval had ontdekt die was gericht tegen meerdere instanties in Oekraïne.[48] Deze wiperware (*Whispergate*) leek weliswaar op gijzelsoftware,[49] maar was dat klaarblijkelijk niet. De malware wiste de data op de aangevallen Windowscomputers en vernietigde vervolgens het opstartmechanisme van die aangevallen computers waardoor ze niet meer te gebruiken waren.

Op de dag voorafgaand aan de invasie vielen pro-Russische hackers het Viasat satelliet-internetcommunicatiesysteem aan. Dat het communicatiesysteem was gehackt, bleek overigens pas nadat de bewakings- en regelapparatuur van zo'n 5.800 windturbines in Duitsland(!) op onverklaarbare wijze was weggevallen.[50] De wiperware (*AcidRain*) bleek ontwikkeld om gegevens van modems en routers te wissen, waardoor die onbruikbaar werden. Als gevolg van die cyberaanval hadden grote delen van Oekraïne geen toegang meer tot internetcommunicatie. Het verlies aan *battlefield communications* in de regio van het destijds zwaar bedreigde Kyiv maakte de Oekraïense troepen aldaar nagenoeg blind voor Russische troepen en hun bewegingen.[51] De aanval op Viasat laat zien dat – mits gecoördineerd en afgestemd in tijd – cyberaanvallen operationele steun kunnen bieden aan andere militaire operaties door technologie van de tegenstander te ontregelen of te vernietigen.[52]

Op diezelfde dag voorafgaand aan de invasie maakten meerdere cybersecuritybedrijven melding van nieuw ontdekte *disk-wiping* mal-

45 IBM Security Intelligence, 'Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East', *IBM X-Force*, december 2019. Zie: https://securityintelligence.com/posts/new-destructive-wiper-zerocleare-targets-energy-sector-in-the-middle-east/.

46 Paul A.L. Ducheine, B.M.J. Pijpers, en Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', in: Jeff Michaels en Tim Sweijs (red.), *Debating the Future of War (after the Invasion of Ukraine)* (Hurst Publishers, nog te verschijnen 2023); Jon Bateman, 'Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications', *Carnegie Endowment for International Peace*, december 2022.

47 Mandiant, M-Trends 2023, Mandiant Special Report, *Initial Destructive Cyber Operations and Military Invasion (February 2022–April 2022)* 57. Zie: https://mandiant.widen.net/s/dlzgn6w26n/m-trends-2023.

48 Microsoft Threat Intelligence Centre (MSTIC), 'Destructive malware targeting Ukrainian organizations', 15 januari 2022.

49 De malware toonde een bericht waarin om losgeld werd gevraagd, waardoor de aanval leek op een ransomware aanval van criminelen.

50 Juan Andrés Guerrero-Saade, 'AcidRain | A Modem Wiper Rains Down on Europe', *Sentinel Labs*, 31 maart 2022. Zie: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

51 Blessing, 'Revisiting the Russian Viasat Hack'.

52 Patrick Howell O'Neill, 'Russia hacked an American satellite company one hour before the Ukraine invasion', *MIT Technology Review*, 10 mei 2022. Zie: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/.

ware. *HermeticWiper*[53] was gericht tegen honderden computersystemen in Oekraïne; voornamelijk in de financiële sector, de krijgsmacht, de luchtvaart en de IT-sector.[54] De wiper-aanval volgde op een wekenlange reeks DDoS-aanvallen op Oekraïense overheidswebsites.[55] De makers gebruikten voor hun cyberaanval eenvoudige, legitieme software om gegevens te wissen.[56]

Op 24 februari 2022, de dag van de invasie, ontdekte cybersecuritybedrijf ESET wederom nieuwe wiperware (*IsaacWiper)*.[57] Ditmaal waren vooral netwerken van de Oekraïense overheid het doelwit. Uit forensisch bewijs blijkt dat de aanval enige maanden tevoren was voorbereid en wellicht zelfs eerder was ingezet tegen andere doelwitten. De malware werkte schijnbaar niet geheel naar wens, want een dag na de initiële inzet lanceerden de aanvallers een nieuwe versie met daarin de mogelijkheid om fouten te kunnen opsporen.

In de eerste week na de invasie trachtten Russische troepen en pro-Russische hackers hun grip op de informatieomgeving in Oekraïne te

53 De malware misbruikte een 'digitaal echtheidscertificaat' van het Cypriotische bedrijf 'Hermetica Digital Ltd', vandaar dat de ontdekkers de malware deze naam gaven. Het bedrijf 'Hermetica' zelf zat niet achter die aanval.

54 Symantec Threat Hunter Team, 'Ukraine: Disk-wiping Attacks precede Russian Invasion', 24 februari 2022.

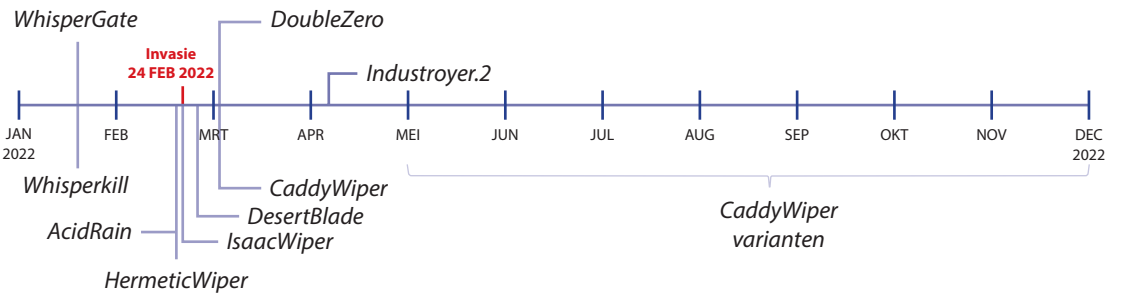
55 ESET, 'HermeticWiper: New data-wiping malware hits Ukraine', 24 februari 2022. Zie: https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/.

56 Juan Andrés Guerrero-Saade, 'HermeticWiper / New destructive malware used in Cyber Attacks on Ukraine', *Sentinel Labs*, 23 februari. Zie: https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

57 ESET Research, 'IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine', 1 maart 2022. Zie: https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/.

USAID-bestuurder Samantha Power (rechts) en de Amerikaanse ambassadeur in Oekraïne Bridget Brink bezoeken een door Russische aanvallen beschadigde energiecentrale in Kyiv. Russische cyberaanvallen met wiperware ondersteunen kinetische militaire campagnes en richten zich ook op kritieke infrastructuur zoals energiecentrales

FOTO U.S. EMBASSY KYIV



Figuur 1 (Ontdekking van) negen soorten wiperware rondom de grootschalige Russische invasie van Oekraïne in 2022

verstevigen. Op 1 maart kondigde Rusland aan doelen uit te schakelen die 'desinformatie' zouden verspreiden.[58] Zijn krijgsmacht voerde vervolgens raketaanvallen uit op onder meer een televisietoren in Kyiv. Diezelfde dag vielen hackers een grote omroepmaatschappij aan met wiperware (*DesertBlade*). De aanvallen suggereerden een gesynchroniseerde actie, erop gericht om zowel kinetische als cybereffecten te creëren tegen de belangrijkste informatiebronnen van de Oekraïense bevolking. Pogingen om mediabedrijven van een afstand uit te schakelen met malware is een trend die in dit conflict voortdurend wordt waargenomen.[59]

In de derde week na de invasie trof cybersecuritybedrijf ESET een nieuwe wiperware aan in de computers en netwerken van Oekraïense organisaties.[60] Deze malware (*CaddyWiper*) blijkt technologisch relatief eenvoudig en vertoont geen overeenkomsten met eerder ontdekte wipers. Dit suggereert dat de malware is ontwikkeld door andere hackers. Rond diezelfde periode dook ook *DoubleZero* op. Deze wiperware hanteerde twee verschillende technieken om gegevens te wissen en was gericht tegen bedrijven in de communicatie- en mediasector.[61]

In april voerden hackers een cyberaanval uit op het Oekraïense elektriciteitsnetwerk. De zogeheten *Industroyer2*-malware was speciaal ontwikkeld tegen ICS en gebaseerd op eerder gebruikte malware die in 2016 (eveneens in Oekraïne) stroomuitval veroorzaakte. Ditmaal was de ICS-malware aangevuld met maar liefst vier verschillende destructieve wiperwarefamilies, gericht tegen verschillende computersystemen en netwerken.[62] Industroyer2 sloot de eerste golf aanvallen met destructieve wipers af.

In de zomermaanden van 2022 bestookten pro-Russische hackers voornamelijk de Oekraïense logistieke en transportsector.[63] Het was de tijd dat wapens en voorraden vanuit het westen werden aangevoerd naar het oostfront, terwijl vluchtelingen via diezelfde routes, maar in tegengestelde richting, een veilig heenkomen zochten. Rusland bestookte de Oekraïense transport-infrastructuur met zowel raketten als wiperware en ransomware. Tegelijkertijd werd de transportsector van NAVO-lid Polen (en knooppunt in de logistieke keten naar en vanuit Oekraïne) bestookt met *Prestige*-ransomware.

Ook in de maanden na de initiële reeks destructieve cyberaanvallen zijn wipers ingezet,

58 TASS Russian News Agency, 'Russian Defense Ministry warns about strikes being prepared on military sites in Kiev'. Zie: https://web.archive.org/web/20220301133913/https://tass.com/defense/1414199.

59 Microsoft Digital Security Unit, *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*, 12.

60 ESET, 'CaddyWiper: New wiper malware discovered in Ukraine', 15 maart 2022. Zie: https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/.

61 Andrii Bezverkhyi, 'DoubleZero Destructive Malware Used in Cyber-Attacks at Ukrainian Companies: CERT-UA Alert', 22 maart 2022. Zie: https://socprime.com/blog/doublezero-destructive-malware-used-in-cyber-attacks-at-ukrainian-companies-cert-ua-alert/.

62 Naast CaddyWiper (tegen ICS-netwerk) gebruikten de aanvallers ook de wipers *OrcShred, SoloShred* en *AwfulShred* (alle gericht tegen Linux en Solaris netwerken). Zie: ESET Research, 'Industroyer2: Industroyer reloaded', 12 april 2022.

63 Microsoft Threat Intelligence, 'A year of Russian hybrid warfare in Ukraine, What we have learned about nation state tactics so far and what may be on the horizon', 15 maart 2023, 8.

maar de aanvallen leken steeds meer gehaast, en minder gecoördineerd uitgevoerd. Bovendien leken spionageactiviteiten en destructieve aanvallen op dezelfde systemen elkaar te dwarsbomen. Verder kon de Oekraïense cyberverdediging die aanvallen veelal snel en effectief identificeren en mitigeren, nog voordat de cyberwapens hun schadelijk werk konden verrichten.

Analyse: strategische effecten?

In een jaar tijd zijn varianten van negen 'wiperware-families'[64] ingezet tegen vooral civiele objecten van de Oekraïense overheid, kritieke infrastructuur (informatietechnologie, communicatie, energie, transport, gezondheidszorg), het bedrijfsleven en de media. Een klein percentage was rechtstreeks gericht tegen de strijdkrachten.[65] Het is opvallend dat de inzet van deze wipers vooral samenviel met de aanloop naar de invasie en de paar weken daarna. Het is goed mogelijk dat de cyberoperaties bewust waren afgestemd op de geplande kinetische operaties.[66] Deze aanpak zou dan volledig in lijn zijn met het belang dat Rusland hecht aan een beslissende aanval (*decisive impact*) in de eerste weken van een oorlog.[67]

Na de eerste golf cyberaanvallen leken de aanvallers bestaande technieken te standaardiseren en te vereenvoudigen. De malware was bovendien minder gelaagd. De aanvallers verrichtten minder inspanning om hun kwaadaardige computercode te verhullen en namen ook niet meer de moeite om te suggereren dat er sprake was van criminele ransomware.

De aanvallers stapten ook af van de verschillende wipers en concentreerden zich vooral op de doorontwikkeling van de snel aanpasbare en multi-inzetbare CaddyWiper. Door de code van de malware steeds licht te wijzigen, was deze door cybersecurity-systemen moeilijker te detecteren. De aanvallen concentreerden zich in de loop van het conflict weliswaar op de Oekraïense overheid, maar leken desondanks niet echt doelgericht. Het hoge operationele tempo waarin de aanvallers nieuwe malware loslieten op hun slachtoffers, wellicht in een poging om het kinetische gevecht te kunnen ondersteunen, leidde tot fouten en daarmee verminderde effectiviteit van die malware.[68] De eenvoudige CaddyWiper was dan weliswaar minder geavanceerd dan de eerder gebruikte technologisch hoogwaardige NotPetya, maar ook met deze *quick-and-dirty*-wipers bleek Rusland nog steeds in staat digitale chaos te creëren.[69]

In de laatste maanden van 2022 veranderde het aanvalspatroon. De cyberaanvallen leken op de eerder uitgevoerde, gehaaste aanvallen, maar werden wel uitgevoerd tegen geselecteerde targets. In lijn met de kinetische aanvallen was de energiesector daarbij het uitgesproken doelwit. Naast meer selectieve aanvallen bleken de aanvallers ook te kiezen voor variatie in de aanvalswapens; naast wiperware ook ransomware. Rusland zette deze vorm van malware in, al dan niet via (pseudo-)hacktivisten om de inzet van deze eveneens schadelijke malware te kunnen ontkennen.[70]

Van de negen wiper-families waren er zes gericht op het vernietigen van (data op) computers met een Windows-besturingssysteem. Twee wipers zijn ingezet tegen Linux-computers en één tegen een computer met een Solaris-besturingssysteem. Onderzoekers die de malware ontleedden, ontdekten nauwelijks tot geen overeenkomsten in de gebruikte computercode.[71] De enige analogie tussen de wipers was hun destructieve intentie. Dat zou erop kunnen wijzen dat de aanvallen het werk waren van verschillende hackergroepen.

64 Een malware-familie bestaat uit verschillende softwareprogramma's die onderling veel gelijkenissen vertonen in hun computercode.
65 Microsoft Threat Intelligence Centre, 'A year of Russian hybrid Warfare in Ukraine', 5.
66 Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War', *Microsoft*, 2022, 3.
67 Michael Kofman et al, *Russian Military Strategy: Core Tenets and Operational Concepts*, CNA Research Memorandum, 19 oktober 2021, 3. Zie: https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.
68 Mandiant, 'M-Trends 2023', 60.
69 Andy Greenberg, 'Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless', *Wired*, 18 november 2022. Zie: https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.
70 Microsoft Threat Intelligence Centre, 'A year of Russian hybrid Warfare in Ukraine', 12.

Opvallend is dat van alle gebruikte wipers er slechts één (HermeticWiper) werd ingezet in combinatie met een 'worm'-component.[72] Door die worm-functie kon deze malware zichzelf reproduceren en verspreiden over het aangevallen netwerk en dus zonder verdere (menselijke) aansturing zijn vernietigende werk doen. Wel was HermeticWiper zo geprogrammeerd dat de 'gewenste' schade bewust beperkt bleef tot lokale IP-adressen binnen het specifiek aangevallen netwerk. De overige wipers hadden alle geen worm-component en konden zich daardoor sowieso niet ongecontroleerd verspreiden. Een onvoorziene uitbraak, en daarmee onvoorziene schade buiten het bewust aangevallen netwerk, zoals eerder wel het geval was met de NotPetya-cyberaanval, is hierdoor niet mogelijk. Dit kan erop duiden dat de aanvallers niet het risico wilden lopen om abusievelijk andere landen (waaronder NAVO-lidstaten) te treffen.

Eveneens opmerkelijk zijn het gewijzigde aanvalspad en aanvalstechnieken van APT28.[73] Deze Russische statelijke actor richtte zijn aanvallen niet langer direct op de computers van zijn slachtoffers, maar op de infrastructuur aan de randen van een netwerk. In plaats van te phishen naar authentieke inloggegevens van gebruikers, exploiteerde de groep voornamelijk kwetsbaarheden in bijvoorbeeld firewalls, routers en email-servers. Zo kreeg de groep indirect toegang tot de gewenste computersystemen, om vervolgens alsnog de gegevens daarvan te wissen en de computers zelf te beschadigen. De rand-netwerkinfrastructuur zelf lieten de aanvallers onaangetast. Hierdoor creëerden zij een permanente aanwezigheid in de netwerken van hun slachtoffers. Deze indirecte manier van aanvallen stelde de hackers in staat om dezelfde computernetwerken snel en meermaals achter elkaar aan te vallen; of na een wiperware-aanval toegang tot dat netwerk te behouden voor bijvoorbeeld spionagedoeleinden zodra het aangevallen netwerk was hersteld.[74] De Russische militaire inlichtingendienst hoeft daardoor niet langer te kiezen tussen bespioneren of vernietigen van een systeem; op deze wijze zijn beide mogelijk.

In de oorlog in Oekraïne is wiperware vooral ingezet vlak voor de Russische invasie en de eerste fase van de oorlog. De wipers brachten schade toe aan Oekraïense computersystemen en -netwerken, maar leken vooral bedoeld om de militair-operationele campagnes te ondersteunen. Mits goed gepland, zorgvuldig in tijd gesynchroniseerd, en gecoördineerd met andere militaire machtsmiddelen, kan een wiper-aanval zelfs strategische effecten teweegbrengen. De aanval op het Viasat satelliet-internetcommunicatiesysteem kwam hiervoor in aanmerking, als deze succesvol was geweest en de effecten niet tijdig door de inzet van Starlink waren geneutraliseerd.

Lessons to learn voor de Nederlandse krijgsmacht

De vraag is nu of uit het gebruik van wipers in het recente Russisch-Oekraïense conflict conclusies zijn te trekken voor de ontwikkeling van dergelijke cyberwapens voor de Nederlandse krijgsmacht. Daarbij merken we allereerst op dat het heimelijke karakter van cyberoperaties de afhankelijkheid van informatie uit open bronnen buitengewoon groot maakt. Deze afhankelijkheid begrenst niet alleen de volledigheid van bronnenmateriaal, maar kan ook de juistheid van een analyse ondergraven. Daar komt bij dat analyses van een lopend conflict ernstig worden bemoeilijkt door de inherente misleiding waarmee oorlogvoering nu eenmaal gepaard gaat. Ondanks de ongetwijfeld bewuste manipulatie van de beschikbare informatie van zowel Russische als Oekraïense zijde, is het toch mogelijk om bepaalde lessen – positieve en negatieve – te trekken uit de Russische inzet van destructieve softwareprogramma's.

71 Recorded Future, 'Overview of the 9 Distinct Data Wipers Used in the Ukraine War', Insikt Group, 12 mei 2022.

72 Een computerworm is een schadelijk softwareprogramma dat zich zelfstandig, dus zonder enige menselijke interactie, kan vermenigvuldigen en snel en ongecontroleerd verder kan verspreiden in een computernetwerk.

73 APT28 is een beruchte, aan de Russische militaire inlichtingendienst GRU gerelateerde statelijke actor/hackergroep.

74 Mandiant, M-Trends 2023, 57.

Past wiperware in de gereedschapskist van de Nederlandse krijgsmacht? FOTO MCD, ZADRACH SALAMPESSY

Het eerste en belangrijkste verschil tussen de ingezette Russische destructieve programmatuur en een eventuele toepassing van dergelijke cybermiddelen door de Nederlandse krijgsmacht in tijd van een gewapend conflict betreft *targeting*. Waar Rusland de wipers inzette tegen een schijnbaar willekeurige mix van militaire doelwitten, civiele objecten en *dual use*-systemen, is de eigen krijgsmacht uiteraard gebonden aan een verantwoord gebruik van dergelijke middelen. Zonder mogelijkheid om toegebrachte schade te kunnen terugdraaien, zouden wipers die onherstelbare schade aanrichten enkel kunnen worden ingezet tegen militaire doelwitten, zoals wapen-, radar- en (personele en materiële) logistieke systemen of *command and control*-systemen. Deze militaire systemen werken doorgaans met andere (soms *custom made*) besturingssystemen dan commerciële computers, wat de kans op onbedoelde nevenschade aanzienlijk verkleint. Desondanks zijn aanvullende maatregelen noodzakelijk om te garanderen dat de destructieve uitwerking beperkt blijft tot de specifiek aangevallen middelen en dat de middelen geen onbedoelde en ongewenste schade aanrichten in andere omgevingen.

Voor andere doelwitten kan een variant van ransomware in aanmerking komen; zonder de gebruikelijke afpersingsfunctionaliteit, maar met behoud van de mogelijkheid om schade ongedaan te maken. Door computerbestanden van het doelwit cryptografisch te versleutelen, kan worden voldaan aan de eisen van subsidiariteit en proportionaliteit van optreden. Ongewenst of onvoorzien aangerichte schade kan dan, met een cryptografische sleutel,[75] ongedaan worden gemaakt. De mogelijkheid om die 'sleutel' te verschaffen aan getroffen partijen kan zowel nevenschade inperken, als in voorkomend geval na afloop van een conflict een tegenstander in staat stellen schade te herstellen.

75 Een cryptografische sleutel is een speciale set gegevens die onder meer wordt gebruikt voor het coderen en decoderen van computerbestanden of berichten. Is de cryptografische sleutel niet (meer) beschikbaar, dan is het in beginsel onmogelijk om de versleutelde (onleesbare) gegevens weer te ontcijferen.

Een volgende les betreft dan ook de beperkte duur van een eventueel ontzeggingseffect van destructieve programmatuur. Als databestanden zijn gewist, dan is dat vervelend, maar wel relatief makkelijk te herstellen. Als een aangevallen partij over goede back-ups beschikt (niet op hetzelfde computersysteem, maar bijvoorbeeld offline, of in de cloud), dan kan die de schade relatief snel herstellen. Bij eerder militair cyberoptreden van het U.S. Cyber Command tegen ISIS was al gebleken dat zelfs een tegenstander met beperkte technische mogelijkheden relatief snel infrastructuur kon herstellen.[76] Het kennelijke verloop van de wiperinzet door Rusland in Oekraïne lijkt deze eerdere les te bevestigen. Hierbij moet wel worden opgemerkt dat Oekraïne daarbij wordt ondersteund door een breed scala aan westerse overheden (VS, VK, EU) en commerciële IT- en cybersecuritybedrijven (waaronder Microsoft, ESET, Google en Mandiant).[77]

Het herstellen van vernietigde besturingssystemen is weliswaar ook mogelijk,[78] maar vergt een grotere inspanning dan het eenvoudig terugzetten van gewiste databestanden. Vanwege die herstelmogelijkheid is in doctrinaire termen het effect van destructieve programmatuur in beide gevallen eerder te bestempelen als verstoring (*disruption*) dan als vernietiging (*destruction*). Voor langdurig ontzeggen van systemen vallen de Russen dan ook terug op kinetische middelen. Het herstel van kinetisch aangerichte fysieke schade aan digitale infrastructuur en overige middelen vergt een grotere inspanning of duur dan herstel van beschadigde virtuele objecten.

De beperkingen aan de duur van ontzegging van middelen hebben een direct verband met de derde les: de noodzaak om een cyberoperatie af te stemmen op andere vormen van militaire inzet, zodat de effecten van beide soorten operaties elkaar kunnen versterken. In het conflict in Oekraïne lijkt een dergelijke afstemming in veel gevallen gebrekkig, al zijn daar wel degelijk uitzonderingen op. Ten dele ligt dat aan de verschillen in de planningscyclus. In tegenstelling tot kinetische wapens worden cyberwapens niet geproduceerd in een fabriek volgens standaardspecificaties met een standaardeffect; noch liggen die cyberwapens ruim van tevoren klaar voor gebruik. Het ontwerpen, ontwikkelen, maken en inzetten van cyberwapens is een proces dat vaak een aanzienlijke voorbereidingstijd nodig heeft. De planning van een cyberoperatie vraagt dan ook meer tijd dan de dagen of uren van de planning van andere vormen van militair optreden. Toch lijkt het erop dat de Russen hiermee in hun voorbereiding op de invasie wel degelijk rekening hebben gehouden. De (wiper)effectoperaties zijn uitgevoerd op systemen waarop de aanvallers in een eerder stadium al toegang en volledige controle hadden verworven. Een effectoperatie is op die manier sneller uit te voeren dan wanneer de hackers de gehele aanvalsketen (*cyber kill chain*) hadden moeten doorlopen vanaf het moment van de invasie.

In een eerder stadium toegang verkrijgen tot een computer of netwerk en pas nadien (op het gewenste moment) effectbrengers inzetten,[79] stelt de aanvallers in staat om de middelen voor een destructief effect eenvoudig te houden; de cyberwapens hoeven slechts in één enkele functionaliteit te voorzien: destructie. Hebben de aanvallers eenmaal toegang tot een systeem, dan kunnen zij ook gebruik maken van 'living off the land'-technieken; ofwel gebruik (misbruik) maken van organieke, legitieme functionaliteiten van het aangevallen doelwitsysteem. Gebruik van organieke en legitieme functionaliteiten vermindert niet alleen het risico op vroegtijdige ontdekking van de cyberaanval door het doelwit, maar voorkomt ook eventuele ontwerp- of programmeerfouten bij het ontwikkelen van *tailormade* malware. Dezelfde technieken kunnen bovendien herhaald worden ingezet zonder aanpassing of desgewenst met minimale wijzigingen.

76 David E. Sanger en Eric Schmitt, 'U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS', *The New York Times*, 12 juni 2017.

77 Bateman, 'Russia's Wartime Cyber Operations in Ukraine', 14.

78 Bijvoorbeeld door een gewiste ingebouwde harde schijf (met ingebouwd besturingssysteem) compleet te vervangen door een nieuwe, of door een nieuwe externe harde schijf op het systeem aan te sluiten.

79 Zie ook: Anoniem, 'All about access', *Militaire Spectator* 191 (2022) (9), https://militairespectator.nl/artikelen/all-about-access.

Omdat een hacker van tevoren nooit zekerheid heeft over het aan te vallen doelwit,[80] zijn vooraf gecreëerde halffabricaten doorgaans niet praktisch bruikbaar om ongeautoriseerd toegang te verkrijgen tot een computer of netwerk (*access operations*). Voor destructieve programmatuur die wordt gebruikt nadat de noodzakelijke toegang is verkregen, kunnen deze voorbereide producten wel degelijk nuttig zijn. Deze opzet is dan ook als een navolgenswaardige *best practice* over te nemen voor het Nederlandse optreden.

De volgende les gaat over de ontwikkeling van destructieve programmatuur. Zoals hierboven genoemd, is het aanmaken van halffabricaten nuttig. De ontwikkeling daarvan vindt bij voorkeur modulair plaats en in gescheiden ontwikkelstraten;[81] dit ondervangt een eventueel *single point of failure*. De naleving van (software)ontwikkelstandaarden borgt de kwaliteit van de op te leveren producten. Het inzetten van ondoordachte of gebrekkig ontwikkelde code kan leiden tot onvoorziene en wellicht zelfs ongewenste uitkomsten. Omdat een slachtoffer het gebruik van destructieve malware waarschijnlijk snel onderkent, is het raadzaam dergelijke middelen bij voorkeur niet als multifunctioneel 'Zwitsers zakmes' te ontwikkelen, maar als specifiek toegespitste code ten behoeve van slechts één enkele functionaliteit. Dat voorkomt dat overige functionaliteiten onnodig vroegtijdig worden onderkend door eventuele opponenten.

Conclusie

In het huidige Russisch-Oekraïens conflict is het gebruik van (destructieve) wiperware om data en computers te vernietigen significant: in de eerste maanden van 2022 is meer wiperware ingezet tegen Oekraïne, dan tegen landen wereldwijd in de afgelopen acht jaar. De inzet van deze wipers viel samen met de aanloop naar de invasie en de paar weken daarna. Het is goed mogelijk dat de cyberoperaties bewust waren afgestemd op de geplande kinetische operaties.

In een gewapend conflict kunnen wipers (ondersteunend) worden ingezet tegen militaire doelwitten, zoals wapen-, radar- en (personele en materiële) logistieke systemen of command and control-systemen. Deze systemen werken doorgaans met andere besturingssystemen dan commerciële computers, wat de kans op nevenschade verkleint. Aanvullende maatregelen voorkomen onbedoelde en ongewenste schade in andere omgevingen.

De inzet van destructieve programmatuur heeft een beperkt ontzeggingseffect in tijdsduur; de schade is relatief snel te herstellen. Doctrinair gezien is er daarom eerder sprake van verstoring (disruption) dan van vernietiging (destruction). De gelimiteerde tijdspanne waarin het effect wordt gecreëerd, noopt tot afstemming van dit soort cyberoperaties op andere vormen van militaire inzet, zodat de effecten van de operaties elkaar optimaal kunnen versterken.

De inzet van cybermiddelen kent een significant langere planningscyclus dan de planning van andere militaire middelen. Vroegtijdige toegang tot een computer of netwerk stelt de aanvaller in staat de middelen voor een destructief effect eenvoudig te houden; de malware hoeft slechts één functionaliteit te bezitten (wipen) en kan van tevoren worden ontwikkeld als halffabricaat.

Vanwege de benodigde planningscyclus en door de herstelmogelijkheid van schade zou de Nederlandse krijgsmacht wiperware bij uitstek strategisch kunnen inzetten, vooral bij een initiële (verrassings)aanval in combinatie met andere militaire middelen. Voor operationeel of zelfs tactisch gebruik in een dynamisch gevecht zijn deze middelen minder of in het geheel niet geschikt. ■

80 Onder meer besturingssystemen, netwerkconfiguratie, hardware, software, firmware, firewalls, indringer preventie en -detectiesystemen, plus alle versies, updates en patches, verschillen doorgaans per doelwit.

81 Kleine teams van ontwikkelaars en programmeurs werken daarbij in verschillende fasen (ontwikkelen, testen, acceptatie, productie) gecompartimenteerd aan bepaalde functionaliteit van de malware.

Speciale operaties in turbulente tijden

Een nieuw perspectief op de inzet van special operations forces

Prof. dr. Martijn Kitzen[1*]

Bij speciale operaties denkt men vaak aan spectaculaire acties. Wat is de realiteit, hoe zien speciale operaties eruit en wie worden daarbij ingezet? Dit artikel schetst een perspectief op de rol van special operations forces in de huidige uitdagende veiligheidssituatie. Het is een bewerking van de oratie die prof. dr. Kitzen op 15 juni 2023 uitsprak ter aanvaarding van de leerstoel Irreguliere Oorlogvoering & Speciale Operaties aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie.

De uitdagende veiligheidssituatie van tegenwoordig heeft een nieuw perspectief nodig op de rol van special forces, zeker voor relatief kleine landen als Nederland en België

FOTO MCD, VALERIE KUYPERS

Waar denkt u aan bij speciale operaties? Grote kans dat deze vraag beelden oproept van een groepje tot de tanden bewapende vechtersbazen die met spectaculaire acties een goed bewaakt doelwit weten uit te schakelen. Dat is immers de manier waarop zulke operaties vaak in films of boeken worden voorgesteld. De oudere generatie herinnert zich waarschijnlijk wel *The Guns of Navarone* en meer recent waren er *American Sniper*, *Zero Dark Thirty* en *12 Strong*. Nu zijn die laatste drie weliswaar gebaseerd op echte ervaringen tijdens de Global War on Terror, maar ook hier geldt dat zulke 'realistische' films een gedramatiseerd en vaak eenzijdig beeld schetsen als het gaat om speciale operaties en de *operators* die ze uitvoeren. Dat valt nog meer op als we naar actiefilms kijken. John James Rambo blijkt het door zijn achtergrond als *Green Beret* tijdens de Vietnamoorlog in zijn eentje te kunnen opnemen tegen een overmacht aan tegenstanders en dat telkens weer. Dat zien we ook bij het *A-Team* – die naam is een rechtstreekse verwijzing naar de special forces van de Amerikaanse landmacht – en in de film *Commando* – ook een duidelijke verwijzing – waarin Arnold Schwarzenegger als gepensioneerd kolonel zijn dochter uit de handen van een criminele bende weet te redden.[2] Speciale operaties spreken zozeer tot de verbeelding dat ze zelfs een thema zijn voor absurdistische films zoals *Inglourious Basterds* en ook genres als fantasy en science fiction maken er dankbaar gebruik van. Zo draait *Star Wars* om een kleine groep van zeer begaafde krijgers, de Jedi, die er met hun acties uiteindelijk in slagen een heel galactisch keizerrijk op de knieën te krijgen.

Tot zover het populaire beeld. Wat is de realiteit, hoe zien speciale operaties eruit en wie worden daarbij ingezet? En wat is de betekenis van dit soort operaties in de huidige veiligheidsomgeving? Het zijn turbulente tijden waarin we te maken hebben met een intensivering van strategische competitie tussen grootmachten,

1 * Professor dr. Martijn Kitzen is hoogleraar Irreguliere Oorlogvoering & Speciale Operaties aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie.

2 A-Team is de kortere naam voor Special Forces Operational Detachment Alpha, de basisformatie waarin de speciale eenheden van de U.S. Army optreden.

Tijdens de middeleeuwen en vroege renaissance groeiden speciale operaties uit tot een veelgebruikt politiek-militair instrument

een grootschalige oorlog in Europa en geavanceerde niet-statelijke dreigingen. Bovendien geldt dat conflicten zich steeds minder laten beperken in tijd en ruimte. Het is moeilijk vast te stellen wanneer een confrontatie precies begint of eindigt en lokale gebeurtenissen kunnen – al dan niet door gebruik van het virtuele domein – wereldwijd effect hebben. Dit artikel wil een perspectief schetsen op de rol van special operations forces in deze uitdagende veiligheidssituatie. Daartoe gaat het eerst in op wat speciale operaties zijn en welke soort eenheden daarbij betrokken zijn. Om die vraag te kunnen beantwoorden wordt achtereenvolgens de geschiedenis van deze vorm van militair optreden en de conceptuele benadering ervan behandeld. Vervolgens is het belangrijk stil te staan bij de dreigingen waarmee we geconfronteerd worden. Al deze elementen vormen de basis voor een nieuw perspectief op de inzet van special operations forces. Hierbij gaat het vooral om het definiëren van het palet van mogelijke taken en rollen vanuit het gezichtspunt van een klein land als Nederland of België. Ter afsluiting staat dit artikel stil bij de betekenis van deze bevindingen voor het onderzoek en onderwijs van de sectie Irreguliere Oorlogvoering & Speciale Operaties aan de Faculteit Militaire Wetenschappen (FMW).

Speciale operaties in historisch perspectief

De geschiedenis zit vol met voorbeelden van wat we tegenwoordig speciale operaties noemen. Er zijn tal van variaties als het gaat om rol, betekenis, uitvoering en betrokken personen. De ontwikkeling van dit soort optreden is waarschijnlijk net zo oud als oorlogvoering zelf en gaat dus terug tot de eerste conflicten. De westerse militaire geschiedenis beschouwt het paard van Troje als een van de eerste op schrift gestelde voorbeelden.[3] Na de klassieke oudheid groeiden speciale operaties tijdens de middeleeuwen en vroege renaissance uit tot een veelgebruikt politiek-militair instrument.[4] Adellijke heersers, ridders en huurlingen zagen het als een middel om langdurige, kostbare oorlogen of een beleg te voorkomen door bijvoorbeeld de leiders van de tegenstander te doden of ontvoeren. We hebben overigens uit deze periode ook voldoende illustraties van het feit dat zulke acties niet altijd even goed verliepen. De 15e-eeuwse *Kroniek van Den Haag* vermeldt bijvoorbeeld een onsuccesvolle poging van de Franse koning om de zoon van zijn rivaal, de hertog van Bourgondië, te ontvoeren uit diens kasteel in Gorinchem.[5] Daartoe ging de Bastaard van Rubempré, een beruchte huurling van de Franse vorst, in 1464 met een bende op pad. De heren namen uitgebreid de tijd om vanuit de meest luxe herberg de boel te verkennen terwijl ze zich voordeden als kooplieden. Na drie weken werd de gastvrouw toch wat achterdochtig en dat leidde tot de ontmaskering van de operatie. Deze hele affaire betekende een strategisch gezichtsverlies voor de Franse koning en versterkte de positie van zijn opponenten. Nu we toch in onze streken zijn aanbeland kunnen we natuurlijk ook niet onbenoemd laten dat op het kasteel van Breda de bekendste speciale operatie uit de Nederlandse geschiedenis heeft plaatsgevonden toen op 4 maart 1590 het turfschip met een verborgen strijdmacht binnen de muren aanlegde. Aangekomen bij deze unieke gebeurtenis en plek, wil ik een sprong maken naar de ontwikkelingen in onze tijd.

Moderne westerse speciale operaties vinden hun oorsprong in de Tweede Wereldoorlog waarin

3 Zie bijvoorbeeld John Arquilla, *From Troy to Entebbe, Special Operations in Ancient and Modern Times* (Lanham, University Press of America, 1996); Derek Leebaert, *To Dare and to Conquer: Special Operations and the Destiny of Nations, from Achilles to Al Qaeda* (New York, Little, Brown & Co, 2006).

4 Yuval Noah Harari, *Special Operations in the Age of Chivalry, 1100-1550* (Woodbridge, The Boydell Press, 2007) 184.

5 Harari, *Special Operations in the Age of Chivalry*, 134-140.

Het populaire beeld van speciale operaties bestaat uit tot de tanden bewapende vechtersbazen die spectaculaire acties uitvoeren. Maar wat is de realiteit? FOTO U.S. NAVY, KATIE COX

diverse nieuwe eenheden werden opgericht om de operaties van conventionele troepen te ondersteunen, strategische doelen uit te schakelen, inlichtingen te verzamelen en het verzet te organiseren, trainen en begeleiden.[6] In deze periode ligt ook de oorsprong van de Nederlandse commando's die vanaf 1942 gevormd werden door het Britse leger. 22 maart, de dag dat de eerste vrijwilligers hun opleiding begonnen, wordt gezien als de geboortedag van het Korps Commandotroepen (KCT).[7] Naast soortgelijke initiatieven vroeg de grote verscheidenheid in missies ook om diversiteit onder wat men toen al special forces noemde. Het eveneens Nederlandse Bureau Bijzondere Opdrachten (BBO) maakte bijvoorbeeld gebruik van speciaal geselecteerde mannen en vrouwen met heel verschillende achtergronden.[8] Direct na het einde van de oorlog werd het grootste deel van de nieuw opgerichte eenheden weer opgeheven. Duitsland en Japan waren verslagen en men zag de noodzaak niet deze capaciteit in stand te houden.

Dekolonisatieconflicten en de Koude Oorlog leidden echter al snel tot een hernieuwde vraag. Het bestrijden van guerrillabewegingen vroeg om een specialistische aanpak en om daarin te voorzien werden er nieuwe eenheden opgericht.

6 Zie bijvoorbeeld Christopher Marsh, James D. Kiras en Patricia J. Blocksome, *Special Operations, Out of the Shadows* (Boulder, Lynne Riener, 2020) 1-2; Bernd Horn, 'The evolution of SOF and the rise of SOF Power', in Jessica Glicken Turnley, Eyal Ben-Ari en Kobi Michael (red.), *Special Operations Forces in the 21st Century, Perspectives from the Social Sciences* (Abingdon, Routledge, 2019) 15-27; Will Irwin en Isaiah Wilson III, *The Fourth Age of SOF: The Use and Utility of Special Operations Forces in a New Age* (Tampa, JSOU Press, 2022) 9-48; Yair Ansbacher en Ron Schleifer, 'The three ages of modern Western special operations forces', *Comparative Strategy* 41 (2022) (1) 32-45. Zowel Irwin & Wilson als Ansbacher & Schleifer onderkennen drie ontwikkelingsgolven in het ontstaan van moderne westerse speciale operations forces. Hoewel de precieze afbakening verschilt komen de drie periodes grofweg overeen met de Tweede wereldoorlog, de Koude Oorlog en de periode daarna, die wordt gedomineerd door de Global War on Terror.

7 Arthur ten Cate en Martijn van der Vorm, *Callsign Nassau, Het moderne Korps Commandotroepen 1989-2012* (Amsterdam, Boom, 2012) 11-14.

8 Jelle Hooiveld heeft in het kader van zijn nog te verschijnen proefschrift over het BBO een uitvoerige schets van het ingezette personeel gemaakt. Voor de oprichting van het BBO zie ook Jelle Hooiveld, *Operatie Jedburgh. Geheime Geallieerde Missies in Nederland 1944-1945* (Amsterdam, Boom, 2014) 27-28.

De Amerikaanse Green Berets zijn wellicht het meest bekende voorbeeld hiervan. President John F. Kennedy sprak daar in 1962 over als 'forces which are too unconventional to be called conventional', bedoeld voor 'another type of war, new in its intensity, ancient in its origins'.[9] Dat laatste is een duidelijke verwijzing naar conflicten die een ander karakter hebben dan grootschalige oorlogvoering en verklaart waarom in het Amerikaanse militaire denken speciale operaties en irreguliere oorlogvoering tot op de dag van vandaag nauw met elkaar verbonden zijn. De onorthodoxe aard van de toenmalige speciale operaties bleek onder andere uit het feit dat psychologische oorlogvoering, inlichtingenvergaring en beïnvloeding van lokale partijen als inherent onderdeel van het optreden werden gezien.[10] Bovendien moesten de eenheden niet alleen tegen irreguliere tegenstanders kunnen optreden, maar zelf ook een guerrilla kunnen voeren tegen een communistische regering of bezettingsmacht. Dit alles onder de noemer Unconventional Warfare. Naast deze activiteiten werd het bestrijden van terrorisme een steeds belangrijkere taak van speciale eenheden. De ontwikkeling hiervan kwam in een stroomversnelling na het gijzelingsdrama tijdens de Olympische spelen in München van 1972.[11] Succesvolle voorbeelden zijn onder andere de Israëlische redding van het merendeel van de passagiers van een gekaapte Air France-vlucht uit het Oegandese Entebbe in 1976 en de ontzetting van de Iraanse ambassade in Londen door de Special Air Service (SAS) in 1980. In Nederland werden in deze periode de Bijzondere Bijstandseenheden (BBE'n) opgericht, met als bekendste wapenfeit de beëindiging van de Molukse treinkaping bij De Punt (1976).[12] De daarbij betrokken BBE-mariniers is overigens een van de voorgangers van onze huidige Maritime Special Operations Forces (MARSOF).

Een volgende stap in de ontwikkeling van westerse speciale operaties vindt zijn oorsprong in de nadagen van de Koude Oorlog. Speciale eenheden kregen in die tijd een definitieve plek in de structuur van veel krijgsmachten en groeiden uit tot een vaste waarde die wereldwijd op een veelzijdige manier kon worden ingezet. In de Verenigde Staten vormde de rampzalige mislukking van operatie Eagle Claw, de poging de gijzelaars uit de Amerikaanse ambassade in Teheran te bevrijden, in 1980 de directe aanleiding voor een reeks hervormingen. Dit leidde in 1987 tot de oprichting van het United States Special Operations Command (US SOCOM) dat voortaan de verantwoordelijkheid kreeg over de ontwikkeling en het inzetten van de speciale eenheden van verschillende krijgsmachtsdelen.[13] US SOCOM groeide al gauw uit tot een bepalende entiteit en gaf een boost aan het conceptuele denken. Speciale operaties moesten voortaan in het hele conflictspectrum een effectieve bijdrage kunnen leveren. Dat kwam goed van pas na de ineenstorting van de Sovjet-Unie en tijdens de oorlogen en vredesoperaties in de periode die daarop volgde. Ook in andere landen sloeg dit aan. Voor Nederland gold dat het KCT en de speciale troepen van het Korps Mariniers zich in de jaren 1990 en 2000 in rap tempo ontwikkelden als eenheden die snel, wereldwijd en met grote precisie konden worden ingezet om strategische effecten te bereiken.[14] De taakstelling die daarbij hoorde varieerde van Special Reconnaissance, het uitvoeren van complexe verkenningen, en Direct Action, het uitschakelen van hoogwaardige doelen, tot Military Assistance, het trainen van lokale bondgenoten. Niet geheel toevallig missies die traditioneel gezien het vaakst terugkomen en in deze periode

9 John F. Kennedy, *Remarks at West Point to the Graduating Class of the U.S. Military Academy*, June 6th 1962. Zie: https://www.presidency.ucsb.edu/documents/remarks-west-point-the-graduating-class-the-us-military-academy.

10 Zie onder meer Alfred H. Paddock, Jr., *U.S. Army Special Warfare, Its Origins* (Lawrence, University Press of Kansas, 2002) 113-139; Sam C. Sarkesian, 'The American Response to Low-Intensity Conflict', in David A. Charters en Maurice Tugwell (red.), *Armies in Low-Intensity Conflict, A Comparative Analysis* (Londen, Brassey's, 1989) 34-39; Hy S. Rothstein, *Afghanistan & The Troubled Future of Unconventional Warfare* (Annapolis, Naval Institute Press, 2006) 36-38.

11 Ansbacher en Schleifer, 'The three ages of modern Western special operations forces', 37.

12 Zie bijvoorbeeld Christiaan van der Spek, *Een Wapen tegen Terreur. De Geschiedenis van de Bijzondere Bijstandseenheid Krijgsmacht, 1972-2006* (Amsterdam, Boom, 2009); Olof van Joolen en Silvan Schoonhoven, *Liggen blijven! Achter de schermen bij de mariniers van De Punt en de terreuracties van 1973-1978* (Amsterdam, Nieuw Amsterdam, 2018).

13 US SOCOM, *US SOCOM History 20 Years 1987-2007* (Tampa, US SOCOM, 2007) 12. Zie: https://irp.fas.org/agency/dod/socom/2007history.pdf.

14 Ten Cate en Van der Vorm, *Callsign Nassau,* 324. Zie ook G.R. Dimitiru, G.P. Tuinman en M. van der Vorm, 'Operationele Ontwikkeling van de Nederlandse *Special Forces*, 2005-2010', *Militaire Spectator* 181 (2012) (3) 107-110.

Special Reconnaissance was een van de taakstellingen voor speciale troepen na het einde van de Koude Oorlog FOTO MCD, LOUIS MEULSTEE

ook doctrinair werden vastgelegd als de kerntaken van westerse special operations forces.[15]

Intussen zorgde de Global War on Terror er vanaf 2001 voor dat speciale eenheden een steeds grotere rol kregen in moderne oorlogvoering. De focus kwam echter meer en meer te liggen op het uitschakelen van belangrijke terroristenleiders. In tegenstelling tot langdurig onconventioneel optreden te midden van complexe lokale samenlevingen in Irak, Afghanistan of Syrië brachten acties gericht op het vijandelijke leiderschap en hun netwerk direct tastbare resultaten. In de ogen van veel politici, beleidsmakers en het grotere publiek zijn contraterrorisme-operaties als Neptune Spear, de uitschakeling van Osama Bin Laden,

15 Simon Anglim, 'Special Forces – Strategic Asset', *Infinity Journal* 1 (2011) (2) 17; Marsh, Kiras en Blocksome, *Special Operations, Out of the Shadows*, 2-3; Rob de Wijk, Frank Bekkers, Tim Sweijs, Stephan de Spiegeleire en Dorith Kool, *The Future of NLD SOF: Towards an All-Domain Force* (Den Haag, HCSS, 2021) 28.

dan ook hét voorbeeld van een speciale operatie.[16] Daarbij vergeet men dat zulke acties op de lange termijn alleen succesvol zijn als ze worden ondersteund door activiteiten gericht op verzoening en het verhogen van de veiligheid van de lokale bevolking.[17]

Dit brengt ons terug bij het populaire beeld. De geschiedenis van speciale operaties leert dat ze in allerlei vormen en soorten bestaan. Toch is de eenzijdige kijk die ons doorgaans wordt voorgeschoteld hardnekkig geworteld in de publieke perceptie van dit soort operaties. Als erfenis van meer dan 20 jaar strijd tegen terreur worden speciale eenheden vooral gezien als 'door kickers' die heel precies terroristenleiders en andere hoogwaardige doelen kunnen uitschakelen. En dat terwijl de huidige internationale veiligheidssituatie vraagt om veelzijdigheid. De speciale operaties-gemeenschap zelf onderkent dat het juist nu belangrijk is het veelzijdige karakter van speciale operaties te behouden en dat eenheden en operators zich blijven ontwikkelen om huidige en toekomstige uitdagingen het hoofd te bieden. Sommigen spreken daarbij zelfs van een nieuw tijdperk in de ontwikkeling van het westerse speciale optreden.[18] Om dit beter te kunnen begrijpen is het nodig in te gaan op de conceptuele benadering van dit soort operaties en de eenheden die erbij betrokken zijn.

Special operations (forces): een conceptuele verkenning

De meeste definities van speciale operaties kunnen worden gezien als pogingen het veelzijdige karakter hiervan onder één noemer te brengen. Funs Titulaer, Willem Emke en Martijn Rouvroije analyseren in *Special Operations Forces Explained: Redux* zowel militaire als academische definities.[19] Ze komen tot de conclusie dat de belangrijkste doctrines, die van respectievelijk de NAVO en de Verenigde Staten, vier overlappende aspecten behandelen.[20] Als eerste worden speciale operaties uitgevoerd door speciaal daarvoor geselecteerde, opgeleide, uitgeruste en georganiseerde eenheden die op onconventionele wijze hun doel weten te bereiken. Een tweede aspect betreft het feit dat speciale operaties wanneer nodig onder geheimhouding kunnen worden uitgevoerd. Als derde is er de notie dat dit soort operaties vaak een hogere mate van politiek, diplomatiek of militair risico met zich meebrengt. Tot slot benadrukken deze definities dat speciale operaties bedoeld zijn om strategische of operationele effecten te bereiken. Aan de academische kant valt op dat de meeste definities zich niet zozeer richten op het beschrijven van de karakteristieken van speciale operaties, maar op de meerwaarde van deze operaties in relatie tot conventionele operaties.[21] Dat nodigt uit hier verder op in te gaan.

Er zijn verschillende theorieën die de verhouding tussen special operations forces en reguliere eenheden beschouwen. Door de bank genomen gaat het daarbij om de manier waarop speciale operaties complementair zijn aan conventionele operaties en strijdkrachten. Tom Searle beschrijft in zijn invloedrijke theorie speciale operaties als 'operations outside the conventional operations box'.[22] In de praktijk kan slechts een deel van alle taken en ver-

16 Dit komt erop neer dat speciale operaties vooral als *Direct Action* worden gezien. Een beeld dat overigens niet alleen in populaire cultuur en de media wordt uitgedragen, maar vaak ook in wervingscampagnes van speciale eenheden zelf. Funs Titulaer en Martijn Kitzen, 'The Population-Centric Turn in Special Operations: A Possible Way Ahead for SOF Informed by a Cross-Disciplinary Analysis of State-Building Interventions', *Special Operations Journal* 6 (2020) (1) 47-50. Zie ook Jack Watling, 'Sharpening the Dagger, Optimising Special Forces for Future Conflict', *Whitehall Report* 1-21 (2021) 2-3. Voor de planning en uitvoering van de uitschakeling van Bin Laden zie, onder andere, Mark Bowden, *The Finish. The Killing of Osama Bin Laden* (Londen, Grove Press, 2012).

17 Zie ook David Kilcullen, 'Counterinsurgency: The State of a Controversial Art', in Paul B. Rich en Isabelle Duyvesteyn (red.), *The Routledge Handbook of Insurgency and Counterinsurgency* (Abingdon, Routledge, 2012) 141-143.

18 Irwin en Wilson, *The Fourth Age of SOF*.

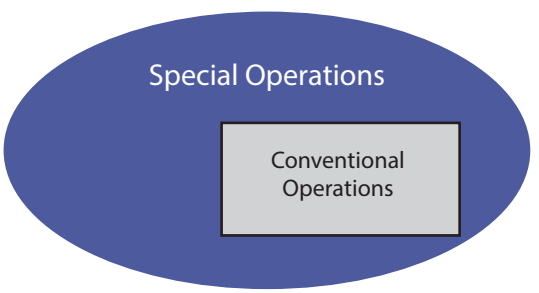
19 Funs Titulaer, Willem Emke en Martijn Rouvroije, *Special Operations (Forces) Explained: Redux. On the nature of Western special operations and the forces that conduct them* (Breda, NLDA, 2023) 14-17. Dit is een verdere uitwerking van Funs Titulaer, 'Special Operations (Forces) Explained. On the nature of Western special operations and the forces that conduct them' *Militaire Spectator* 190 (2021) (2) 84-99.

20 Het gaat hier om NATO, *Allied Joint Doctrine for Special Operations AJP-3.5 (B Version1)* (Brussel, NATO, 2019) en U.S. Department of Defense, *Joint Publication 3-05: Special Operations* (Washington, DoD, 2014).

21 Zie bijvoorbeeld Arquilla, *From Troy to Entebbe*, xv-xvi; Colin S. Gray, *Explorations in Strategy* (Westport, Praeger, 1998) 149-150; Anglim, 'Special Forces – Strategic Asset', 16. Robert G. Spulak, Jr., 'A Theory of Special Operations: The Origins, Qualities and Use of SOF', *JSOU Report 07-7* (2007) 1, 21.

22 Tom Searle, 'Outside the Box: A New General Theory of Special Operations', *JSOU Report 17-4* (2017) 14.

antwoordelijkheden van het militaire apparaat (de ellips in Figuur 1), worden vervuld door conventionele strijdkrachten. Het niet door de conventionele *box* bestreken gebied vormt de kloof in militaire capaciteit – ook vaak *the void* genoemd – die door speciale operaties moet worden afgedekt. Hierbij geldt dat zowel de ellips als de conventionele box groter of kleiner kan worden. Dat hangt samen met veranderingen in de veiligheidssituatie en met wat de politiek van haar strijdkrachten verlangt. Speciale Operaties zijn in deze opvatting dus een functie van de politiek-strategische context en zullen continu moeten innoveren om hierop te kunnen inspelen.[23]



Figuur 1 Speciale operaties volgens Searles 'Outside the Box'[24]

Colin Gray beschrijft in *Explorations in Strategy* waarom speciale operaties zo geschikt zijn deze kloof in militaire capaciteit op te vullen. Hij doet dat aan de hand van twee 'master claims', namelijk 'economy of force' en 'expansion of choice'.[25] Het laatste slaat op het feit dat speciale operaties politieke en militaire leiders meer opties geven als het aankomt op de inzet van het militaire middel. Een capaciteit voor speciale operaties staat garant voor flexibiliteit, minimaal geweldsgebruik en precisie. Dat wordt grotendeels mogelijk gemaakt door de eerste master claim, economy of force, die erop neerkomt dat speciale operaties significante resultaten kunnen bereiken met beperkte middelen. Daar zijn meerdere redenen voor te noemen, maar hier wil ik vooral ingaan op de aard van special operations forces. Volgens Robert Spulak onderscheiden deze eenheden en hun personeel zich door hun vermogen met Clausewitziaanse frictie om te gaan. Met andere woorden, ze zijn in staat risico te mitigeren en zelfs zeer moeilijke missies tot een goed einde te brengen.[26] Dat is een rechtstreeks gevolg van de manier waarop deze elitesoldaten onder zware fysieke en mentale druk geselecteerd en opgeleid worden, de flexibiliteit die wordt geboden door kleine groepen van breed inzetbare individuen en de mogelijkheid creatief op te treden omdat ze in tegenstelling tot reguliere eenheden minder zijn gebonden aan starre doctrinaire en operationele raamwerken en daardoor op een onorthodoxe manier kunnen opereren.[27] Speciale eenheden onderscheiden zich dus zowel in de fysieke en mentale als conceptuele component.[28]

Als laatste is het van belang hier nog wat uitleg te geven over de van oorsprong Amerikaanse term special operations forces, die ik tot nog toe als synoniem met speciale eenheden heb gebruikt. Het is echter van belang te benadrukken dat special operations forces niet alleen slaat op de operators zelf, maar ook op ander personeel dat bij operaties betrokken is. In de Verenigde Staten worden bijvoorbeeld de ondersteunende squadrons van de luchtmacht – net als in Nederland overigens – en de speciale helikoptercapaciteit van de landmacht hiertoe gerekend, evenals eenheden voor psychologische oorlogvoering en civiel-militaire samenwerking.[29] Speciale operaties draaien weliswaar om een harde kern van operators, maar ze zijn daarbij afhankelijk van ondersteunende eenheden die ervoor zorgen dat zij hun missie kunnen vervullen.

23 Ook Richard Rubright benadrukt het belang van een grondige analyse van de huidige en toekomstige context als basis voor het vaststellen van het precieze werkgebied van speciale operaties. Richard W. Rubright, 'A Unified Theory for Special Operations', *JSOU Report 17-1* (2017) 39-40.

24 Rubright, 'A Unified Theory for Special Operations', 18.

25 Gray, *Explorations in Strategy*, 168-174.

26 Zie ook Jonathan Schroden, 'Why Special Operations? A Risk Based Theory', *CNA Occasional Paper* (Arlington, CNA, 2020).

27 Spulak, 'A Theory of Special Operations', 19-21.

28 Zie ook James D. Kiras, *Special Operations and Strategy, From World War II to the War on Terrorism* (Abingdon, Routledge, 2006), 6-7. Voor het belang van training, groepscohesie en leiderschap zie William H. McRaven, *Spec Ops. Case Studies in Special Operations Warfare: Theory and Practice* (Novato, Presidio Press, 1995) 390-391.

29 Linda Robinson, *Masters of Chaos. The Secret History of the Special Forces* (New York, Public Affairs, 2004) XII-XIII. Zie ook Bas Brust, 'The Roles and Utility of Small States' Special Operations Forces in the Great Power Competition; From Theory to Tangible Advice', *Thesis Master Military Strategic Studies* (Breda, NLDA, 2022) 32-33.

Turbulente tijden: het 21e-eeuwse internationale veiligheidslandschap

Zoals in de inleiding gezegd leven we in turbulente tijden waarin we te maken hebben met een groot aantal verschillende dreigingen.

De oorlog in Oekraïne is het meest zichtbaar, maar ook op andere plekken zorgt de toenemende competitie tussen grootmachten, de groeiende rol van sterke regionale spelers en de opkomst van geavanceerde gewelddadige niet-statelijke actoren voor instabiliteit. David Kilcullen spreekt in deze context ook wel over 'draken en slangen' die steeds meer op elkaar gaan lijken.[30] Hij bedoelt daarmee dat landen als Rusland, China, Noord-Korea en Iran – de

30 David Kilcullen, *The Dragons and the Snakes. How the Rest Learned to Fight the West* (Londen, Hurst, 2020).

draken – naast de dreiging met conventionele of nucleaire middelen tegenwoordig veelvuldig gebruik maken van onorthodoxe methodes om invloed te winnen en hun eigenbelang veilig te stellen. Dat hebben ze afgekeken van de slangen: niet-statelijke groeperingen als al-Qaida, Hezbollah of Islamitische Staat die de afgelopen twintig jaar hebben geleerd hoe je (gedeeltelijk) overeind kunt blijven in een oorlog tegen het Westen. Op hun beurt is het de slangen gelukt hun geweldscapaciteit uit te breiden en ze deinzen er zelfs niet meer voor terug om op dezelfde manier als reguliere legers op te treden als dat kan. Dit alles betekent dat we niet alleen onze conventionele afschrikking op orde moeten hebben, maar ook irreguliere dreigingen moeten kunnen afstoppen.

Als we naar de huidige trends kijken dan is het de verwachting dat deze ontwikkeling zich

Speciale operaties draaien om een harde kern van operators, maar ze zijn daarbij afhankelijk van ondersteunende eenheden, zoals helikoptercapaciteit

FOTO MCD, JAN DIJKSTRA

Speciale operaties vormen door hun 'economy of force' een relatief goedkoop instrument

verder doorzet.[31] Wapens en andere middelen voor oorlogvoering zijn steeds breder beschikbaar. De vergaande verbondenheid van de moderne wereld zorgt er niet alleen voor dat we beter kunnen samenwerken, maar maakt ons ook kwetsbaar voor partijen die onze fysieke en virtuele netwerken willen misbruiken of treffen. En dan tekenen zich ook nog eens de contouren af van een technologische revolutie waarbij de eerste signalen er al op wijzen dat kunstmatige intelligentie een grote impact zal hebben op oorlogvoering.

Deze drie ontwikkelingen zorgen ervoor dat staten en gewelddadige niet-statelijke spelers in rap tempo meer capaciteiten krijgen om zowel op een conventionele als irreguliere manier druk uit te oefenen.[32] Dit wordt nog eens extra gecompliceerd door een vervaging van de klassieke tijd- en ruimtegrenzen. Conflicten beperken zich zelden nog tot één gebied, maar hebben vaak een veel verdere impact. Dat uit zich niet alleen in fysieke acties, maar ook via middelen als communicatiesatellieten en het internet. Het is dan ook niet meer dan logisch dat cyber en space tegenwoordig als domeinen van militair optreden worden gezien. Zelfs onze eigen samenlevingen zijn het toneel van een voortdurende sociaal-politieke informatiestrijd waarin externe partijen binnen onze landsgrenzen proberen invloed uit te oefenen.[33] Deze methode wordt door autoritaire rivalen als China en Rusland ook succesvol gebruikt om in niet-westerse landen het wantrouwen jegens het Westen verder aan te wakkeren met als gevolg een verlies van westerse invloed.[34] Dat heeft potentieel grote gevolgen in regio's in Afrika en het Midden-Oosten waar vergaande destabilisering al dan niet indirect effect op Europa gaat hebben, of die we nog hard nodig zullen hebben om te voorzien in onze vraag naar grondstoffen. Zulke beïnvloedingscampagnes illustreren dat er continu sprake is van acties die erop gericht zijn onze belangen te schaden. Dat maakt het moeilijk te bepalen wanneer een conflict precies begint of eindigt. In de huidige competitie is het niet altijd even duidelijk wanneer een potentieel escalerende actie is ingezet. Dat geldt zeker als die zich afspeelt onder de drempel van wat wij als oorlog beschouwen en het schimmig is wie er precies achter zit. We zullen dan ook klaar moeten zijn om hybride of ambigue activiteiten in dit grijze gebied (de *grey zone*) tussen oorlog en vrede te detecteren, attribueren en indien nodig af te stoppen.

Een nieuw perspectief op de inzet van special operations forces

Wat is nu de rol van special operations forces in het moderne veiligheidslandschap? Een antwoord hierop begint bij het vaststellen waar precies de kloof, the void, ligt tussen de capaciteit van reguliere eenheden en de verantwoordelijkheden en taken van de krijgsmacht als geheel. Aangezien dit niet alleen afhankelijk is van de veiligheidssituatie, maar ook van nationale politiek, is dit voor ieder land anders.

31 Voor de hierna beschreven trends zie Rob Johnson, Martijn Kitzen en Tim Sweijs, *The Conduct of War in the 21st Century, Kinetic, Connected and Synthetic* (Abingdon, Routledge, 2021) 295-302.

32 Dat uit zich niet alleen in traditionele en irreguliere oorlogvoering, maar ook in het tweezijdige karakter van moderne strategische competitie waarbij enerzijds sprak is van conventionele afschrikking, anderzijds van irreguliere acties. Zie Eric Robinson, 'The Missing, Irregular Half of Great Power Competition', *Modern War Institute*, 8 September 2020: https://mwi.usma.edu/the-missing-irregular-half-of-great-power-competition/.

33 Jahara Matisek en Buddhika Jayamaha, *Old & New Battlespaces. Society, Military Power, and War* (Boulder, Lynne Rienner, 2022) 136-137.

34 Jonathan Holslag, *Van muur tot muur. De wereldpolitiek sinds 1989* (Amsterdam, De Bezige Bij, 2022) 380-381. Over Chinese en Russische beïnvloedingsoperaties zie ook Mick Ryan, *War Transformed. The Future of Twenty-First-Century Great Power Competition and Conflict* (Annapolis, Naval Institute Press, 2022) 108-112.

Toch is er een algemene trend waarneembaar. Op dit moment richten westerse krijgsmachten zich namelijk weer massaal op hun originele hoofdtaak, conventionele afschrikking. De box wordt daarmee een stuk kleiner, want de afgelopen twintig jaar waren reguliere eenheden – althans op papier – naast deze taak ook bezig met expeditionaire counterinsurgency- en stabilisatieoperaties.[35] Tegelijkertijd zijn er met de intensivering van strategische competitie en het voortduren van de strijd tegen terroristische organisaties en andere gewelddadige niet-statelijke groeperingen ook meer taken bijgekomen voor het militaire apparaat. Dat betekent dus dat the void groter is geworden door enerzijds een krimpend takenpakket van reguliere eenheden en anderzijds een uitbreiding van de militaire verantwoordelijkheid in haar geheel. Kolonel der mariniers Bas Brust heeft de gevolgen hiervan voor westerse special operations forces in kaart gebracht.[36] Hij concludeert dat speciale eenheden in de huidige context in totaal zo'n 25 (inter)nationale en binnenlandse rollen kunnen vervullen en 19 verschillende strategische effecten kunnen bereiken. Het gaat te ver hier op al deze punten in te gaan, maar opvallend is dat het zwaartepunt ligt in het irreguliere deel van competitie en oorlogvoering.[37] Ook andere rapporten wijzen op een heel spectrum aan taken waarbij het belangrijk is te blijven innoveren om bijvoorbeeld in samenwerking met cyber- en space-middelen in meerdere domeinen effecten te bereiken.[38]

Onze turbulente tijden vragen dus om special operations forces met een veelzijdig karakter. Voor kleine landen als Nederland en België komt dit erop neer dat weloverwogen keuzes gemaakt moeten worden om met beperkte middelen een gebalanceerde capaciteit te genereren.[39] Dat vraagt om heldere politiek-militaire besluitvorming en een einde aan de 'strategische vaagheid' die de afgelopen decennia heeft gekenmerkt.[40] Het helpt daarbij niet dat er nog steeds een eenzijdig beeld bestaat van speciale operaties waarbij de focus op dit moment ligt op conventionele afschrikking en oorlogvoering. Waar zo'n prioritering mij voor reguliere eenheden overigens niet meer dan terecht lijkt, is dit voor speciale eenheden anders omdat zij vooral het verschil kunnen maken als het gaat om de irreguliere aspecten van moderne competitie, crises en conflicten.[41]

Onderzoek door Ricky van der Pas biedt een welkom inzicht in de koers die een klein land kan varen als het aankomt op de ontwikkeling en inzet van hedendaagse special operations forces.[42] Het draait daarbij om het verkrijgen van veiligheidsgaranties van bondgenoten door relevante bijdrages die niet alleen een militair probleem oplossen, maar tegelijkertijd ook gewicht geven aan het eigen politieke standpunt. Speciale operaties vormen door hun 'economy of force' een relatief goedkoop en betrouwbaar instrument voor dit doeleinde.[43] Bovendien genieten special operations forces prestige en dat maakt het voor kleine landen aantrekkelijk om

35 Uitzondering hierop is Security Force Assistance, het trainen en steunen van lokale bondgenoten, dat eerder vooral als onderdeel van Military Assistance door speciale eenheden gebeurde. Op dit moment trainen Nederlandse conventionele eenheden bijvoorbeeld Oekraïense militairen. Zie, onder andere, Ivor Wiltenburg en Martijn Kitzen, 'What's in a Name? Clarifying the Divide between Military Assistance and Security Force Assistance', *Small Wars Journal*, 9 November 2020: https://smallwarsjournal.com/jrnl/art/whats-name-clarifying-divide-between-military-assistance-and-security-force-assistance.

36 Brust, 'The Roles and Utility of Small States' Special Operations Forces in the Great Power Competition', 45-47, 55-56. Brust maakt onderscheid tussen internationale rollen voor de NAVO, VN of EU, rollen in het nationaal belang tijdens internationale operaties en binnenlandse rollen.

37 Daarbij geldt ook dat de meeste van deze rollen en effecten nauw verwant zijn met diplomatieke acties en dat er hierin een zekere wisselwerking tussen speciale operaties en diplomatie bestaat. Ibidem, 42-44.

38 Zie, onder andere, Joost Tuinman en Matthias Schwarzbauer, 'The Strategic Utility of SOF in Great Power Competition: A NATO Perspective', *Master Thesis Defense Analysis* (Monterey, NPS, 2022); De Wijk, Bekkers, Sweijs, De Spiegeleire en Kool, *The Future of NLD SOF*; Watling, 'Sharpening the Dagger'.

39 Zie ook Ulrica Pettersson, Gunilla Eriksson en Urban Molin, 'Conclusion', in Gunilla Eriksson en Ulrica Pettersson (red.), *Special Operations from a Small State Perspective. Future Security Challenges* (Cham, Palgrave Macmillan, 2017) 180-181.

40 M.W.M. Kitzen en F.H. Thönissen, 'Strategische vaagheid, Hoe het gebrek aan strategische visie het lerend vermogen van de Koninklijke Landmacht beperkt', *Militaire Spectator* 187 (2018) (4) 206-223.

41 Voor de situatie in Nederland zie Brust, 'The Roles and Utility of Small States' Special Operations Forces in the Great Power Competition', 55.

42 Ricky van der Pas, 'Status, Smallness, and Special Forces. A theoretical introduction to the defence policies of small states', *Thesis Master Military Strategic Studies* (Breda, NLDA, 2022) 43-45.

43 Naast 'economy of force' bieden speciale operaties ook in kleine landen 'expansion of choice'. Colin Gray noemt ter aanvulling van deze 'master claims' ook nog 7 andere claims, waarbij voor kleine landen vooral geldt dat special operations forces innovatie aanjagen en competentie demonstreren. Voor een overzicht van de claims zie Gray, *Explorations in Strategy*, 168-185.

via dit middel hun internationale status en invloed te vergroten. Wat Nederland betreft hebben we dit gezien bij inzet van speciale eenheden in onder meer Afghanistan, Irak en Mali.

Met de oprichting van het Nederlandse Special Operations Command (NLD SOCOM) in 2018 heeft het denken over speciale operaties als strategisch instrument van ons buitenlands beleid een nieuwe impuls gekregen. Dat is onder ander terug te zien in het visiedocument *Netherlands Special Operations Forces 2035* dat stelt dat onze special operations forces een strategische niche vullen door hun vermogen met precisie te opereren in extreem gevaarlijke situaties met een hoog politiek of militair risico waarin grootschalige aanwezigheid ongewenst of onmogelijk is.[44] Hierbij is nadrukkelijk aandacht voor de rol van speciale eenheden als middel om Nederland te positioneren als sterke en betrouwbare partner binnen internationale allianties en netwerken, in het bijzonder het zogeheten 'global SOF network'.[45] Om relevant te blijven is het van belang het eigen SOF-systeem en de mensen die daarin centraal staan voortdurend te ontwikkelen en deze binnen de Nederlandse krijgsmacht als aanjagers van innovatie te laten fungeren.[46] Dit stelt onze special operations forces in staat een veelzijdig karakter te behouden waarmee veel verschillende rollen binnen het hele conflictspectrum kunnen worden vervuld.

Het gaat dan niet alleen om traditionele taken en doorontwikkelingen daarvan, maar ook om nieuwe rollen die ons in staat stellen de acties van tegenspelers in het grijze gebied tussen oorlog en vrede beter te doorzien. Dat kan bijvoorbeeld door zogenaamde afgeschermde operaties in samenwerking met de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en eventueel het Defensie Cybercommando.[47] Ook Early Forward Presence (EFP) in een potentieel conflictgebied biedt mogelijkheden meer grip te krijgen op complexe veiligheidsdynamieken waarbij deze rol bij uitstek geschikt is om Nederland internationaal onderscheidend te positioneren. Verder blijft het belangrijk hoogwaardige doelen uit te kunnen schakelen en is er ook veel vraag naar Unconventional Warfare zoals het trainen en organiseren van verzetsgroepen in de Baltische Staten.[48] Onze Nederlandse special operations forces kunnen zo niet alleen bijdragen aan afschrikking in Europa, maar bovenal ook aan het detecteren en tegengaan van beïnvloeding en instabiliteit in kwetsbare gebieden om ons heen. Gezien de huidige focus op het indammen van Moskous agressie is het niet meer dan logisch na te denken over de rol van onze speciale eenheden bij het tegengaan en afschrikken van Russische activiteiten – al dan niet via organisaties als Wagner – in fragiele staten aan de buitenranden van Europa.

Onderzoek en onderwijs sectie Irreguliere Oorlogvoering & Speciale Operaties

In zijn oratie 'Oorlog en het Schild van Athena. De waarde van Krijgswetenschappen' schetst Frans Osinga drie wetenschappelijke functies van het vakgebied, namelijk het verduidelijken

Uitreiking gevechtsinsigne aan mariniers van de Special Operations Land Task Group in Mali

44 NLD SOCOM, *Netherlands Special Operations Forces 2035. Any time, any place – a strategic course of action for special operations* (Den Haag, Ministerie van Defensie, 2022) 13-14.

45 NLD SOCOM, *Netherlands Special Operations Forces 2035*, 40-43.

46 Ibidem, 35-38, 45-48.

47 Special operations forces hebben als onderdeel van Special Reconnaissance altijd al inlichtingenvergaring als rol gehad. Gedurende de Global War on Terror heeft deze rol zich verder ontwikkeld en in de huidige multi-domeinomgeving zijn er nog meer mogelijkheden. Voor ontwikkeling tijdens de Global War on Terror zie bijvoorbeeld John Hardy, 'Hunters and Gatherers: The Evolution of Strike and Intelligence Functions in Special Operations Forces', *International Journal of Intelligence and CounterIntelligence* 36 (2023) (4) 1-21. Voor de specifieke rol in kleine landen zie Ben Haspels en Flemming Haar, 'The Strategic Utility of Small-State Special Operations Forces (SOF) as Information Collectors Supporting National Decision-Making', *Master Thesis Defense Analysis* (Monterey, NPS, 2018).

48 Zie bijvoorbeeld Otto Fiala en Ulrica Pettersson, 'ROC(K) Solid Preparedness. Resistance Operations Concept in the Shadow of Russia', *PRISM* 8 (2020) (4) 17-28. Voor het Nederlandse perspectief op Unconventional Warfare zie Nico Zoontjens, 'A Study on the Feasibility of Netherlands Special Operations Forces Conducting Unconventional Warfare', *Master Thesis Defense Analysis* (Monterey, NPS, 2022).

van de aard van hedendaagse oorlog(voering), het verklaren van de logica en het succes van militair geweld, en theorievorming en toetsing.[49] De verkregen kennis kan onder andere direct worden ingezet voor de gebruikers – militairen, besluitvormers en beleidsmakers – die bij de inzet van krijgsmacht betrokken zijn. Dat kan middels onderwijs, maar ook door valorisatie in de vorm van advies, kennisborging of andere activiteiten. Luitenant-kolonels Joost Tuinman en Matthias Schwarzbauer wijzen in een recent onderzoek bijvoorbeeld op de meerwaarde van een academisch perspectief bij het nadenken over toekomstige effecten, strategieën en concepten voor speciale operaties.[50]

Sinds haar oprichting is de sectie Irreguliere Oorlogvoering & Speciale Operaties op alle hiervoor genoemde terreinen actief. Daarbij ligt de focus op zowel speciale operaties als irreguliere oorlogvoering met als doel op deze twee onderwerpen zo breed mogelijk en op een multidisciplinaire manier kennis op te bouwen voor de Nederlandse en Belgische krijgsmachten en in het bijzonder de respectievelijk SOCOM's. Dat gebeurt onder andere op basis van de in dit artikel verwerkte ideeën, theorieën, concepten en inzichten. Samen met de Amerikaanse hoogleraar James Kiras wordt er op dit moment gewerkt aan een nieuw boek, *Into the Void*. Dat analyseert – inderdaad – hoe special operations forces om kunnen gaan met de huidige kloof in militair optreden, welke uitdagingen daarbij

49 Frans Osinga, 'Oorlog en het Schild van Athena. De Waarde van Krijgswetenschappen', Oratie (Leiden, Universiteit Leiden, 2019). 44-46.

50 Tuinman en Schwarzbauer, 'The Strategic Utility of SOF in Great Power Competition', 165.

FOTO MCD: SJOERD HILCKMANN

Buluitreiking op de NLDA. De sectie Irreguliere Oorlogvoering & Speciale Operaties is inmiddels met verschillende vakken actief in nagenoeg alle opleidingen van de NLDA

FOTO MCD, LOUIS MEULSTEE

komen kijken en welke vormen van optreden het meest succesvol zijn in de hedendaagse veiligheidssituatie.

Het gros van het onderzoek binnen de sectie wordt echter verricht door promovendi vanuit het aio-programma van het Commando Landstrijdkrachten. Recentelijk promoveerde majoor Martijn van der Vorm op een proefschrift waarin het lerend vermogen van de krijgsmacht tijdens en na operaties werd geanalyseerd.[51] Luitenant-kolonel Ivor Wiltenburg zal postuum promoveren op Security Force Assistance, een taak waarin veel overlap bestaat tussen speciale en conventionele eenheden. Met behulp van onderzoeksassistent Vibeke Gootzen is dit onderzoeksthema overigens verder opgepakt om de huidige ervaringen met het trainen van Oekraïense militairen te analyseren. Majoor Marnix Provoost houdt zich bezig met complexe insurgencies zoals we die op dit moment zien in bijvoorbeeld de Sahel, maar is inmiddels ook uitgegroeid tot een veelgevraagd expert over Russische strategische cultuur en oorlogvoering.

51 Martijn van der Vorm, 'The Crucible of War: Dutch and British military learning processes in and beyond Southern Afghanistan', proefschrift (Leiden, Universiteit Leiden, 2023).

Luitenant-kolonel Gijs Tuinman verdiept zich in de complexiteit van oorlog en de manier waarop krijgsmachten daarmee omgaan. En tot slot onderzoekt majoor Peter Schrijver hoe Oekraïne in de strijd tegen Rusland succesvol gebruik weet te maken van informatiemanoeuvre. Daarnaast zijn er ook nog enkele buitenpromovendi actief, zoals Aiden Hoyle, die Russische desinformatie onder de loep neemt, en luitenant-kolonel Rick Breekveldt, die onderzoek doet naar beïnvloeding als onderdeel van speciale operaties. Maarten Broekhof – zelf diplomaat – analyseert de rol van buitenlandse zaken in militaire operaties en Jelle Hooiveld bestudeert het eerdergenoemde Bureau Bijzondere Opdrachten tijdens de Tweede Wereldoorlog als vroege vorm van Unconventional Warfare.

Het toegankelijk maken van deze kennis gebeurt middels valorisatie, waarbij Martijn Rouvroije en kapitein-commandant Jan Weuts een sleutelrol spelen. Zij overbruggen de kloof, onze eigen void, tussen de academie en de praktijk van respectievelijk Nederlandse en Belgische special operations forces. Daarnaast onderzoeken beiden de strategische en theoretische context van speciale operaties. Voor onderwijs geldt dat de sectie inmiddels met verschillende vakken actief is in nagenoeg alle opleidingen van de NLDA, waarbij binnen de Master Military Strategic Studies ook samen met studenten onderzoek wordt gedaan. De in dit artikel genoemde studies van kolonel der mariniers Bas Brust en Ricky van der Pas zijn voorbeelden hiervan. Binnenkort verschijnt er ook nog een monoloog bij de Amerikaanse Joint Special Operations University waarin kapitein Tijs Althuizen en de schrijver van dit artikel de ontwikkeling van de gecombineerde inzet van speciale eenheden, lokale bondgenoten en het luchtwapen analyseren. Als laatste zijn er speciale themadagen en de cursus Strategic Awareness for SOF Operators waarin Nederlands en Belgisch personeel gezamenlijk wordt meegenomen in de strategische context van speciale operaties. Daarbij wordt ook gebruik gemaakt van de inzichten van de Belgische soldiers-scholars kapitein Pieter Balcaen en korporaal Pierre Jean Dehaene. Inmiddels zijn er verschillende iteraties geweest en is er interesse vanuit onder andere Denemarken en Zweden.

Het global SOF network is academisch stevig geworteld

Dat laatste is een mooie illustratie van het feit dat het vakgebied internationaal steeds meer belangstelling krijgt en dat de sectie binnen de gemeenschap bekendheid geniet. Daarbij moet ook vermeld worden dat er een solide samenwerking bestaat met het Irregular Warfare Initiative (gesponsord door West Point en Princeton) en met diverse buitenlandse masterprogramma's in irreguliere oorlogvoering. In die laatste categorie valt bijvoorbeeld de band met de Amerikaanse Naval Postgraduate School (NPS), waar luitenant-kolonel Ben Gans op dit moment doceert en onderzoek doet naar multi-domeinaspecten van speciale operaties. Verder bereidt majoor Erik Ringenier zich binnen de sectie voor op zijn plaatsing in Amerika waar hij onder andere de Joint Special Operations Master of Arts aan de National Defense University zal volgen. Zo blijkt dat het global SOF network ook academisch stevig geworteld is en dat het onderwijs en onderzoek van de sectie Irreguliere Oorlogvoering & Speciale Operaties van de Faculteit Militaire Wetenschappen daar een vast deel van uitmaakt. ■

PHOTO MCD, GERBEN VAN ES

Conceptual manoeuvring

The interpretation of Information Manoeuvre within the Netherlands Ministry of Defence

Marije Timmer and Paul Ducheine*

To capture and adapt to the resulting changes in the operational environment, the concept of Information Manoeuvre was introduced in the Royal Netherlands Army

Concepts such as Information Warfare, Information Operations, Influence Operations, Intelligence, and Cyberspace and Electromagnetic Activities, to mention but a few, compete with Information Manoeuvre for prominence and together cloud the conceptual field. As a result, Information Manoeuvre is at risk of being shrouded in ambiguity. Divergence of interpretations and misunderstandings could hamper successful implementation of the concept and trigger intra-organizational disputes about responsibilities. Therefore, there is a need to provide clarity on the conceptual foundations of Information Manoeuvre and the manner in which it is interpreted within the Netherlands Ministry of Defence.

Throughout human history, from Sun Tzu, via Alexander the Great, to the current war in Ukraine, information has played a prominent role in the conduct of war. Nevertheless, while the use of information is nothing new to armed conflict, the process of 'informatisation' has in recent decades had a major impact on our societies, and by extension, on modern warfare.[1] To capture and adapt to the resulting changes in the operational environment, the concept of Information Manoeuvre was introduced in the Royal Netherlands Army. The concept quickly rose to prominence, leading to the establishment of the Land Information Manoeuvre Centre (LIMC), the founding of the Information Manoeuvre Arm,[2] and the adoption of the concept as a new vision of the conduct of future military operations.[3]

Notwithstanding its popularity, the term Information Manoeuvre is not universally acknowledged. In fact, it has only been adopted by the armies of the United Kingdom and the Netherlands. In academic circles it is a similarly uncommon term. Yet, a plethora of terms exists to describe similar or overlapping notions and approaches. Concepts such as Information Warfare, Information Operations, Influence Operations, Intelligence, and Cyberspace and Electromagnetic Activities, to mention but a few, compete with Information Manoeuvre for prominence and together cloud the conceptual field. As a result, the concept is at risk of being shrouded in ambiguity. Divergence of interpretations and misunderstandings could hamper successful implementation of the concept and trigger intra-organizational disputes about responsibilities. Therefore, this article aims to provide clarity on the conceptual foundations of Information Manoeuvre and the manner in which it is interpreted within the Netherlands Ministry of Defence (MoD). To do so, the

* Marije Timmer MSc MA works for the Dutch Ministry of Defence and is a graduate of its Military Strategic Studies master's degree programme. Brigadier-General Paul Ducheine is Professor for Cyber Operations and Cyber Security at the Netherlands Defence Academy.

1 Jelle van Haaster, *On Cyber: The Utility of Military Cyber Operations during Armed Conflict* (University of Amsterdam, 2019) 70-84; Roy van Keulen, *Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age* (Leiden University, 2018) 19-38.

2 Paul Ducheine, Corstiaan de Haan and Norbert Moerkens, 'Informatiemanoeuvre en nieuwe traditieverbanden in de Koninklijke Landmacht', *Militaire Spectator* 190 (2021) (5) 258-267.

3 Royal Netherlands Army, Information-Driven Operations for the Royal Netherlands Army: Manoeuvring in the Information Environment (2020) 11.

underlying concepts of Information and Manoeuvre are examined before a comprehensive definition of Information Manoeuvre is provided and its interpretation within the MoD explored.

The meaning of 'information'

'Information' might seem a self-explanatory and commonly understood term. Yet, in reality, it is quite ambiguous. In general, four different conceptualizations of information can be distilled. These conceptualizations are not mutually exclusive and can exist side by side. Yet, depending on the context in which the term 'information' is used, either may be dominant.[4]

Information as a resource for decision-making
Information can be treated as purely consisting of data in the environment, which may comprise various types of data, from objects and events to sounds and smells. Anything that can be observed, measured, processed, and analysed is considered to be information.[5] In military tradition, such data are considered a resource for (understanding and) decision-making. Information understood as a resource corresponds to the interpretation of intelligence as 'information that meets the stated or understood needs of [decision-makers] and has been collected, processed, and narrowed down to meet those needs'.[6] As such, information as a resource is considered to be one of the main functions of military conduct.[7] NATO states that intelligence is an 'aid to provide situational awareness, develop understanding and is a critical tool for decision-making'.[8] In this way, intelligence can bestow a 'decision advantage' or 'information edge' upon decision-makers.[9]

Information as stored knowledge
Information can be considered as a representation of knowledge in a physical, digital, or cognitive form.[10] The principles and

Information	Information is interpreted in four main ways based on its supposed function. Information can be conceptualized as a resource for decision-making, as stored knowledge, as a means to influence, and as part of communication. Information can take different shapes: cognitive, virtual, and physical.
Information Environment	The Information Environment concept comprises three dimensions – cognitive, virtual, physical – in which observations are obtained, understanding and decision-making takes places, operations are conducted and entities can be engaged.
Information Manoeuvre	Information Manoeuvre comprises the direction and execution of activities in the cognitive, virtual, and physical dimensions of the information environment, to achieve a position of advantage in respect to an audience in order to accomplish a mission.
Information-driven Operations (IGO)	Information-driven Operations is an umbrella term to denote the various uses of information, including intelligence, communication and information-sharing, and delivering effects, in addition to organization management.

Overview of key concepts

4 Maureen McCreadie and Ronald Rice, 'Trends in Analyzing Access to Information. Part I: Cross-Disciplinary Conceptualizations of Access, *Information Processing and Management* 35 (1999) 46-48.
5 Ibid.
6 Mark Lowenthal, *Intelligence. From Secrets to Policy* (Thousand Oaks, SAGE Publications, 2020) 1.
7 NATO, *Allied Joint Doctrine for the Conduct of Operations – AJP 3* (2019) 1.23; Ministry of Defence, *Netherlands Defence Doctrine* (The Hague, 2019) 90-91.
8 NATO, *AJP 3*, 1.23.
9 Peter Oleson (ed.), *Guide to the Study of Intelligence* (Falls Church, Association of Former Intelligence Officers, 2016) 4.
10 McCreadie and Rice, 'Trends in Analyzing Access to Information', 9; Van Haaster, *On Cyber*, 184-185.

In general, four different conceptualizations of information can be distilled

practices that armed forces take into account when pursuing their objectives is enshrined in military doctrine and policy and is stored in the experience and education of military personnel. All this knowledge forms a frame of reference against which individuals judge new information they encounter.[11] In this manner, knowledge presents an internal resource which, together with external data, provides the basis upon which to develop understanding of a situation.[12] The perspective of information as knowledge is present in much of day-to-day military conduct, especially in the areas of military science and in education and training departments.

Information as a means to influence

Information can be understood as a message, as something that can be produced, distributed, manipulated, and controlled and can therefore be used by the sender in different ways and for various purposes.[13] This perspective is based on the assumption that the receiver's observation and subsequent interpretation of the message can be steered toward the sender's intentions in a process of communication that is both deliberate and purposeful. This, too, is a perspective familiar to armed forces that have used information to gain an advantage over opponents by disrupting their decision-making.[14] Similar to intelligence, the military tradition of deception is said to be 'as old as warfare itself'.[15] There is a wide variety of methods used to deceive an audience, including dissimulation (hiding true information) and simulation (showing false information), denying information, misdirection, spreading disinformation, increasing ambiguity, and targeted misleading.[16] Using information to influence the perceptions, attitudes and behaviour of relevant actors is also one of two facets subsumed under the information function of modern military conduct.[17]

Information as part of communication

Information can be conceptualized as being part of the communication process. It emphasizes that information is a feature of every human interaction and that understanding is heavily dependent upon human behaviour and sense-making processes.[18] In military organizations, information plays a crucial role as part of the internal communication and information-sharing processes. Two functions of military conduct are – at least partially – concerned with ensuring an efficient information flow: command and control and the information function.[19] For both these functions it is important that information is managed in such a way that all departments at all levels in the organization have access to the required information when necessary. In this process, modern information infrastructure and appropriate procedures are vital to ensure information-sharing throughout the organization.

11 Rasha Abdel Rahman and Werner Sommer, 'Seeing What We Know and Understand. How Knowledge Shapes Perception', *Psychonomic Bulletin & Review* 15 (2008) (6) 1055-1061.
12 Idem, 2.5.
13 McCreadie and Rice, 'Trends in Analyzing Access to Information', 46-48.
14 Hy Rothstein and Barton Whaley (eds.), *The Art and Science of Military Deception* (Boston, Artech House, 2013) xix; Peter Pijpers and Paul Ducheine, 'Deception as the Way of Warfare. Armed Forces, Influence Operations and the Cyberspace Paradox', *The Hague Centre for Strategic Studies*, 2023.
15 Mark Lloyd, *The Art of Military Deception* (Barnsley, Pen & Sword Books Limited, 1997) 1.
16 Han Bouwmeester, *Krym Nash. An Analysis of Modern Russian Deception Warfare* (Utrecht University, 2020) 95-102.
17 NATO, *AJP 3*, 1.24.
18 McCreadie and Rice, 'Trends in Analyzing Access to Information', 46-48.
19 NATO, *AJP 3*, 1.22-1.24.

PHOTO MCD, GERBEN VAN ES

Modern information infrastructure and appropriate procedures are vital to ensure information-sharing throughout the armed forces

The information environment

These four conceptualizations of information denote the different ways in which the function, purpose, and character of information can be interpreted. Yet, information can take on many different shapes. Information is not limited to written or spoken words but also includes all information that can be found in a person's mind and in social settings, such as beliefs, thoughts, opinions, norms, values, and emotions. In addition, information can be found in virtual forms, for instance as social media profiles, email-addresses, text messages, bits, and software. A third shape that information may take is a physical one, in the form of people,

The notion of an information environment allows for the co-existence of different conceptualizations of information

When taking on the perspective of information as a means, three dimensions provide both the tools and targets to influence the decision-making processes of others

(network) infrastructure, and terrain, to add some examples. These three categories of information are also called the dimensions – cognitive, virtual, and physical – that together make up the 'information environment'.[20] The information environment construct describes the setting in which understanding and decision-making takes places and operations are conducted, what kind of entity is engaged or targeted and in which of the three dimensions this occurs.

The notion of an information environment allows for the co-existence of the different conceptualizations of information. When viewing information through the 'resource' lens, the three dimensions can be considered as three different categories of data to be observed. For example, the beliefs and values of certain individuals can be examined in the cognitive dimension, social media profiles can be assessed in the virtual dimension, and behaviour can be analysed in the physical dimension.

20 Van Haaster, *On Cyber*, 184-185.

Alternatively, when taking on the perspective of information as a means, those three dimensions provide both the tools and targets to influence the decision-making processes of others. For example, individuals may be persuaded to alter their behaviour by persuasion in the cognitive dimension; text and visual data can be manipulated in the virtual dimension whereas infrastructure can be disrupted or destroyed in the physical dimension.

Conceptualizations in a generic decision-making process

The different conceptualizations of information appear at different moments throughout the decision-making process, comprising a sequence starting with observing, understanding, deciding, orchestrating and, finally, acting. The resulting activities or the consequences thereof can themselves be observed, thus continuing the cycle. When the environment is observed and analysed, information is conceptualised as a resource for decision-making. Here, pre-existing knowledge plays a role in shaping the interpretation of external observations. When attempting to generate effects in the information environment, information is conceptualised as a means to do so. When ensuring a properly functioning information flow throughout the decision-making process, information is conceptualized as communication. The different conceptualizations of information at different stages in the decision-making process are visualized in figure 1.

It must be highlighted how important one's perspective is when considering the information concept. Not only can the way that information is understood differ at various points in the decision-making process but it also makes a difference whether information is viewed from the perspective of one's own forces or rather from the perspective of the audience. For example, information that is viewed as a resource for one's own forces and can in fact be the instrument of opponents in an attempt to influence, and vice versa. Therefore, what is a resource to one party can actually be a means

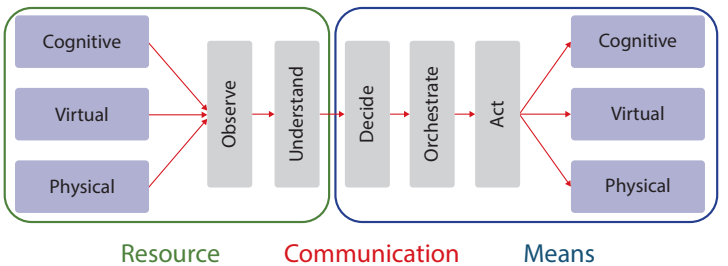


Figure 1 Conceptualizations of information in decision-making[21]

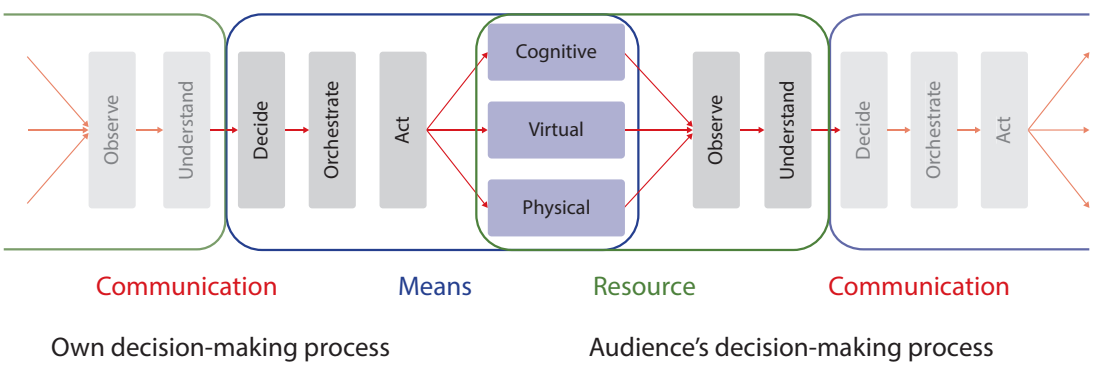


Figure 2 Information in one's own decision-making process compared to the audience's[22]

for another and, conversely, what may be a means to one side can be viewed as a resource to the other. These relationships are demonstrated in figure 2.

Manoeuvre

Manoeuvre is a concept that may be difficult to grasp and, although it is laid down in doctrine, it is not always universally understood.[23] The term may take on different meanings, depending on the context in which it is used, and 'has a possible applicability at every level of warfare, in all environments, and throughout the spectrum of military activity'.[24] The most general definition of manoeuvre as a noun is that of 'a movement or set of movements needing skill and care'.[25] This perspective is also found in a military context where the traditional form of manoeuvre is indeed most often related to physical movement. An alternative interpretation of manoeuvre sees it as an attempt 'to control or influence a person or situation in a particular way'.[26] The latter of these two emphasises cunningness and cleverness in an attempt to manipulate or otherwise influence someone.[27] This does not necessarily include physical movement but is primarily concerned with the mind.

21 Note. Adapted from Peter Pijpers and Paul Ducheine, ''If You Have A Hammer…' Reshaping The Armed Forces' Discourse On Information Maneuver', *Amsterdam Law School Research Paper* 34 (2021) 1-20.
22 Idem.
23 John Kiszely, 'The Meaning of Manoeuvre', *RUSI Journal* 143 (1998) (6) 36.
24 Idem, 40.
25 Cambridge Dictionary, s.v. 'manoeuvre', https://dictionary.cambridge.org/dictionary/english/manoeuvre.
26 Ibid.
27 Kiszely, 'The Meaning of Manoeuvre', 36.

As Kiszely points out, the most common military interpretation of manoeuvre combines the two interpretations.[28] As a combination of a physical and mental activity, manoeuvre is also defined by NATO as the 'employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy in order to accomplish the mission'.[29] Manoeuvre is also an official joint function of military conduct.[30] In this regard, manoeuvre includes the focus on targeting an actor's weak points, the clever directing of fighting power, and the emphasis on the mental as much as on the physical component.[31] This is the spirit of what has been termed the 'manoeuvrist approach', i.e. an approach that emphasises 'shattering the enemy's overall cohesion and will to fight'.[32] To concretise the means by which this goal is achieved, this classic form of manoeuvre relies on 'attacks on the enemy's command and control systems and the requirement for high tempo and simultaneity'.[33] As a broad concept, varying forms of manoeuvring can be found across the spectrum of military activity. It may include the decision-making, orchestration, and execution phases of the decision-making process and take place at all levels of conflict.[34]

Information Manoeuvre

The term Information Manoeuvre is the joining of the words 'information' and 'manoeuvre'. The complexity of the information aspect and the breadth of the manoeuvre aspect complicates defining Information Manoeuvre. Information does not have a straightforward definition; instead, four conceptualisations of information exist that are dependent on the context in which the term 'information' is used. In addition, it has been asserted that information can take a physical, digital, or cognitive shape. What follows is that it is in these three dimensions of the information environment that information manoeuvre takes place.

The previously discussed principles of manoeuvre have a number of implications for the Information Manoeuvre concept. It means that Information Manoeuvre combines the two facets of manoeuvre: it comprises movement or action as well as the 'deceptive, elusive, scheming adroitness' that causes someone to be influenced or manipulated. [35] Information Manoeuvre emphasises the exploitation of the audience's vulnerabilities and the clever directing of activities where they can have maximum effect. As a result, it underlines economy of effort. In addition, manoeuvring in the information environment relies on the intelligent use of methods in all three of its dimensions instead of relying purely on kinetic methods. Similar to manoeuvre as previously characterized, Information Manoeuvre can just as well be concerned with the mind as with physical action. Furthermore, manoeuvre can involve both decision-making and planning and the execution of those decisions and plans at all three levels of conflict.[36] The same therefore applies to Information Manoeuvre, which is concerned with the decision-making, coordination, and execution of actions in the information environment.

These considerations lead to the following definition: Information Manoeuvre comprises the direction and execution of activities in the cognitive, virtual, and physical dimensions of the information environment, to achieve a position of advantage in respect to an audience in order to accomplish a mission.

Similar to 'regular' manoeuvre, Information Manoeuvre can be likened to a game of chess, with 'one opponent seeking to mentally outmanoeuvre the other', which may involve

28 Ibid.
29 NATO, *Glossary of Terms and Definitions AAP-06* (2013) 2M.2.
30 NATO, *AJP 3*, 1.21; Ministry of Defence, *Netherlands Defence Doctrine*, 90.
31 Ministry of Defence, *Netherlands Defence Doctrine*, 90.
32 Kiszely, 'The Meaning of Manoeuvre', 37.
33 Ibid.
34 S. Davison, 'Manoeuvre,' *Australian Defence Force Journal* 152 (2002), 43-48.
35 Kiszely, 'The Meaning of Manoeuvre', 36.
36 Davison, 'Manoeuvre', 43-48.

physical action but does not require it.[38] If manoeuvring in the information environment involves the use of information with the intention to get an advantage, information is thus primarily seen as the instrument or means to do so. Information Manoeuvre therefore seems to be most strongly associated with the conceptualization of information as a means. What follows from this is that the purpose of Information Manoeuvre is to gain an advantage by affecting the decision-making of a target audience. Nevertheless, information used as a resource and information used as communication are both prerequisites to the functioning of military operations.[39] Hence,

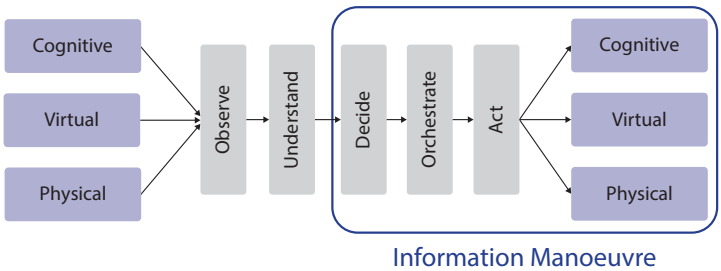


Figure 3 Information Manoeuvre in decision-making[37]

37 Note. Adapted from Pijpers & Ducheine, 'If You Have A Hammer…'.
38 Kiszely, 'The Meaning of Manoeuvre', 36.
39 NATO, *AJP 3*, 1.21-1.24.

The first alternative interpretation considers Information Manoeuvre to be nearly equivalent to the concept of Information-driven Operations

PHOTO US MARINE CORPS, JERROD MOORE

Information Manoeuvre seems to be most strongly associated with the conceptualization of information as a means

they are also essential to Information Manoeuvre.

Information Manoeuvre can include any activity that takes place in any dimension of the information environment, which in any shape or form attempts to deliberately affect, influence, manipulate, or disrupt the perceptions, attitudes, behaviour and, ultimately, the decision-making of a target audience in a favourable direction. As such, Information Manoeuvre has adopted the breadth of the manoeuvre concept. Therefore, familiar disciplines and concepts such as command and control warfare, public affairs, strategic communications, psychological operations, cyber and electromagnetic activities, as well as kinetic action, to mention but a few, can all be used for Information Manoeuvre. Influencing an audience's decision-making process can, for example, take the shape of influencing a target group through a public affairs campaign, through undermining the audience's information and communication systems, or through something as traditional as the use of physical decoys. Therefore, while there is a wide variety of available tools and methods, when used to manoeuvre in the information environment, they share the fundamental aim to achieve a position of advantage in respect to an audience.

40 Due to their anonymized nature, the transcripts of the interviews are not published.
41 Abbreviation in Dutch.
42 Abbreviation in Dutch.
43 Abbreviation in Dutch.

Information Manoeuvre in the MoD

The complexity of the Information Manoeuvre concept and the ambiguity surrounding the constituting terms 'information' and 'manoeuvre' potentially leave room for divergent interpretations. To investigate the presence of such alternative interpretations within the Dutch MoD, policy documents and other official publications were scrutinized and interviews conducted. These anonymised interviews were held with six subject-matter experts associated with some of the military organizations involved in the implementation or execution of Information Manoeuvre.[40] The Army Staff and Directorate-General for Policy (DGB)[41] were chosen to include staff and policy level perspectives on the concept. The Land Information Manoeuvre Centre (LIMC) was chosen because of its singular focus on information manoeuvre, and the Military Intelligence and Security Service (MIVD)[42] in order to include an intelligence perspective on Information Manoeuvre. The results of this examination demonstrate a significant variation in the manner in which Information Manoeuvre is understood. Three of the most prominent deviations from the previously established definition are discussed. These deviations are related to each other and might stem from a confounded understanding of 'information'. Conceptualizations of information as a resource intertwine with those that see information as a means and those that see information as communication to create a muddled understanding of what it means to manoeuvre in the information environment.

#1 Information Manoeuvre ~ Information-driven Operations

The first alternative perspective on Information Manoeuvre is one that broadens the definition of Information Manoeuvre significantly. This interpretation considers Information Manoeuvre to be nearly equivalent to the concept of Information-driven Operations (IGO) (see figure 4).[43] IGO is generally understood to be an umbrella term to denote the various uses of information, including intelligence, communication and information-sharing, and

delivering effects.[44] Moreover, to complicate matters even further, the term IGO is also used to refer to organization management outside operations. IGO therefore includes not only a perspective on information as a means to generate effects, but also as a resource for decision-making and as communication. As such, IGO is a much broader concept than Information Manoeuvre, which is based on the conceptualization of information as a means to generate effects. Nevertheless, the perspective that equates Information Manoeuvre with IGO was found to be pervasive, encountered both in a document published by the Army Staff and in an interview with a subject-matter expert.[45] In this interpretation, Information Manoeuvre is the military translation of the IGO concept, more concerned with operational affairs than with data management and organizational processes, yet in most ways identical. What this interpretation does is consider Information Manoeuvre as essentially a catch-all phrase; a concept that encompasses most, if not all, uses of information in a military organization.

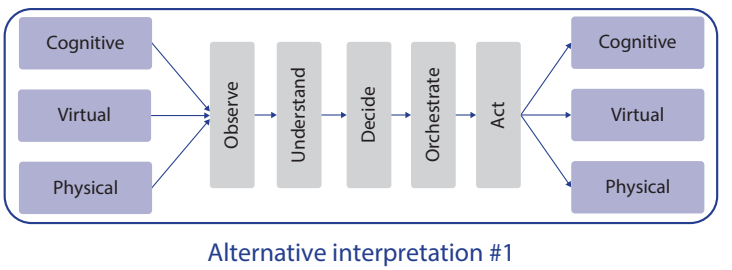


Figure 4 Information Manoeuvre as the equivalent of IGO

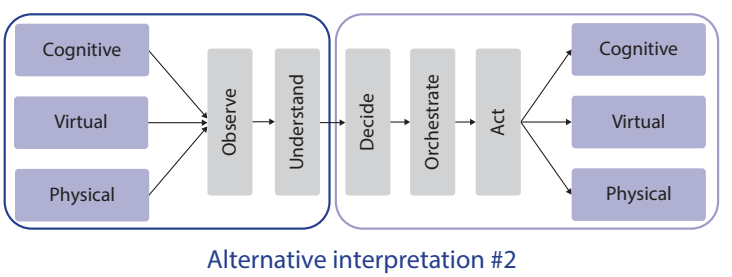


Figure 5 Information Manoeuvre as Intelligence 2.0

#2 Information Manoeuvre ~ Intelligence 2.0
Intelligence was previously defined as 'information that meets the stated or understood needs of [decision-makers] and has been collected, processed, and narrowed to meet those needs'.[46] This process of collecting and processing information to support decision-making was argued to be critically important to, yet fundamentally distinct from, Information Manoeuvre. Nevertheless, the second alternative perspective considers intelligence, or intelligence-like processes and activities, as part of Information Manoeuvre (see figure 5).

In some cases, intelligence was very deliberately mentioned and included as part of Information Manoeuvre.[47] In other cases, intelligence was not referred to as such but still consciously included, albeit through the use of alternative terminology. Both the *Delphi Study* and the *Army vision on IGO* documents use the term 'information exploitation' to denote the identical process of collecting and processing information to support decision-making.[48] Yet in other cases, intelligence-like processes and

Manoeuvring in the information environment relies on the intelligent use of methods in all three of its dimensions instead of relying purely on kinetic method

44 Ministerie van Defensie, 'Kamerbrief Beleidsvisie Informatiegestuurd Optreden' (The Hague, 2023), https://www.rijksoverheid.nl/documenten/kamerstukken/2023/07/04/kamerbrief-beleidsvisie-informatiegestuurd-optreden; Royal Netherlands Army, *Information-Driven Operations*, 11.
45 Interview #1, interview by author, May 24, 2022; Interview #4, interview by author, June 21, 2022.
46 Lowenthal, *Intelligence. From Secrets to Policy*, 1.
47 Interview #1, interview by author, May 24, 2022.
48 Ministerie van Defensie, *Informatie als wapen, middel en doel* (The Hague, 2016); Royal Netherlands Army, *Information-Driven Operations*.

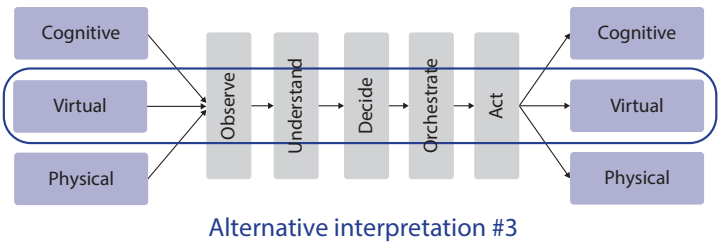


Figure 6 Information Manoeuvre as primarily concerned with the virtual dimension

activities were included in a much more unconscious manner. For example, some interviewees did not include intelligence or 'information exploitation' in their definition of Information Manoeuvre. Instead, they emphasized its fundamental goal of generating effects. However, they contradictorily implied that the use of novel technologies to gather better and more timely information with the intention to create or improve situational awareness is considered Information Manoeuvre.[49]

This perspective on Information Manoeuvre is evocative of an Intelligence 2.0 approach.[50] It emphasizes that in modern conflict 'the side with better information that could be refined into knowledge to guide tactical and strategic decision-making' has the edge over its opponents.[51] This search for an 'information edge' is fundamentally different by nature from the search for a way to influence an audience through activities in the information environment. Due to their different goals and functions, it serves to distinguish between the two to prevent confusion and muddling their conceptual underpinnings.

The unclear relationship between the terms Intelligence and Information Manoeuvre is also visible in discussions on responsibilities. The confounding of these concepts could become problematic if the blurred distinction between the two terms is reflected in a similarly blurred distinction in legal mandates and responsibilities. See for example the discussions surrounding the LIMC experiment.[52] In addition, the broad interpretation of Information Manoeuvre as including intelligence or intelligence-like processes and products risks clashing with the interpretations of intelligence work as described by some respondents. Some interviewees argued that the narrow view of intelligence organizations as solely concerned with developing understanding is somewhat outdated.[53] As such, a broad and ambiguous understanding of the Information Manoeuvre concept could risk blurring responsibilities between armed forces and intelligence organizations.

#3 Information Manoeuvre ~ the virtual dimension

This alternative interpretation of Information Manoeuvre strongly emphasizes manoeuvring in the virtual dimension, cyberspace, and the electromagnetic spectrum (see figure 6). The definition as previously formulated in this article underscored that manoeuvring in the information environment can take place in the cognitive, virtual, and physical dimensions. Yet, the view of Information Manoeuvre as primarily concerned with activities in cyberspace and the electromagnetic spectrum proved to be pervasive. A draft policy document divided Information Manoeuvre into two main types of operations: Cyber Operations, which seek to deliver effects primarily in and through the virtual dimension, and Information Operations, which aim to deliver effects primarily in and through the cognitive dimension.[54] This is already more limited than the definition adopted in this article, which also includes activities in the physical dimension. However, one interviewee emphasized the virtual dimension even more, pointing out that activities in the cognitive dimension which aim to directly influence the behaviour of a target audience, are considered to be very sensitive and are often shied away

49 Interview #3, interview by author, June 14, 2022; Interview #4, interview by author, June 21, 2022.
50 Term used by Pijpers & Ducheine, 'If You Have A Hammer…'.
51 John Arquilla, *Bitskrieg. The New Challenge of Cyberwarfare* (Cambridge, Polity Press, 2021) 14.
52 Commissie-Brouwer, onderzoeksrapport LIMC *Grondslag gezocht*, 2023.
53 Interview #2, interview by author, June 9, 2022.
54 Ministerie van Defensie, *IGO: Informatie als doel, middel en wapen* (draft version 5-01-22) (The Hague, 2022) 21-23. [document is archived with author].

from.[55] As a result, more emphasis is put on activities in the virtual dimension.[56] Another interviewee went even further in underlining the importance of the virtual dimension, arguing that the distinguishing feature of Information Manoeuvre lies in its use of cyberspace and the electromagnetic spectrum. In this interpretation the cognitive, and, to a lesser extent, the physical dimension is affected exclusively through the virtual dimension.[57] It is not unreasonable to assume that cyberspace and the electromagnetic spectrum will play an increasingly important role in Information Manoeuvre. Yet, this alternative perspective could risk creating conceptual confusion due to potential for conflating the terms Information Manoeuvre and Cyber Operations.

Conclusion

This article set out to provide clarity on the conceptual foundations of Information Manoeuvre and the manner in which it is interpreted within the Netherlands MoD. Information was shown to be conceptualized in four distinct manners: as a resource for decision-making, as stored knowledge, as a means to influence, and as a part of the communication process. Information can take shape in cognitive, virtual, or physical form, which are the three dimensions that together make up the 'information environment' in which military organizations operate. Assuming that Information Manoeuvre is essentially manoeuvre that takes place in the information environment, the following definition can be formulated: Information Manoeuvre comprises the direction and execution of activities in the cognitive, virtual, and physical dimensions of the information environment with the aim to achieve a position of advantage in respect to an audience in order to accomplish a mission.

The interpretations of Information Manoeuvre have been shown to differ quite significantly within the MoD. Three main deviations could be discerned, which sometimes overlap. One alternative perspective considers Information Manoeuvre to be the military translation and near equivalent of Information-driven Operations (IGO). Another perspective sees Information Manoeuvre as essentially Intelligence 2.0. A third deviation regards Information Manoeuvre as an approach primarily concerned with the virtual dimension. These deviations might stem from a confounded understanding of what 'information' is. Contextual factors and personal experience determine which of the four conceptualizations of information is dominant. At the same time, the manner in which information is conceptualized has major consequences for the way in which a concept such as Information Manoeuvre is interpreted. The identified interpretations vary to the extent that the differences in understanding could hamper communication and lead to misunderstandings. The obvious risk is that 'using these same terms differently in different contexts is likely to create conceptual confusion that in turn can also result in misallocation and misalignment of resources and capabilities.'[58] Clarity, specificity, and consistency are absolutely key aspects for the successful implementation of a new approach or vision.[59] Indeed, the field of information-related approaches to warfare is riddled with concepts that have been rendered essentially useless due to the lack of accurate definition, incomprehensibility, and inconsistency in their use. [60] If the Information Manoeuvre concept is to remain relevant, it must rise above the terminological issues that plague the field and be defined and employed in a sharp, clear, and simple manner. ■

55 Interview #3, interview by author, June 14, 2022.
56 Ibid.
57 Interview #4, interview by author, June 21, 2022.
58 Herbert Lin, 'Doctrinal Confusion and Cultural Dysfunction in DoD', *The Cyber Defense Review* 5 (2020) (2), 100.
59 Sergio Fernandez and Hal Rainey, 'Managing Successful Organizational Change in the Public Sector', *Public Administration Review* 66 (2006) (2) 169-170.
60 Martin Libicki, *Conquest in Cyberspace. National Security and Information Warfare* (New York, Cambridge University Press, 2007) 17-19.

‘Nederland moet blijven deelnemen aan VN-missies’

Caecilia van Peski ziet ook in de toekomst een rol voor de volkenorganisatie

Frans van Nijnatten

Na de terreuraanval van Hamas vanuit Gaza op Israël begin oktober, de daaropvolgende gijzelings- en vluchtelingencrisis en onrust aan de grens met Libanon maakten topfunctionarissen van de VN overuren. Een ontwerpresolutie waarin werd opgeroepen tot een gevechtspauze voor het doorlaten van humanitaire hulp haalde het medio oktober niet door een Amerikaans veto. De VS stemde tegen omdat de resolutie nergens het recht van Israël op zelfverdediging noemde. KLTZ (SD) Caecilia van Peski volgt de ontwikkelingen met grote belangstelling. Zij werkte immers zelf voor de VN aan conflictbeheersing en kent de organisatie van binnenuit. In een interview met de *Militaire Spectator* legt ze uit waarom de VN imperfect én onmisbaar is. Haar loopbaan, die haar naar talloze conflictgebieden voerde en binnenkort naar Ramallah, is een zoektocht naar de dynamiek die conflict en uiteindelijk vrede aandrijft. Voor Nederland ziet zij een voortzetting van de participerende rol: ‘Laten we VN-vredesmissies vooral blijven ondersteunen’.

De aanval van Hamas en de daaropvolgende Israëlische vergeldingsacties hebben al aan duizenden mensen het leven gekost. Het hoofdkwartier van UNRWA, het VN-Agentschap dat al sinds 1949 humanitaire hulp verleent aan naar de Gaza en de Westelijke Jordaanoever verdreven Palestijnen, liep schade op bij Israëlische luchtaanvallen en zeker 57 VN-medewerkers kwamen daar bij om. Het conflict vraagt het nodige van een toch al overbelaste VN, die op volle toeren moet draaien door onrust, oorlog en uitputting in verschillende delen van de wereld. Verschuivingen in het geopolitieke spectrum hebben gezorgd voor een afname van financiële bijdragen aan mondiale multilaterale organisaties, terwijl ook de maatschappelijke support daalt. Zo vroeg Armenië eind september om VN-toezicht in Nagorno-Karabach, de enclave in Azerbeidzjan waar tot dan etnische Armeniërs woonden in een zelfverklaarde republiek die vanaf het nieuwe jaar zal worden opgeheven. Omliggende landen hebben uiteenlopende belangen in de regio en Rusland is als vredesmacht in het gebied aanwezig. In die situatie greep de VN niet in. Begin oktober besloot de VN-Veiligheidsraad een internationale troepenmacht naar Haïti te sturen om het oplaaiende geweld daar in te dammen. Rusland en China onthielden zich in de raad van stemming, wat een breder VN ingrijpen tegenhield. De jongste ontwikkelingen komen als een extra zorg bij het toch al zeer intensieve werk dat de VN sinds de Russische annexatie van de Krim (2014) in Oekraïne en in

FOTO PAUL TOLENAAR

KLTZ (SD) drs. Caecilia Johanna van Peski (1970) richt zich vanuit CZSK en krijgsmachtbreed op civiel-militaire interactie, internationale betrekkingen en politiek-militaire zaken. Zij studeerde onderwijs- en cultuurpsychologie aan de Universiteit van Tilburg met een minor omgaan met oorlogstrauma. Haar academische loopbaan zette zij voort aan de Bundeswehr Universiteit in Hamburg en het OSCE Border Management Staff College in Doesjanbe, Tadzjikistan. Van Peski werkte onder meer voor de EU, NAVO, OVSE en de VN. In 2010 sprak zij de Algemene Vergadering van de VN toe in New York als lid van de Nederlandse Koninkrijksdelegatie. De VN selecteerde haar voor de UN Senior Women Talent Pipeline en kort daarop werd zij door de Sociaal Economische Raad benoemd tot SER-Topvrouw. Van Peski is voorzitter van de Raad van Advies van de Nederlandse Vereniging voor de Verenigde Naties, die op 1 december in Den Haag een rondetafelconferentie houdt over 75 jaar vredeshandhaving en 75 jaar Universele Verklaring van de Rechten van de Mens. In januari vertrekt zij naar het Bureau van de US Security Coordinator for Israel and the Palestinian Authority, met als standplaats Ramallah op de Westelijke Jordaanoever.

Rusland uitvoert. Onder de internationale druk kraakt de VN-organisatie – inmiddels 78-jaar oud – in haar voegen; een kwetsbare positie in het licht van de ontwikkelingen in de wereldpolitiek.

‘De VN is sinds de oprichting bedoeld als grensoverschrijdend overlegmechanisme, een organisatie waar ook pragmatische compromissen gesloten kunnen worden omdat landen het

‘Hoe het wereldbestel zich ontwikkelt is geen zaak van de VN’

in veel gevallen niet volledig met elkaar eens zijn’, zegt Van Peski. ‘Hoe het wereldbestel zich ontwikkelt is ook geen zaak van de VN. Neem bijvoorbeeld de tegenovergestelde belangen tussen de Gobal South-landen versus landen in de Global North. Je ziet momenteel dat opkomende landen op het zuidelijk halfrond zich afwenden van het noorden: ze schudden onze manier van zaken doen af en zoeken alternatieven. Zoals de BRICS-naties, die landen die met hen mee willen doen aan weten te trekken met nieuwe beloftes voor een betere toekomst’. De originele BRICS-landen Brazilië, Rusland, India, China en Zuid-Afrika kenden de afgelopen jaren economieën die groeiden in kracht en macht en propageren een soortgelijke ontwikkeling voor landen met dezelfde hoop. Inmiddels hebben al veertig landen aangegeven graag onderdeel van BRICS te willen worden. Zo ontstaat er een nieuw politiek-economisch machtsblok dat de potentie heeft om eerdere multilaterale structuren te eroderen. Nadat Rusland door zijn invasie van Oekraïne in 2022 te maken kreeg met westerse sancties, is Moskou er alles aan gelegen elders in de wereld steun te zoeken. Afgelopen augustus kwamen vertegenwoordigers van BRICS samen in Johannesburg en maakten zij bekend dat in eerste instantie zes landen zich concreet bij de organisatie zullen aansluiten: Argentinië, Egypte, Ethiopië, Iran, Saudi-Arabië

en de Verenigde Arabische Emiraten. Groeit dit uit tot een alternatief voor de Beweging van Niet-Gebonden Landen, of voor nieuwe diplomatieke kanalen buiten de VN om? ‘Het is een recent en een ander fenomeen, want Rusland heeft nooit tot de in 1961 opgerichte Beweging behoord’, zegt Van Peski. ‘Doordat Rusland met de invasie van Oekraïne meer geïsoleerd is komen te staan in de wereld komt het nu goed uit dat zij in 2009 het initiatief namen tot de oprichting van BRICS en daarmee dus een alternatief in handen hebben. Naast Rusland heeft ook China sindsdien landen in de Global South financiële steun gegeven plus een overlegstructuur die via een andere route dan het Westen loopt. Dat wil in principe nog niet zeggen dat landen de communicatie- en onderhandelingslijnen die zij al hadden bij de VN of westerse landen af zullen kappen – dat pad om invloed uit te oefenen wil niemand kwijt. Maar het ontstaan van divergentie kan wel inhouden dat de momenteel juist zo noodzakelijke gezamenlijke communicatie op wereldniveau onderbrekingen ondervindt. Dat kunnen wij ons niet permitteren.’

Enkele dagen na de Russische invasie van Oekraïne kwam de VN-Veiligheidsraad met een resolutie waarin stond dat er geen unanimiteit onder de permante leden was om verdere actie te ondernemen. Rusland vond hier een bondgenoot in China, India en de VAE. De V-Raad riep wel een speciale zitting van de Algemene Vergadering bijeen, die op 2 maart 2022 in een resolutie met 141 landen voor en vijf tegen de onmiddellijke Russische terugtrekking uit Oekraïne eiste. Ondanks druk van Oekraïne en andere landen nam Rusland afgelopen april voor een maand volgens schema het voorzitterschap van de V-Raad op zich. De keer daarvoor dat Rusland voorzitter was, in februari 2022, viel het Oekraïne binnen. Velen willen al jarenlang hervormingen van de V-Raad, waar de Permanente Vijf (P5) – de VS, het Verenigd Koninkrijk, Frankrijk, China en Rusland – het met hun vetorecht voor het zeggen hebben. De roep om verandering is door de Russische invasie van Oekraïne alleen maar luider geworden. ‘En heel terecht’, zegt Van Peski. ‘In het verleden is beslist dat economisch sterke landen als

De VN-Veiligheidsraad op 18 oktober in New York bijeen om te stemmen over een ontwerpresolutie over de situatie in het Midden-Oosten: ‘Hervorming van de V-Raad is een titanenstrijd voor volhouders’

Duitsland en Japan meer te zeggen zouden moeten hebben. Maar zolang de Permanente Vijf er niet aan mee willen werken om deze landen meer invloed te geven binnen de VN – angstig als zij zijn om een stukje van hun eigen macht af te moeten staan – staan de P5-leden binnen de V-Raad het waarmaken van de intrinsieke belofte

FOTO VN, EVAN SCHNEIDER

van de VN in de weg. Andere landen hebben daar steeds mee moeten dealen en intussen hun diplomatieke mogelijkheden moeten benutten, soms zelfs uit moeten putten. Ik denk trouwens dat Nederland zijn mogelijkheden goed gebruikt, omdat het omgaan met ambigue omgevingen Nederlandse beleidsmakers wel ligt. En ik zie dat de jongere generatie diplomaten, die ik ken uit de lesomgeving binnen universiteiten en onderzoeksinstituten, daar ook in uitmunt. Zij nemen met durf, persoonlijkheid en een groot maatschappelijk besef aan de onderhandelingstafel plaats. Het is niet voor niets dat de VN in haar beleid rondom conflictbemiddeling een voorrangspositie voor ogen heeft voor vrouwen én voor jongeren.'

Na de invasie van Oekraïne heeft Rusland in 2022 zijn veto gebruikt om een resolutie te blokkeren waarin de onmiddellijke terugtrekking werd geëist. Ook torpedeerde Rusland een resolutie die aangekondigde referenda in

vier bezette oblasts (districten) in het oosten van Oekraïne 'illegaal' noemde. Richard Gowan, directeur VN bij de International Crisis Group, zegt dat Moskou in de V-Raad vooral politiek theater bedrijft en de diplomatie naar achteren heeft geschoven om een narratief te pushen via social media en de wereldpers.[1] Omdat agressor Rusland zelf permanent lid is en de V-Raad vleugellam kan maken, hebben andere landen hun krachten gebundeld in de Algemene Vergadering om zo de druk op Moskou te verhogen. Sinds maart 2022 heeft de Algemene Vergadering meerdere resoluties tegen Rusland aangenomen. Terwijl landen via zulke resoluties proberen het Russische narratief te de-legitimeren, maakt Oekraïne slim gebruik van de Algemene Vergadering om zijn eigen verhaal op de internationale bühne te vormen, zegt Gowan.[2] 'Het dwarsliggen van Rusland hoeft niet te betekenen dat de hele VN meteen niet meer werkt', zegt Van Peski. 'Dat zou een kapitale denkfout zijn die een ongelooflijk risico in zich draagt. Naast de Algemene Vergadering verrichten secretaris-generaal António Guterres en de verschillende VN programma's, agentschappen en organisaties resultaatrijk werk op humanitair-, diplomatiek- en ontwikkelingsvlak. Vorig jaar leidde die inzet van de VN tot het akkoord over de heropening van Oekraïense havens voor de graanexport. De VN is de enige organisatie die op wereldniveau werkt aan werelddoelen (de duurzaamheids-doelen of SDG's), bedoeld voor de vooruitgang van alle bewoners van deze planeet. Daarnaast draaien VN-organisaties ondanks de fallout van de oorlog in Oekraïne onder steeds complexere condities onophoudelijk door. Bij hulpverlening spelen wel de nodige problemen, omdat sommige gebieden gewoonweg niet bereikbaar zijn of te onveilig om er te kunnen werken. Het relatief grote aantal doden onder VN-personeel in de Gazastrook laat dat ook zien.'

SDG's en uitdagingen

Een van de doelen van de VN, het handhaven van vrede en veiligheid, is sinds de oprichting in 1945 in een aantal gevallen wel, maar vaak ook niet behaald. Dat heeft de organisatie er echter nooit van weerhouden ambitieus te zijn en te zoeken naar wegen die kunnen leiden naar het hoogste doel van absolute vrede. Zo namen alle 193 lidstaten in 2015 de 17 Sustainable Development Goals (SDG's) aan, die de positie van burgers wereldwijd voor 2030 moeten verbeteren (UN Agenda 2030). De SDG's schetsen een weg naar een duurzamere, veiligere wereld waarin armoede is uitgeroeid. 'Je kunt je afvragen of dat allemaal niet te idealistisch gesteld is. Toch kunnen we er niet omheen dat de VN als enige organisatie in staat is gebleken om überhaupt een samenhangend beleid te formuleren op het gebied van heel complexe ontwikkelingsfactoren. Zelf heb ik mij al in 2000, bij de formulering van de Millennium-ontwikkelingsdoelen, de voorloper van de SDG's, gecommitteerd aan SDG 16, 'Vrede, justitie en sterke publieke diensten'. SDG 16 stel ik sindsdien centraal in mijn werk en bij alles wat ik doe probeer ik een inschatting te maken van hoe mijn acties en handelen bijdragen aan het behalen van dat doel. Om die reden stel ik mij gereed voor uitzending naar conflictgebied, ben ik politiek actief, klimaatdoener en voorstander van Europese defensie-integratie. Ik doe en laat specifieke dingen in mijn leven in het licht van SDG 16. Uiteindelijk gaan de SDG's over vooruitgang voor ieder mens (*leave no-one behind*) en het behoud van de wereld en daar zou iedereen zich voor in moeten willen zetten', zegt Van Peski. 'De SDG's zijn geen bedenksel van mensen in New York en worden ook niet centraal door de VN getrokken. Het zijn burgerplatforms, wetenschappers en leden van alle nationale regeringen van VN-lidstaten die de SDG's hebben voortgebracht. De uitwerking ervan wordt gedaan door landelijke organisaties waarbij talrijke maatschappelijke- en belangengroepen aangesloten zijn, zoals SDG Nederland. Daardoor is het mogelijk jaarlijks in ieder land te meten in hoeverre de doelen behaald zijn of niet. Dit maakt het mogelijk om bij te sturen en waar nodig nog harder te duwen.'

1 Betul Yuruk, '1 year into Ukraine war, how has UN used its tools?', *Anadolu*, 23 februari 2023.

2 Idem.

FOTO VN, CIA PAK

Projectie van de 17 SDG's op het hoofdkwartier van de VN in New York: Van Peski stelt SDG 16, 'Vrede, justitie en sterke publieke diensten', centraal in haar werk

Inconvenient Realities

De International Crisis Group somde in een recent rapport tien uitdagingen op voor de VN in 2023-2024, waaronder het vinden van nieuwe manieren voor politieke betrokkenheid bij Mali.[3] Afgelopen juni gaf de Malinese regering te kennen dat de VN-missie MINUSMA, ingesteld in 2013, uiterlijk eind dit jaar beëindigd dient te worden. In september keerden de laatste drie Nederlandse officieren die nog aan MINUSMA verbonden waren naar Nederland terug. De leiders van Mali zoeken sinds 2021 hun heil bij andere partijen, zoals de Russische huurlingengroep Wagner, en niet meer bij de voormalige koloniale macht Frankrijk of bij de VN.

Onderzoekers van het Nederlandse ministerie van Buitenlandse Zaken zijn intussen tot de conclusie gekomen dat de Nederlandse missies in Afghanistan, Mali en Zuid-Sudan tussen 2015-2022 nauwelijks resultaat hebben opgeleverd. Er gaapt een kloof tussen de ambities en de werkelijke invloed bij de toepassing van de Defence, Diplomacy and Development-benadering (3D). De onderzoekers bevelen aan om de Nederlandse doelstellingen en strategieën bij interventies in fragiele gebieden te her-evalueren.[4] Voormalig Commandant der Strijdkrachten Tom Middendorp zei recent in een interview dat effecten van missies moeilijk te meten zijn en dat bijdragen neer kunnen komen op een druppel 'in een hele grote emmer'.[5]

3 *Ten Challenges for the UN in 2023-2024* (New York, International Crisis Group, 14 september 2023) 32-36.

4 Rens Willems en Caspar Lobrecht, *Inconvenient Realities. An evaluation of Dutch contributions to stability, security and rule of law in fragile and conflict-affected contexts* (Den Haag, ministerie van Buitenlandse Zaken, augustus 2023).

5 'Onderzoek: Nederlandse missies in het buitenland hebben nauwelijks succes', *NOS.nl*, 31 augustus 2023.

‘Het is een belangrijk onderzoek dat een heel breekbare omgeving en condities aanwijst’, zegt Van Peski, ‘maar het is geen reden om in de toekomst niet meer aan missies mee te doen. Wat we van de voorbije missies vooral dienen te leren is dat we een veel betere *cultural awareness* moeten opbouwen voordat we naar een gebied gaan. We kunnen militairen wat dat betreft nog een stuk beter voorbereiden, niet alleen voorafgaand aan een uitzending, maar door hun gehele loopbaan heen.’ Betekent dat ook het accepteren van plaatselijke culturele regels die in het Westen als anti-democratisch worden gezien? ‘We kunnen in sommige gevallen niet anders dan dat, maar ik ben geen cultuur-relativist die vindt dat we nooit moeten proberen verandering in gang te zetten binnen de context van internationale waarden, zoals die beschreven zijn in de Universele Verklaring van de Rechten van de Mens.’ Dat in lang niet alle landen die de UVRM 75 jaar geleden onder-tekend hebben, burgers die rechten ook echt hebben, zal voorlopig een gegeven zijn.

Fascinatie

Van Peski werkt vanuit een fascinatie voor de dynamiek van oorlog en vrede. Tijdens haar inzet in tal van landen deed zij de nodige intellectuele bagage en ervaringsdeskundigheid op, maar raakte zij ook zwaargewond in missiegebied en was zij in 2014 als een van de eersten ter plaatse bij de neergeschoten vlucht MH17 in Hrabove, Oekraïne. Ingrijpende ervaringen en tegenslagen zetten haar uiteraard aan het denken, maar kunnen haar ambitie om het lot van mensen op de lange termijn te verbeteren niet aan het wankelen brengen. Van Peski hanteert een progressief denken en wijst naar positieve ontwikkelingen, zoals ze deed tijdens de NIM-Veteranenlezing 2023 *In the Service*

‘Wat we van voorbije missies vooral moeten leren is dat we een veel betere cultural awareness moeten opbouwen’

FOTO MCD, EVA KLIJN

of Peace die ze in september hield in Roermond en waarin ze uitgebreid sprak over 75 jaar VN-vredeshandhaving. In 1948 en nog vele jaren daarna 'waren VN-vredeshandhavers soldaten, nagenoeg allemaal afkomstig uit Europa en altijd man'. Tegenwoordig leveren 120 landen zowel vrouwen als mannen voor zulke missies, terwijl naast militairen ook politiepersoneel en internationaal civiel personeel wordt ingezet.[6] Omdat ze zelf langjarig op uitzending is geweest voor de OVSE, de EU en de NAVO, heeft Van Peski een bijzonder oog ontwikkeld voor de opkomst van vrouwen in de internationale vredeshandhaving. Vrouwen nemen daar de mogelijkheid ter hand om te beschermen wat hén dierbaar is. 'Nederland voert een feministisch buitenlandbeleid en ondersteunt daarmee vrouwen die voor internationale organisaties in conflictgebieden werken. Tegelijkertijd zet Nederland zich in voor kansengelijkheid voor vrouwen die in die gebieden wonen. Dat inbreken op patriarchale structuren gaat uiteraard stap voor stap.' Soms moeten er ook stappen terug worden gedaan, zoals in Afghanistan, waar tijdens de ISAF-periode voor meisjes en vrouwen bereikte doelen ongedaan zijn gemaakt door de terugkeer van de Taliban.

De Nieuwe Agenda voor Vrede

Sinds de oprichting in 1945 heeft de VN talloze missies geïnitieerd, waarvan sommige volgens Van Peski zeer terecht hevige kritiek kregen. Zo lukte het de VN-vredeshandhavers in 1994 niet om in Rwanda de massamoord op de Tutsi's een halt toe te roepen, terwijl sommige VN'ers in Cambodja, Congo en Haïti misbruik maakten van hun positie door de plaatselijke bevolking te intimideren of seksueel geweld te plegen. 'Er zijn in het verleden afschuwelijke dingen gebeurd, zoals de genocides in Rwanda en Srebrenica, die ieder menselijk voorstellingsvermogen te boven gaan. Het mondiale multilaterale stelsel staat onder grote druk en verdere fragmentatie dreigt. Voor een deel is de kritiek op de VN zeker terecht, maar we moeten verder trekken op de weg die ons het meeste perspectief biedt op een vreedzame en duurzame toekomst. Als we het multilateralisme in stand willen houden – en niet kiezen voor het scenario 'ieder voor zich' – moeten we via de VN met elkaar blijven samenwerken. We kunnen niet zonder het *top-level*, inclusieve diplomatieke kanaal dat de VN biedt. Daarnaast moeten we vooral niet vergeten dat de VN de afgelopen tientallen jaren onnoemelijk veel heeft bereikt. Denk bijvoorbeeld ook aan vaccinatieprogramma's, mensenrechten, het faciliteren van verkiezingen, bescherming van ecologie en habitat, ondersteuning van rechtsstatelijke principes en instituties en noodhulp', zegt Van Peski. 'Een goed functionerende VN dient een van de belangrijkste doelen van het Nederlandse buitenlandbeleid te zijn.'

'We kunnen niet zonder het top-level, inclusieve diplomatieke kanaal dat de VN biedt'

Nederland kan dat volgens Van Peski onder meer laten zien door de New Agenda for Peace te promoten, de vervanger van de originele Agenda for Peace uit 1992, die nog onder VN-chef Boutros Boutros-Ghali tot stand was gekomen, en de aanbevelingen uit het Brahimi Report uit 2000. 'De New Agenda is in ons belang, want hij

6 KLTZ (SD) Caecilia van Peski, 'In the Service of Peace. 75 jaar VN-vredeshandhaving' (1948-2023). (lezing Roermond, 2 september 2023).

'Nederland voert een feministisch buitenlandbeleid en ondersteunt daarmee vrouwen die voor internationale organisaties in conflictgebieden werken'

legt de nadruk op preventie, diplomatie en peace building. Het gaat daarbij ook om het vinden van duurzame oplossingen voor slachtoffers van oorlog en geweld. Het is dan wel noodzakelijk vredeshandhavingsoperaties aan te passen aan de hedendaagse conflicten. Guterres durft met de New Agenda ook weer de hervorming van de V-Raad en de Algemene Vergadering te prioriteren, wat politiek gezien een titanenstrijd is voor volhouders, maar nu meer urgentie heeft dan ooit. Opmerkelijk is ook dat Guterres geen enkel blad voor de mond neemt in zijn roep om het doorbreken van patriarchale structuren. De New Agenda legt overigens minder de nadruk op interventie door bijvoorbeeld VN-vredesmissies en meer op preventie en de eigen verantwoordelijkheid hierin van een staat. Ook geeft Guterres richting aan een overdracht van

FOTO MINUSMA, HARANDANE DICKO

‘De hervorming van de VN-Veiligheidsraad is politiek gezien een titanenstrijd voor volhouders’

verantwoordelijkheid en handhavingsmacht van internationale vredestroepen naar vredestroepen op het eigen continent, bijvoorbeeld onder gezagvoering van de Afrikaanse Unie. De VN maakt dan via het beschikbaar stellen van middelen zo’n AU-inzet mogelijk. Dit zijn initiatieven die binnen de gangbare context als revolutionair kunnen worden aangemerkt. Maar het zal niet verbazen dat de New Agenda geen voorstel doet tot het instellen van nieuwe multilaterale instituties voor het oplossen van mondiale problemen.’

Op de Summit of the Future, de geplande VN-top in september 2024, zullen landen praten over hervormingen en het behalen van doelen in de komende jaren. De top zal een slotdocument opleveren met de titel Pact for the Future. ‘We kunnen ons nog sterker inzetten voor het bestrijden van ongelijkheid, armoede en instabiliteit in de wereld en het bevorderen van een cultuur van vrede’, zegt Van Peski. Dat lang niet alle landen diezelfde doelen hebben realiseert zij zich goed. Onlangs concludeerde een door de VN ingesteld onderzoeksteam dat Rusland systematisch heeft gemarteld in de Oekraïense regio’s Cherson en Zaporizja. Op een hoorzitting in Genève kon Rusland een weerwoord geven, maar bleef daar weg. Extra pijnlijk voor Van Peski, die vele jaren voor de OVSE in de Oekraïense Donbas aan conflictbeheersing werkte. Van Peski: ‘Ja, ook dat is de VN. Er zijn vaak frustraties. Maar daar staan talloze verworvenheden tegenover.’

Van Peski zal al haar ervaring in conflictresolutie, mediation en crisismanagement gebruiken als zij in januari 2024 aantreedt als stafmedewerker van de United States Security Coordinator for Israel and the Palestinian Authority (USSC), met als standplaats Ramallah op de Westelijke Jordaanoever. Haar jarenlange betrokkenheid bij toonaangevende vredesinitiatieven tussen Israëliërs en Palestijnen zullen haar daarbij goed van pas komen, evenals haar optimistische levenshouding. ■

Gevechtstenue en naaldhakken

Jaus Müller

Zes verkleinde portretten van vrouwen, allen lachend naar de camera, tegenover een uitvergroot beeld van een streng kijkende man in uniform met de mondhoeken strak naar beneden: deze collage ging twee jaar geleden het hele internet over. De vrouwen op de foto zijn de ministers van Defensie van België, Denemarken, Frankrijk, Duitsland, Spanje en Kajsa Ollongren. De man op de foto is de Russische minister van Defensie Sergej Sjojgoe. De tekst eronder luidt: 'Sorry, we're fucked'.

Vrouwen zijn klein en zwak, mannen zijn doortastend en sterk. Dat is de boodschap die dit beeld uitdraagt. Het suggereert ook dat deze groep vrouwen aan de top van verschillende Europese krijgsmachten niet opgewassen is tegen Sjojgoe. De subtekst lijkt dus: vrouwen bij Defensie zijn nutteloos in tijden waar het er écht op aankomt, zoals bij *war fighting* tegen een tegenstander als Rusland.

Laat ik beginnen te stellen dat dit volledig achterhaalde onzin is. Defensie kampt met duizenden vacatures die uitstekend kunnen worden ingevuld door vrouwen, net zoals door medewerkers met een biculturele of lhbt-achtergrond. In juli 2023 daalde het vullingspercentage voor militairen verder naar 78,7 procent, een voorlopig dieptepunt.[1] De rekensom is dus simpel: met alleen jonge mannen komen we er niet. Om het percentage op te krikken, moet Defensie wel breder werven. Sinds enkele jaren voert Defensie daarom een actief diversiteitsbeleid, gericht op het aantrekken van vrouwen, lhbt'ers en biculturele minderheden. Dit is essentieel om op termijn te voldoen aan de primaire taak van de krijgsmacht: het beschermen van het eigen grondgebied en dat van bondgenoten.

De hernieuwde focus op war fighting, zoals we dat nu zien in Oekraïne en sinds kort ook in het Midden-Oosten, brengt een nieuw probleem met zich mee. De inzet van grootschalig geweld wordt in de beeldvorming al snel gekoppeld aan brute mannelijkheid, zoals bij de meme van Sjojgoe. Dit gaat hand in hand met cliché-beelden van vechten in de modder, loopgraven en ontembare oerdriften; niet het imago dat Defensie als moderne werkgever in 2023 wil uitstralen of waarmee je potentieel vrouwelijk en lhbt-personeel uit generaties millen-

nials en Gen Z enthousiasmeert voor een baan in het leger.

We moeten nadenken over hoe we de volgende paradox oplossen: enerzijds is het niet verkeerd om de rauwe realiteit van oorlogvoering in het hoge geweldsspectrum te tonen (als waarschuwing dat dit ook onze richting uit kan komen), maar anderzijds werkt het te nadrukkelijk uitbeelden van oorlog als een ruige 'macho-business' afschrikkend en staat het het bouwen van een diverse krijgsmacht in de weg. Het geeft bovendien een vertekend beeld van de realiteit: niet elke militair is dagelijks bezig met strijd in de voorhoede. Achter elke infanterist staat een heel team ter ondersteuning in geneeskunde, logistiek, inlichtingen en meer.

Het is nu belangrijker dan ooit om af te stappen van de stereotypering van militairen als uitsluitend mannelijk of macho. Het helpt als we militairen zien als individuen met zowel een machokant als een zachtere, mogelijk meer feminiene kant, net als ieder ander. Door clichés te benadrukken bewijzen we niemand een dienst en negeren we de complexiteit van de mens achter de militair, die zowel masculien als feminien kan zijn. Het wordt tijd dat te erkennen. We kunnen hierbij een voorbeeld nemen aan Oekraïne, nota bene een land dat (tot voor kort) niet bepaald voorop liep met lhbt-emancipatie. Door oorlog is het land snel aan het veranderen, met veel meer oog voor diversiteit, zeker ook binnen de krijgsmacht, simpelweg omdat het ook geen keuze heeft: de hele samenleving wordt gemobiliseerd in de strijd tegen Rusland. Steeds meer lhbt'ers vechten aan de frontlijn, waardoor de grenzen tussen masculiniteit en gender juist beginnen te vervagen. Neem als voorbeeld het Instagram-account van een Oekraïense hospik, sergeant Ivan Honzyk. Hij deed mee aan de loopgraven-strijd in onder andere Bachmoet, maar is ook allesbehalve bang om zijn *queer*-identiteit te uiten. Zijn Instagrampagina is een eclectische mengeling van foto's in gevechtstenue afgewisseld met gestileerde beelden van hem met naaldhakken en zwarte engelen-verenpakket. 'My fellow soldiers are really impressed with what I've done in Bakhmut, the massive scale of work that I did there, and after that they just don't care about who I sleep with', zei Honzyk (27) in april tegen *NBC News*.[2]

Dit toont aan dat we moeten afstappen van clichés over mannelijkheid en vrouwelijkheid in het leger. Laten we daarom eens en voor altijd afrekenen met die afschuwelijke stereotiepe meme van Sjojgoe en de zes vrouwelijke ministers waarmee ik begon. Ik baseer me op de feiten: het uniform van Sjojgoe. Het lijkt imposant, maar de werkelijkheid is dat de man nul militaire ervaring heeft en vooral carrière heeft gemaakt als burgerambtenaar in het Russische staatsapparaat. Hij draagt een generaalsuniform zonder dat hij enig benul heeft van het leven als militair. Dat is niet stoer, maar triest.[3] Als we de meme in de juiste tijd plaatsen, blijkt dat deze de wereld overging toen Russische tanks de buitenwijken van Kyiv bereikten en het leek alsof Sjojgoes leger dicht bij de overwinning was. We weten wat er daarna gebeurde: de opmars naar Kyiv werd snel gevolgd door een vernederende terugtocht naar Rusland. Wat volgde was een mislukte militaire semi-staatsgreep die Sjojgoe niet kon tegenhouden met militaire middelen. Hij stuurde daarna nog eens duizenden Russen de dood in tijdens een mislukt offensief in de Donbas, zonder door de linies van de door westerse landen getrainde en bevoorrade Oekraïners te breken.

Wie heeft dit bereikt? Juist, die zes Europese vrouwelijke ministers van Defensie. ■

1 *Stand van Defensie. Voortgang bouwen aan een toekomstbestendige krijgsmacht* (Najaar 2023). (Den Haag, ministerie van Defensie, 19 september 2023).

2 Mo Abbas, Matt Bradley en Ostap Hunkevych, 'As Ukraine's LGBTQ soldiers fight on the front line, acceptance grows in the conservative country', *NBC News*, 16 april 2023.

3 Lees vooral hierover: Mark Galeotti, *Putins Wars. From Chechnya to Ukraine* (Oxford, Osprey Publishing, 2020).

De paradigmaverschuiving van oktober 2023

Sergei Boeke

De geschiedenis kent grote keerpunten. De aanval van Hamas op 7 oktober is er een van. Voor Israël is het zowel een 9/11 als Pearl Harbor-moment. De verschrikking was een monumentale *intelligence failure* van een van de meest geroemde inlichtingengemeenschappen ter wereld. Veel Israëliërs zijn nog in shock of rouwen om de meer dan 1400 doden. Het lot van meer dan 200 gijzelaars is nog ongewis. Over de gruwelijke feiten bestaat geen twijfel – Hamas heeft de moordpartijen tenslotte zelf op video gezet. Niets kan dit rechtvaardigen. Het Israëlische recht op zelfverdediging staat buiten kijf. De daders van de wreedheden verdienen geen medelijden en krijgen deze vast niet; hopelijk wel binnen de kaders van het oorlogsrecht. Ook zal duidelijk zijn dat de Hamasstrijder en de Palestijnse burger niet tot eenzelfde categorie behoren, al is de grens in de praktijk soms moeilijk te trekken. Het conflict roept wereldwijd tegengestelde emoties op die teruggrijpen naar een complex en pijnlijk verleden, tot en met de Holocaust en de Nakba aan toe. Zuivere en diepgaande analyses zijn redelijk schaars. Zo zijn bijvoorbeeld de tv-optredens van Dominique de Villepin, een Franse topdiplomaat, een aanrader om te volgen. Het Israëlisch-Palestijns conflict blijft een mijnenveld voor analisten en columnisten, maar dreigt nu grote gevolgen te hebben voor de internationale veiligheid en stabiliteit. Het gevaar schuilt op drie vlakken.

Overreactie

Een belangrijk doel van terroristische groepen is provoceren. Zo hoopt een kleine niet-statelijke actor de veel sterkere staat uit te lokken om te overreageren. Hoe verschrikkelijker de aanslag, hoe groter de politieke druk om keihard terug te slaan: 'We zullen vuur met vuur bestrijden'. De ultieme overreactie is binnenlandse repressie/surveillance, een buitenlandbeleid gebaseerd op het predicaat 'je bent vóór of tegen ons' en een militaire strategie geënt op de totale vernietiging van de terreurbeweging. De VS heeft dit na 9/11 met zijn Global War on Terror geprobeerd; een groot succes is het niet geworden. Israël kan deze weg ook inslaan, en de voorgeschiedenis van premier Bibi Netanyahu stemt niet tot optimisme. Op tactisch niveau zal het grondgevecht in de Gazastrook een uitdaging zijn. Op strategisch niveau is het probleem nog groter. Niet alleen kan het militaire instrument Hamas niet volledig vernietigen, maar alleen al deze doelstelling kan geen politieke oplossing bieden. Deze ligt elders, namelijk bij een twee-staten-oplossing. Tot slot is Gaza maar één van drie fronten, want het is al weken onrustig in de Westelijke Jordaanoever en het is nog onduidelijk of Hezbollah zich volledig in de strijd stort (disclaimer: deze column is geschreven voordat Hassan Nasrallah zijn toespraak hield). Iran schuilt achter meerdere proxygroepen, die Israël en de VS stelselmatig uitlokken. Afgelopen jaren stond Netanyahu meermaals in de startblokken om het Iraans kernprogramma militair aan te grijpen, maar zijn commandanten hebben hem ervan kunnen weerhouden. Nu zal dit lastiger zijn. Hoe verschrikkelijk ook, terreuraanslagen betekenen meestal geen existentiële dreiging voor Israël. Een breder conflict in het Midden-Oosten mogelijk wel.

De rules-based international order

Sinds het vorige kantelpunt – 24 februari 2022, de Russische inval in Oekraïne – hebben westerse diplomaten hard gewerkt om de zogeheten Global South mee te nemen in het veroordelen van Russische agressie. De Algemene Vergadering van de VN heeft het Russisch optreden in Oekraïne meerdere keren met grote meerderheid (zo'n 150 landen) veroordeeld. De B(R)ICS hielden zich weliswaar afzijdig en een half dozijn paria's stemde met Rusland mee. Westerse landen kregen wel *pushback* tegen deze campagnes: waarom zoveel aandacht voor Oekraïne, terwijl conflicten elders al jarenlang om aandacht smeken? Nu, enkele weken na de aanslag van Hamas, is de situatie volledig gedraaid. Een Braziliaanse resolutie voor een 'humanitaire pauze' in Gaza kreeg een Amerikaans veto. Resoluties in de Algemene Vergadering voor hulp aan Palestijnse burgers werden met grote meerderheid aangenomen, maar ditmaal zaten westerse landen in het kamp van onthouders en tegenstemmers. In de Global South heerst de perceptie dat het Westen graag Russische aanvallen op Oekraïense burgers en kritische infrastructuur veroordeelt, maar wegkijkt als het om Israël en de Palestijnen gaat. Ook zeggen zij: als het internationaal recht zo belangrijk is, waarom heeft Israël dan jarenlang allerlei VN-resoluties naast zich neer kunnen leggen? Als gevolg staat het hele stelsel van de *rules-based international order* op de helling. Deze stond natuurlijk al langer onder druk, maar westerse diplomaten hoeven er nu even niet mee aan te komen in Afrika, Zuid-Amerika, het Midden-Oosten en Azië. Rusland en China spinnen er garen bij.

Verstrengelde conflicten

Het conflict in het Midden-Oosten is nauw verbonden met andere conflicthaarden, zoals Oekraïne, Iran, Noord-Korea, en Taiwan en de Zuid-Chinese Zee. In deze regio's heeft Amerikaans militair overwicht tot nu toe afschrikwekkend gewerkt en een delicaat evenwicht weten te behouden (Amerikaanse motieven en eerdere militaire avonturen hier buiten beschouwing gelaten). Dit evenwicht staat desalniettemin onder enorme spanning. Oekraïne heeft met de tegenaanval weinig eigen grondgebied kunnen bevrijden en Kyiv gaat een zware winter tegemoet. Russische oorlogsproductie overtreft westerse wapenleveringen aan Oekraïne en momenteel schreeuwt elk land in het Midden-Oosten om extra luchtverdedigingsmiddelen. Een impasse in Oekraïne is duidelijk in het voordeel van Rusland. Ondertussen hebben rond China een aantal onveilige intercepties van westerse jachtvliegtuigen plaatsgevonden en voert de VS de *freedom of navigation*-vaartochten in de Straat van Taiwan en de Zuid-Chinese Zee verder op. Vietnam en de Filipijnen worden door Beijing zwaar onder druk gezet. Noord-Korea blijft een onvoorspelbare *spoiler*. De wereld staat nog niet in brand, maar een simpel ongeluk of een militair misverstand kan alles op scherp zetten.

Conclusie

Kortom, de verschrikkingen in Israël en de Palestijnse gebieden hebben eveneens grote gevolgen elders. Westerse regeringen hebben niet de bandbreedte om meerdere crises tegelijk te blussen en de VS kan niet overal zijn militaire overmacht aanwenden. Momenteel wordt de Amerikaanse militaire aanwezigheid in het Midden-Oosten met *carrier groups* tegelijk uitgebreid en de hoop is dat deze afschrikwekkend en niet escalerend werkt. De vriendschap tussen Beijing, Moskou en Teheran is wellicht oppervlakkig, maar als zij individueel of collectief een kans zien om de VS en het Westen een hak te zetten zullen ze het niet laten. Hiernaast geven veel politieke leiders in het Midden-Oosten (en aan de Zwarte Zee) gemengde boodschappen af. Hun handelingen wijzen op een wens tot de-escalatie en behoud van de status quo, maar hun woorden gooien olie op het vuur. Hun toespraken zijn immers bedoeld voor binnenlandse consumptie, om niet uit de pas te lopen met de gevoelens op straat. Maar de wal kan zo het schip keren, zeker als het conflict lang duurt en de beelden uit Gaza de emoties verder laten oplopen. Westerse maatschappijen worstelen met antisemitisme en een latente terreurdreiging (door bijvoorbeeld al-Qaida) kan zo weer opleven. De ellende en het leed in het Midden-Oosten lijken misschien ver weg, maar het kantelmoment van oktober 2023 geldt ook voor Europa. De vraag is alleen of de lont kort of lang is. ■

The Army that got away

The 15. Armee in the summer of 1944
Door Jack Didden en Maarten Swarts
Drunen (Zwaardvisch Publishers) 2022
532 blz.
ISBN 9789080039392
€ 85,-

In veruit de meeste boeken over militaire geschiedenis gaat de aandacht uit naar oorlogshandelingen van Amerikaanse of Britse eenheden en daarbinnen exclusief naar de dunne schil van aanvallende gevechtstroepen. Dit resulteert in boekenplanken vol met titels over de Somme, Overlord en Market Garden, waaraan elk jaar titels worden toegevoegd met op de kaft de ronkende claim dat sprake is van geheel nieuwe inzichten op basis van volstrekt nieuwe bronnen.

Was het maar waar. De bovenmatige aandacht voor aanvallende geallieerden is een van de onhebbelijkheden van het genre militaire geschiedenis. Alleen al om die reden valt het toe te juichen dat er boeken verschijnen zoals die van Jack Didden (tekst) en Maarten Swarts (beeldredactie) over het Duitse vijftiende leger. *The Army that got away* beschrijft de Duitse wijze van verdedigen in de tweede helft van 1944 tegen de geallieerde opmars die plaatsvond tussen Normandië en Nederland. Het vult daarmee een lacune in de literatuur. Vrijwel alle boeken over het westfront in de Tweede Wereldoorlog springen van Overlord (juni 1944) naar Market Garden (september 1944) en Infatuate in Walcheren (november 1944) alsof er daartussen niets gebeurde. Gelukkig wordt de fascinerende tussenfase nu diepgravend bestudeerd in *The Army that got away*.

Vertragende gevechten of vlucht?
Het interessante en relevante van deze casus is dat het Duitse vijftiende leger de terugtocht overleefde. Het vijftiende leger wist veel langer weerstand te bieden dan men voor mogelijk houdt, gezien de gevechtsverhoudingen. Natuurlijk werd het zeer zwaar gesleten door de talloze confrontaties met Britten, Polen en Canadezen. Maar desondanks ontsnapte het leger, na de wekenlange terugtocht via het Albertkanaal en Walcheren, om eind 1944 opnieuw de strijd aan te gaan tegen de legers van Montgomery. Hoe kon dit Duitse vijftiende leger na negen maanden felle strijd nog steeds in staat zijn tot gecoördineerde tegenstoten en terugvallen? Of was dat misschien niet zo? Ging het wellicht om geïmproviseerde vertragende gevechten die maskeren dat het uiteindelijk toch allemaal neerkwam op een chaotische vlucht voor de geallieerde troepen uit?

Voor dat laatste lijkt veel te zeggen. Men zou goed kunnen verdedigen dat het Duitse vijftiende leger na juli 1944 langzamerhand tot militair gruis uiteenviel en overleefde door puur geluk. Uiteindelijk, zo zou de conclusie kunnen zijn, begon de geallieerde opmars bij de Belgische grens te haperen om logistieke redenen en vergat Montgomery prioriteit te geven aan de vernietiging van de restanten van het vijftiende leger. Fascinerend genoeg is Jack Didden het daarmee oneens. Zijn interpretatie is dat het Duitse vijftiende leger gedurende de terugtocht van 500 kilometer juist steeds weer opnieuw blijk gaf van opmerkelijke groepscohesie, volharding en onverminderde professionele aansturing. Ondanks voortdurend schaarser wordende middelen en een bijkans hopeloze militaire situatie brak het leger niet. Didden probeert met behulp van steeds nieuwe voorbeelden in elk hoofdstuk opnieuw aannemelijk te maken dat het Duitse vijftiende leger zich karakteriseerde door initiatiefrijkheid, improvisatievermogen, onverminderd hoog moreel en intrinsieke militaire kwaliteit en dat het daardoor in staat bleef om effectief te vechten in de moeilijke maanden tussen juli en november 1944.

Dit is een interessante these. Het ontbreekt in *The Army that got away* helaas wel aan een instrumentarium c.q. criterium voor het meten en beoordelen van die veronderstelde hoge Duitse gevechtskwaliteit en -effectiviteit. Het heeft alles te maken met de aard en opzet van *The Army that got away*. Didden opteert voor een klassieke vorm van geschiedschrijving, waarin het hoofdaccent ligt op de chronologische beschrijving. *The Army that got away* is een feitelijke en verhalende studie. Didden schreef al eerder vergelijkbare boeken, waaruit zijn voorkeur voor de beschrijvende 'eenheidsgeschiedenis' ook blijkt.[1] Niet het

vechtende individu met zijn oorlogservaring staat erin centraal, of de bredere strategische en maatschappelijke context, noch de krijgswetenschappelijke analyse, of het comparatieve perspectief, maar een legereenheid en haar 'geschiedenis'. Didden wenst, naar eigen zeggen, de *day-to-day fighting* van een eenheid in kaart te brengen. Vervolgens richt hij zich op de beoordeling van de kwaliteit van de keuzes erbij van de militaire hoofdrolspelers en de effectiviteit van het optreden van de betrokken eenheden. De optelsom van de passages daarover moet de lezer overtuigen van het gelijk van zijn interpretatie over een ongebroken Duitse gevechtskracht.

Fundgrube

De vraag dringt zich op of herhalen niet iets heel anders is dan verklaren. Maar *The Army that got away* is hierdoor in ieder geval wel een absolute *Fundgrube* geworden. Het is volledig, nauwgezet en zeer rijk aan interessante details. Het boek biedt nieuwe feiten en inzichten over een oorlogsfase die normaliter in een halve pagina wordt afgedaan. Direct na de inleiding bevat het boek boeiend onbekend materiaal over de gevechten op de oostelijke flank van Overlord. Didden komt erna te spreken over de onderbelichte gevechten bij Mantes-Gassicourt (Seinegebied) en die in de omgeving van Rouen. Vervolgens zijn de operaties rond Parijs en richting Amiens aan de beurt. Ook komt de reactie ter sprake op operatie Supercharge (Parijs, Beauvais en noordwaarts). Daarna volgen nog de gevechten in het Sommegebied rond Amiens, Arras en Cambrai, die aan de grens met België rondom Lille, in de pocket Mons, en rondom operatie Sabot (de gevechten richting Brussel). Het boek eindigt met de gevechten bij Antwerpen, de Schelde en in Zeeuws-Vlaanderen.

Didden geeft hierbij blijk van een fenomenale kennis van zaken. De orders, routes, gevechten, successen en tegenslagen tijdens de terugtocht van het vijftiende leger komen heel goed uit de verf. Bijzonder krachtig is dat alles steunt op origineel archiefonderzoek. *The Army that got away* is gebaseerd op de *Kriegstagebücher* van de deelnemende eenheden. Dit tilt het boek ver uit boven de middelmaat van de militairhistorische studies. Didden houdt verder goed greep op de materie en verliest de samenhang tussen de onderdelen van het verhaal nooit uit het oog. De fotoredactie, onder verantwoordelijkheid van Maarten Swarts, is eveneens indrukwekkend. Elke pagina biedt gemiddeld wel 3 tot 4 boeiende foto's. Hiermee is *The Army that got away* ook een prachtig kijkboek geworden. Kort en goed, *The Army that got away* is ongetwijfeld het te raadplegen boek voor wie zich wil gaan verdiepen in de oorlogsfase aan het westfront tussen de operaties in Normandië en Nederland in.

Een keerzijde is wel dat dit een boek is geworden voor de ingewijde enthousiasteling, die een kloeke feitelijk-verhalende interpretatie verkiest boven een abstractere generaliserende analyse. Het is bijna onmogelijk om niet te bezwijken onder de 500 pagina's boordenvol met feiten. Didden beseft dit zelf gelukkig ook. Met een vette knipoog erkent hij dat zijn boek het karakter heeft van 'an avalanche of facts'.

Misschien had Didden er goed aan gedaan om net iets meer ruimte te besteden aan de betekenis van alle beschreven verplaatsingen en gevechten en de koppeling van de gebeurtenissen aan de context daarvan. De vergelijking met andere Duitse terugtochten bijvoorbeeld, de connectie met de specifiek Franse situatie, of aandacht voor de pikante en veel bediscussieerde relatie tussen fascisme, indoctrinatie en 'gevechtskracht', waren op zijn plaats geweest. Legers vechten niet in een vacuüm.

Kampfgruppen

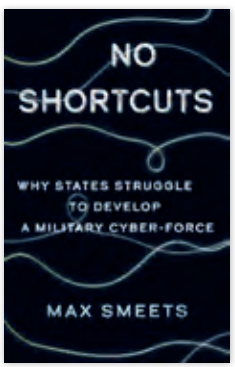
Ondertussen kent Diddens boeiende boek wel degelijk een impliciet achterliggend hoofdthema, dat in potentie alle onderdelen betekenis en samenhang zou kunnen verlenen en een verklaring zou kunnen bieden voor het voortbestaan van het vijftiende leger. Uiteindelijk vertelt *The Army that got away* het verhaal van de gevechten van *Kampfgruppen*: samengeraapte Duitse troepen onder leiding van ervaren officieren die de geallieerde opmars trachtten te vertragen. Juist deze Kampfgruppen lijken effectief te zijn geweest. Dát is een heel fascinerend gegeven. Didden heeft *The Army that got away* naar eigen zeggen geschreven als een soort voorgeschiedenis van zijn eerdere studies over Kampfgruppen zoals Chill en Walther. Nu die voorgeschiedenis klaar is zou Didden eigenlijk al zijn studies en kennis eens moeten samennemen en verknopen, en daarbij wat gas terugnemen op het vlak van feitelijke volledigheidsdrang, om meer

1 Zie bijvoorbeeld: *Einddoel Maas. De strijd in zuidelijk Nederland tussen september en december 1944* (Weesp, 1984); *Autumn Gale/Herbststurm. Kampfgruppe Chill, schwere Heeres Panzerjäger-Abteilung 559 and the German recovery in the autumn of 1944* (Drunen, 2013; eerder ook als dissertatie verschenen) en *Kampfgruppe Walther and Panzerbrigade 107. A thorn in the side of Market Garden* (Drunen, 2016).

algemenere uitspraken te doen over het karakter, de ontwikkeling en de vermeende effectiviteit van het alternatief voor de reguliere Duitse commandovoeringsstructuur en gevechtsvormen: de Kampfgruppen. Wat was de relatie precies met de formele organisatie, doctrine, militaire cultuur en *Auftragstaktik* van het Duitse leger? Waarom vochten de Kampfgruppen zo effectief?

Jack Didden is de aangewezen persoon om die vragen te beantwoorden, nu er meerdere indrukwekkende boeken van zijn hand zijn verschenen waarin Kampfgruppen het hoofdonderwerp vormen. Ik voel nóg een indrukwekkend boek aankomen.

Dr. Henk de Jong, NLDA ■



No Shortcuts

Why States Struggle to Develop a Military Cyber-Force
Door Max Smeets
Londen (Hurst) 2022
296 blz.
ISBN 9781787386877
€ 44,99

Rond 2010 zijn meerdere landen bezig met het vraagstuk 'hoe de staat te verdedigen tegen cyberdreigingen', maar ook over het zelf uitvoeren van cyberaanvallen. Maar behalve het Amerikaanse U.S. Cyber Command zijn het in die tijd vooral de inlichtingenorganisaties die zich bezighouden met operaties in cyberspace. In de daaropvolgende jaren richten veel landen separate Cyber Commando's op, zo ook Nederland – initieel met een Task Force Cyber (2012) en later in 2015 het Defensie Cyber Commando (DCC). Maar met een instellingsbeschikking, het inhuren van cybersecuritycursussen of het inschakelen van een pool aan cyberreservisten heb je nog geen offensieve cybercapaciteit; daar is een weloverwogen en zorgvuldig opgebouwd plan voor nodig. Er zijn, aldus Max Smeets in zijn recente boek, 'no shortcuts' om cybercapaciteit op te bouwen.

Aspiraties en middelen

Smeets is een Nederlandse cyberwetenschapper werkzaam bij de Eidgenössische Technische Hochschule in Zürich, directeur van het European Cyber Conflict Research Initiatief en daarnaast verbonden aan het Amerikaanse Stanford en het Britse RUSI. Smeets schreef al eerder over het DCC en ook in *No Shortcuts* is Nederland een van de casestudies. In zijn boek analyseert Smeets diverse cyber commands door statelijke cyberaspiraties af te meten aan de beschikbare middelen en de (opgelegde) operationele beperkingen (blz. 51 e.v.). Sommige landen hebben veel middelen, maar zijn mede door juridische en ethische kaders (zoals Amerika tot 2018 toen een nieuwe cyberwetgeving is aangenomen) beperkt in hun optreden.[1] Andere landen, zoals Rusland, zijn dat niet (type I). Noord-Korea (type II) laat zien dat een actor met weinig middelen nog steeds ellende kan veroorzaken als restricties niet gelden (zie figuur 1). In geval van pech zijn zowel de middelen als het raamwerk waarbinnen optreden mogelijk is beperkt: een zogeheten Paper Tiger, waar niet alleen Nederland, maar ook vele andere Europese cyber commands onder vallen.

Een staat kan enkel strategische waarde hebben ofwel een strategisch effect genereren met een cyber command als de operationele beperkingen niet te groot zijn. Dat betekent dat type III- en IV-staten dus niet in staat zijn strategische effecten te genereren (blz. 74).
Als een staat actief en effectief wil zijn in cyberspace en offensieve acties wenst uit te voeren zal hij met vijf elementen rekening moeten houden. Ten eerste personeel – voor Smeets het belangrijkste element – waarbij het niet alleen gaat om hackers, maar juist ook om taalwetenschappers, ontwikkelaars, juristen en strategen. Om effectief te zijn heeft een staat ook zogeheten *cyberexploits* nodig. Een exploit is software die gebruik kan maken van fouten in programmatuur. De

1 U.S. House of Representatives, 'John S. McCain National Defense Authorization Act (NDAA)', *Congressional Records* 164, No. 1 (2018) 1636-2423.

		Operationele beperkingen	
		Hoog	Laag
Beschikbare middelen	Hoog	Type III Gentle Giant	Type I Loose Cannon
	Laag	Type IV Paper Tiger	Type II Troublemaker

Figuur 1 Typologie cyberactoren (bron: Smeets, No Shortcuts)

exploit werkt slechts tot het moment waarop een ICT-bedrijf een software-update aanbiedt. Bij de Stuxnet-operatie in 2010 zijn (minimaal) vier exploits gebruikt. Volgens Smeets ligt er te veel nadruk op het bezit en de handel in exploits; het gaat immers om het samenspel tussen de vijf elementen en vooral het cognitieve vernuft van de menselijke gebruikers. Tools zijn – ten derde – ondersteunende softwareprogramma's die nodig zijn om een exploit uit te buiten. Veelal zijn dit bestaande programma's – of de programma's die door de opponent worden gebruikt – om onontdekt te blijven. Om een actie uit te kunnen voeren is een goede infrastructuur nodig tijdens de operatie zelf, maar bovenal in de voorbereiding ervan, denk aan een gesimuleerde internetomgeving of *cyber battlespace*. Tot slot dient de staat al deze elementen organisatorisch goed in te bedden. Een cyber command kan personeel wel werven, maar als er geen structuur is om hen te behouden, te stimuleren of te laten groeien neemt de effectiviteit snel af.

Smeets zet deze denktrant voort als hij de lezer meeneemt naar het vraagstuk over wapenhandel of het beperken van de proliferatie van cybermiddelen. De analogie met nucleaire wapenbeperking of conventionele wapenhandel gaat daarbij mank. Wat is immers 'handelswaar' in cyberspace? Smeets geeft ook hierbij aan dat het niet om 'cyberwapens' zoals payload of exploits gaat, maar om het verkrijgen en behouden van kennis en vaardigheden van cyberexperts, van mensen. Een interessante observatie is dat een offensieve actie van land A (neem Rusland) tegenover land B (Oekraïne) onbedoeld een overdracht van kennis is. Door de offensieve Russische acties sinds 2014 te analyseren komen de Oekraïners er immers achter wat de wijze van optreden en gebruikte vaardigheden zijn, waardoor het defensief in te richten is; een van de oorzaken van de sterke Oekraïense cyberdefensie op dit moment.

Papieren tijger DCC

Wetenschappelijke literatuur over (activiteiten in) cyberspace grijpt vaak terug op bestaande theorie uit het recht, internationale betrekkingen of bestuurskunde. Smeets doet een zeer verdienstelijke aanzet tot theorievorming vanuit cyberspace zelf; sterker nog, hij laat met zijn denken over het overdragen van kennis en vaardigheden zien dat het klakkeloos overnemen van denkbeelden uit de fysieke wereld eerder een valkuil dan een uitkomst is. Alleen al hierom is *No Shortcuts* een lezenswaardig boek. Maar wat het voor Nederland nog interessanter maakt is dat Smeets de Nederlandse case (inclusief het DCC) gebruikt in zijn vergelijkende onderzoek naar capaciteiten en beperkingen van landen, daar waar de focus toch vaak op de VS, Rusland, China of Noord-Korea ligt. Smeets geeft in zijn onderzoek aan dat cyberspace geen *level playing field* is. De cyberpikorde in staten wordt bepaald door beschikbare middelen, maar ook door de aanwezigheid van of het gemis aan een strategische visie, operationele capaciteiten en bovenal door al dan niet zelfopgelegde juridische en ethische beperkingen. Zo ook voor het DCC, want dat heeft een taak toegewezen gekregen tijdens het (gewapende) conflict. Dit mandaat staat in schril contrast tot de beperkingen buiten dat conflict. Smeets legt hier de vinger op de zere plek: het DCC kan en mag zich niet voorbereiden op een inzet omdat er buiten het (gewapende) conflict geen juridisch raamwerk is. Het DCC kan in de gereedstellingsfase niet oefenen en geen mensen stimuleren en uitdagen. Combineren we dit met Smeets' argument dat mensen de primaire kracht van een cyber command zijn, dan heeft het DCC geen mogelijkheden om personeel te behouden, en zonder opgeleid en gemotiveerd personeel blijft het commando een papieren tijger.

Kol dr. Peter Pijpers, NLDA ■

‘Het gebruik van micro-organismen voor oorlogsdoeleinden’

Wiperware kan onder bepaalde omstandigheden en voorwaarden een nuttig hulpmiddel zijn in de Nederlandse militaire gereedschapskist, is te lezen in deze editie van de *Militaire Spectator*. In 1954 maakte men zich druk om een ander type virus – als onderdeel van biologische oorlogvoering.[1] Majoor der Infanterie G.K. Fraay lichtte in dat jaar de zogeheten ABC-oorlogvoering toe (Atomisch, Biologisch en Chemisch), waarbij vooral voor de ‘B’ nieuwe mogelijkheden aandacht verdienden door moderne techniek en wetenschap.

Biologische oorlogvoering is, schrijft Fraay, ‘de oorlogvoering, die gebruik maakt van micro-organismen of hun afgescheiden stoffen, met het doel zoveel mogelijk vijanden uit te schakelen, gewassen te vernietigen en de veestapel aan te tasten.’ Dit is dus niet per se gericht tegen materieel en daardoor ‘Een belangrijk verschil met de explosieve middelen waarmee de oorlog in het algemeen wordt gevoerd.’

Na een korte introductie over internationale verdragen rond biologische oorlogvoering gaat Fraay in op de geschiedenis van dit type wapen. Er zijn gevallen bekend van met kadavers vergiftigde waterbronnen in de oudheid en besmettelijke ziekten in de middeleeuwen. ‘In hoeverre daarbij echter biologische strijdmiddelen opzettelijk werden toegepast, is hier slecht te beoordelen’, aldus Fraay. Hij noemt een bekend voorbeeld waarbij een biologisch wapen wel opzettelijk werd toegepast: ‘toen een Engels generaal in de strijd tegen de Indianen in Noord-Amerika aan deze met gulle hand dekens liet verstrekken, waarin nog kort tevoren pokkenpatiënten hadden gelegen. Het succes was groot, want de Indianen bleken weinig

FOTO BEELDBANK NIMH

Rijdende artillerie in linieformatie. De paarden van de tegenstander vormden een interessant doelwit voor biologische oorlogvoering

FOTO BEELDBANK NIMH

Militairen van de Kader School Infanterie oefenen in beschermende kleding met gasmasker in het opsporen en herkennen van ABC-strijdmiddelen (Atomisch, Biologisch, Chemisch). Volgens Fraay was Nederland in staat snel ABC-gevaar te bestrijden

weerstand tegen deze ziekte te hebben en stierven in groten getale.'

In de Eerste Wereldoorlog waren Duitse pogingen tot biologische oorlogvoering vooral gericht tegen de paarden van de tegenstander, maar met weinig succes. Het Japanse leger probeerde in de Tweede Wereldoorlog met een omslachtig plan zelfs de builenpest op China los te laten: 'Door middel van vliegtuigen verspreidden zij besmette rijst, die bij ratten builenpest veroorzaakte en bij de mens dezelfde ziekte teweegbracht.' Maar: 'Ook hier slechts een gering resultaat', schrijft Fraay.

Wat betekende dit nu voor de Nederlandse krijgsmacht? Fraay: 'Hoewel toepassingen in het verleden weinig of geen succes hebben gehad, sluit dit niet in, dat in de toekomst weinig of geen waarde aan dit strijdmiddel mag worden gehecht. (…) In geen geval mag de grote psychologische invloed van het gebruik van deze middelen worden onderschat, zeker niet, wanneer in vredestijd de nodige maatregelen ter bestrijding ervan niet zijn genomen, waardoor de strijdkrachten en de burgerbevolking onvoorbereid daaraan zouden worden blootgesteld.'

'Niet elke willekeurige ziekteverwekkende bacterie, virus of schimmel is echter als strijdmiddel te gebruiken', dus Fraay noemt een aantal eisen aan biologische strijdmiddelen, zoals ziektes die moeilijk te identificeren en bestrijden zijn en een hoge mate van besmettelijkheid hebben. Via een aantal 'maatregelen tegen biologische gevaren' komt Fraay tot zijn conclusie: 'De biologische oorlogvoering leent zich meer voor strategisch dan voor tactisch gebruik. Reeds in vredestijd kunnen vele maatregelen worden genomen om de gevaren van biologische strijdmiddelen te voorkomen.'

Fraay besluit met een optimistische constatering ten aanzien van de potentieel verschrikkelijke uitwerking van biologische oorlogvoering: 'Op grond van de ervaringen in het bestrijden van besmettelijke ziekten in de laatste jaren opgedaan, kan worden vastgesteld, dat Nederland in staat is, snel het gevaar te bestrijden.' ■

1 G.K. Fraay, 'De ABC-oorlogvoering', *Militaire Spectator* 123 (1954) (5). Zie: https://militairespectator.nl/sites/default/files/bestanden/uitgaven/MS%201954-05.pdf.

Civil defence in Sweden: building resilience by involving society as a whole

Interview with Carl-Oskar Bohlin and Johan Berggren

Annelies van Vark and Huib Zijderveld*

Times are changing. After decades of peace in Europe war is now back on the continent, stimulating European states to reconsider the role of their armed forces. Investments in the armed forces are on the rise and focus is shifting from stability operations towards the original core task of the armed forces: the defence of (allied) territory. In the Dutch defence and security discourse, terms like 'whole of society' and 'resilience' are increasingly used, often accompanied by a reference to the Nordic countries. But what does a 'whole of society' approach mean and why do we need it? And how can we increase resilience in society? To find out, civil-military relations researchers visited Sweden and spoke with Minister of Civil Defence Carl-Oskar Bohlin and his State Secretary Johan Berggren.

Civil defence and resilience

The new Swedish government that came into office in the Fall of 2022 decided to strengthen the civilian components of total defence and to appoint a special minister of civil defence at the Ministry of Defence. What is civil defence and why and how is Sweden working to strengthen it?

Hosting us at the Ministry of Defence, Carl-Oskar Bohlin is visibly passionate about his work and convinced of its necessity. He explains that 'the essence of civil defence is basically to get the whole of society to line up behind the effort of providing resistance against an antagonist or an aggressor', with the aim of 'securing the existence of the Swedish state'. The concept is in that sense basically the same as the one that was used during the Cold War: to make sure that in case of an armed assault resistance and resilience in all layers of society is high, and that the whole society is committed to helping the military defence to solve its tasks. Bohlin further explains that 'resilience is about the will and the ability to resist armed aggression'. He points at Ukraine, which since the first invasion in 2014 has started to build up its civil defence and has proven to be successful during the second invasion and the war that is still going on today. As Bohlin points out, 'They have been able to keep their electricity going while it has been under attack, while it has been a clear Russian aim to break the backbone of Ukrainian society by attacking the civil part of society.' At the

* Annelies van Vark is Senior coordinating adviser at the Transition Team, Defence Staff and PhD candidate at Leiden University. Captain Huib Zijderveld is a PhD candidate at the Netherlands Defence Academy and Free University Amsterdam.

The Swedish Home Guard exercises in Ystad PHOTO JONN LEFFMANN

same time, 'resilience has kept up the will to resist among the public of Ukraine.'

Security of supply

Johan Berggren adds, explaining that sustainability is important in that context, as 'it's not enough to be able to deal with something complicated or challenging for a few days or weeks, it (the war) goes on for a long time'. That goes for military defence as well, and an important part of the work being done at the ministry now is about how to achieve security of supply, for which cooperation with the private sector is essential. Bohlin explains: 'I would say there is not one task within the military or in civil defence that can be maintained without the help or the participation of private entities.' He is not only talking about building stockpiles, but also about the possibilities to redirect production, which is not only important in times of war, but also during crises other than war, such as disasters and complex emergencies. The COVID-19 pandemic is an example that immediately comes to mind. During that time production was redirected 'almost organically', to produce masks or sanitation equipment for example, but 'it needs to be more institutionalized, so that we have a preparedness for that in advance.'

Sense of urgency

An essential precondition to rebuild civil defence is a sense of urgency in society. Bohlin sees ample evidence in Swedish society for a growing sense of urgency, indicated for example by an increased will to defend Sweden in the general population and by a very large influx of volunteers into the voluntary defence organizations Sweden has. He explains that the government has been actively pushing this sense of urgency, 'since we find ourselves in a very dire security situation, in which we don't know what lies around the corner. We don't know where the endgame in this might take us.' He does not foresee a situation in which the current situation will go away and go back to prior 2014, or 2008. In addition Berggren explains that Sweden's geographical situation is very different from that of the Netherlands or countries further southwest: 'Sweden is where it is, and we have always lived under the shadow of the East.'

What can a country like the Netherlands, where the sense of urgency is at a much lower level, learn from Sweden in this respect? Bohlin is very clear on this issue: 'We need to prepare ourselves for a worse scenario than we are finding ourselves in right now. And that is a concern for every European country I would say.' Berggren

'Willingness to fight for your country (percentages)'					
	Denmark	Finland	Netherlands	Norway	Sweden
Yes	74.6	74.8	46.7	87.6	80.5
No	23.3	18.3	40.9	10.4	15.6
Does not know	2.0	6.2	11.8	1.9	3.0
No answer	0.1	0.7	0.6	0.1	0.9

Survey 'Willingness to fight for your country', C. Haerpfer, R. Inglehart, A. Moreno, C. Welzel, K. Kizilova, J. Diez-Medrano, M. Lagos, P. Norris, E. Ponarin, and B. Puranen (Eds.), World Values Survey: Round Seven - Country-Pooled Datafile. Madrid, Spain & Vienna, Austria: JD Systems Institute & WVSA Secretariat (2020).

continues by saying: 'Geographically, the Netherlands may be far away from the front lines, but in modern days geography matters less.' One can think about cyber sabotage, espionage, or other grey zone threats. Not to forget the port of Rotterdam: 'I believe Rotterdam is the biggest port in Europe and would be a key point of entry for reinforcements into Western Europe', which would make it a target for an aggressor.

Conscription and voluntary defence

As part of the effort to rebuild civil defence, Sweden has decided to reactivate conscription, starting with 4,000 conscripts per year in 2018, and expanding the total number of conscripts to 8,000 in 2025, including both men and women. The whole cohort receives a call-up letter when they are 18 and are obliged to fill out a digital form. Based on their qualifications and motivation, around 20,000 young people are invited for a medical check-up and two days of briefings, after which the final selection takes place.

As the numbers of draftees are (still) relatively low at around 10 per cent of the cohort, the Swedes are selective in their recruitment procedures, only allowing the most capable and motivated to serve, as Johan Berggren explains. After fulfilling their conscription, former conscripts are placed in a reserve unit for 10 years and can be called up to serve in case of a state of high alert.[1]

An important ambition for Carl-Oskar Bohlin is to establish civil conscription as a complement to military conscription, starting in the sector of the rescue services, which are a municipal responsibility. He explains: 'The experiences from Ukraine show the enormous amount of stress that the rescue services are under in terms of equipment requirements, personnel and new tasks.' What comes to mind is, for example, clearing unexploded ammunition and recovering people from collapsed buildings. This makes the rescue services the logical starting point for the establishment of civil conscription. An enquiry is currently underway, looking at other sectors where civil conscription would be useful, 'similar to what we had during the Cold War, when we had civil conscription for people working with power lines, and in health care, functions that need extra support during an assault.'

By preparing for the worst (an armed attack on Sweden) the country is also better prepared for disasters and complex emergencies. In addition to government organizations, voluntary defence organizations play an important role. Bohlin explains that voluntary defence organizations get government funding to fulfil certain tasks during a peacetime crisis but also during high alert or an armed assault. Around 350,000 Swedes are members of such a voluntary defence organization and usually they are connected to

1 If the Swedish government judges that Sweden is at war, or that war is imminent, it can declare a 'state of high alert'. During a 'state of high alert' the government's powers increase and there are a set of pre-prepared laws that ensure that Sweden can secure its needs for resources and personnel, amongst other things.

Total defence in Sweden

The Swedish model for total defence emerged during the Second World War, when an expert commission concluded that the boundaries between the military and the civil domain had been erased and war had become total. This called for total defence, including both a military and a civil component.[1] The model consisted of four elements, namely military defence, economic defence (including storage and supply of key provisions), psychological defence (including countering disinformation), and civil defence (including shelters, evacuation planning, et cetera). The whole population was in fact involved in preparing for the eventuality of a war. During the Cold War, Sweden had conscription for males and could mobilize up to 850,000 men.

Until the 1980s total defence had only been focussed on a possible external invasion. Starting in the mid-1980s experts began to point at possible threats from within the country itself. However, it was not until the early 2000s that the threat of an invasion was more or less written off, and was replaced by threats such as asymmetrical attacks, major accidents and natural disasters.[2] These security problems did not necessarily lie in the domain of the armed forces.[3] This marked the beginning of a 'strategic timeout' for the traditional total defence model and a downsizing of the Swedish armed forces. The defence budget shrank from approximately 2 per cent of GDP in 1990 to approximately 1 per cent in 2010 and the conscript system was replaced by an all-volunteer force in the 2009 defence bill.[4] In this period, a new term entered the security discourse: 'societal security'.

In the 2010s a new shift took place. With the changing geopolitical situation and the rising Russian threat, Sweden again began to increase its military capabilities. On 15 December 2020 the Total Defence Bill 2021-2025 was approved by the Riksdag. Total defence is designed to be able to counter an armed attack against Sweden. The starting point is that Sweden should be able to survive during a security crisis in Europe causing disruptions to society as well as during actual war for a period of time, at least three months. Important measures in the bill are the strengthening of both civil and military defence, including a substantial budget and personnel increase, increase of conscription volumes, and the strengthening of cyber defence. In 2022 a new Psychological Defence Agency (MPF) was created, mainly aimed at identifying, analysing, and countering foreign influence operations and disinformation taking place on social media, for example.

The new Swedish government, installed in the Fall of 2022, decided to move both MPF and the Swedish Civil Contingencies Agency (MSB) from the Ministry of the Interior to the Ministry of Defence, under the coordination of the new Minister of Civil Defence, in an effort to strengthen the civilian components of total defence, more specifically, civilian defence and crisis preparedness.[5]

As part of the reinstatement of total defence, the national defence courses that Sweden organized during the Cold War have been reinvigorated as well. These courses are organized at different levels (e.g. middle and senior management) and aim to bring people from different backgrounds (government, private sector, NGOs, et cetera) together to learn about national security. During the Cold War, the courses concerned total defence issues but recently they have been expanded to include crisis management.

1 S. Larsson, 'Swedish total defence and the emergence of societal security', in S. Larsson and M. Rhinard (Eds.), *Nordic societal security; convergence and divergence* (Routledge, 2021).
2 Larsson, 'Swedish total defence and the emergence of societal security'.
3 J. Stiglund, 'Threats, risks, and the (re)turn to territorial security policies in Sweden', in S. Larsson and M. Rhinard (Eds.), *Nordic societal security; convergence and divergence* (Routledge, 2021).
4 O. Kronvall and M. Petersson, 'Doctrine and Defence Transformation in Norway and Sweden', *Journal of Strategic Studies* 39 (2016) (2) 280-296.
5 U. Kristersson, *Statement of Government Policy*, (2022). See: https://www.government.se/speeches/2022/10/statement-of-government-policy/.

PHOTO GOVERNMENT OFFICES OF SWEDEN, TOM SAMUELSSON

Minister of Civil Defence Carl-Oskar Bohlin (right) and his State Secretary Johan Berggren

different municipalities and have arrangements to assist during peacetime crises. As these voluntary defence organizations were never abolished or scaled down, 'they have the institutional memory of Swedish civil defence from before.'

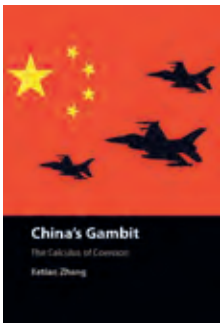
Domestic role of the armed forces

The main purpose of civil defence is to funnel all of society's efforts into one direction: to protect the Swedish state from an armed aggressor. However, in peacetime the armed forces can support civilian authorities as well. An important principle in the Swedish governance model is the responsibility principle, 'which means that the agency or actor that has the responsibility for a task during peacetime, also has that responsibility during crisis or ultimately war, with some exceptions.' Bohlin illustrates this with an example from the rescue services, which are primarily responsible in case of an earthquake or a flood, for example, but can escalate up the chain, if necessary. 'Ultimately, the state can also ask for military assistance to provide resources to help out in a peacetime crisis.' The armed forces can in that sense be seen as the last resort in case of civil crises and can provide assistance when needed. On the other hand, he explains, 'in the event of an armed assault or attack on Sweden, all of civil society is then committed to support the military defence to carry out its task.'

Lessons learned

What is the main lesson the Netherlands can learn from the Swedish system for civil defence? Referring to the low popular commitment to defend the Netherlands, Bohlin is very clear: 'Getting the whole of society involved raises awareness about what is the ultimate task that needs to be carried out. Resilience and resistance start with your own personal preparedness and your own will to defend.' A holistic approach involving the whole of society may eventually lead to a higher will to defend as well 'because it comes closer to every citizen. It is not only the people in uniform who are carrying out the total defence effort, it is every individual within society that has to feel engaged when doing that.' ■

SIGNALERINGEN



China's Gambit

The Calculus of Coercion
Door Ketian Zhang
Cambridge (Cambridge University Press) 2023
226 blz.
ISBN 9781009423816
€ 95,-

Wanneer maakt China gebruik van *coercion* in zijn buitenlandse politiek? Die vraag onderzoekt Ketian Zhang, universitair hoofddocent internationale veiligheidsstudies aan George Mason University, in haar boek *China's Gambit*. Zhang keek onder meer naar de relaties met Taiwan, Tibet en Japan (Zuid-Chinese Zee) en stelde vast dat China sinds 1990 selectief naar coercion gegrepen heeft als antwoord op gepercipieerde dreigingen voor de nationale veiligheid. De auteur stelt vast dat China vooral niet-militaire middelen gebruikt om andere landen zijn wil op te leggen. Zhang plaatst haar onderzoek tegen de achtergrond van de groeiende economische belangen die China heeft in verschillende delen van de wereld.

NATO and the Russian War in Ukraine

Strategic Integration and Military Interoperability
Door Janne Haaland Matlary en Rob Johnson (red.) Londen (Hurst) 2024
264 blz.
ISBN 9781911723141
€ 51,-

Met de val van de Sovjet-Unie viel de directe dreiging voor de NAVO weg; de alliantie verwelkomde nieuwe lidstaten en ging zich concentreren op *out-of-area* operaties. De NAVO heeft daarvoor een hoge prijs betaald op het vlak van strategische integratie en interoperabiliteit, zeggen auteurs in de bundel *NATO and the Russian War in Ukraine*. Ontwikkelingen in operabiliteit hebben slechts beperkt plaatsgevonden in het lucht- en maritieme domein en pas bij de Russische annexatie van de Krim in 2014, maar vooral na de Russische invasie van Oekraïne in 2022, gingen op het NAVO-hoofdkwartier alarmbellen af. De auteurs betrekken ook China in hun casestudies.

Women in Intelligence

The Hidden History of Two World Wars
Door Helen Fry
New Haven (Yale University Press) 2023
464 blz.
ISBN 9780300260779
€ 40,-

Op basis van nog niet eerder gebruikt archiefmateriaal concludeert Helen Fry in *Women in Intelligence* dat Britse vrouwen tijdens de Eerste en Tweede Wereldoorlog cruciaal werk leverden voor de inlichtingendiensten, ook in leidinggevende functies, en daarmee ingingen tegen de conventies van die tijd. Fry, gespecialiseerd in inlichtingengeschiedenis, beschrijft vrouwen die spionnennetwerken of ontsnappingsroutes leidden, achter de vijandelijke linies werden gedropt of verantwoordelijk waren voor het ondervragen van gevangenen. Het ging daarbij niet alleen om vrouwen die dienst hadden genomen, maar ook om vrouwen die als burger meewerkten aan het coderen van boodschappen of andere operaties van de inlichtingendiensten tegen de asmogendheden.

The Korean War Remembered

Contested Memories of an Unended Conflict
Door Michael J. Devine
Lincoln (University of Nebraska Press) 2023
346 blz.
ISBN 9781496234698
€ 61,-

Michael Devine onderzoekt in *The Korean War Remembered* vanuit internationaal perspectief hoe de beeldvorming rond de oorlog en het daarop volgende bestand in vier betrokken landen is bepaald. Devine gebruikt de term *theaters of memory* om te kijken hoe het conflict in Noord- en Zuid-Korea, de VS en China verwerkt is in literatuur, populaire cultuur, onderwijs, monumenten en musea. In de decennia na de oorlog van 1950-1953, met constante spanningen rond de gedemilitariseerde zone tussen de Korea's, pasten de landen de beeldvorming meermaals aan voor doelen in de binnenlandse en buitenlandse politiek. Devine kijkt ook naar eventuele parallellen met de Vietnamoorlog.


ERVAL