

MILITAIRE SPECTATOR

MINDER FOSSIELE BRANDSTOFFEN: INNOVATIE VEREIST

- Mensen, materieel en financiën bij Defensie
- Turkije en de NAVO
- Cyber-enabled Influence Operations
- Report: 'Maybe Russia cannot be deterred'



FOTO US ARMY, RICHARD LUTZ



In *Militaire Spectator* 7/8-2023 verschijnt onder meer: 'Assad or we Burn the Country'. Siege Warfare in the Syrian Civil War' van Luuk van den Boomen.

Siege warfare has been the defining feature of the Syrian Civil War. Several 'rebellious' towns, cities and neighbourhoods were under long-term siege between 2013 and 2018, most notably Dara, Homs, Hama, Aleppo, and various neighbourhoods on the outskirts of Damascus.

The grim logic of sieges is simple. If you deny your foe food and medicine, eventually,

they lose the physical and mental capability to fight. Sieges typically combine two key elements: encirclement of an area for the purpose of isolating it, and bombardment. Throughout the conflict, the Syrian regime has successfully exploited siege tactics at the core of its counterinsurgency campaign. Through deliberate and methodical siege tactics, the Syrian regime was able to quell the revolt and gradually capture and regain opposition-held territory. But what exactly is the logic of siege warfare as counterinsurgency, and how was it put into practice by the Syrian regime and its allies? ■

SYMPOSIUM HYPERWAR KVBK

De KVBK organiseert op dinsdag 3 oktober in Den Haag een symposium over hyperwar. Deskundigen kijken naar strategische, technische en ethische vraagstukken rond deze manier van oorlogvoeren.

Meer informatie volgt binnenkort op de website www.kvbk.nl.



Oekraïne: en hoe nu verder?

Met de Russische invasie op 24 februari 2022 intensiverde het conflict in Oekraïne, dat al met de inname van de Krim in 2014 was begonnen. Hopelijk zal deze oorlog een keer stoppen. De vraag is: en wat dan?

Het is contra-intuïtief om tijdens een gewapend conflict al na te denken over de *post-war* periode. De overwegingen en afwegingen die strijdende partijen tijdens het conflict maken zijn onvermijdelijk ingegeven door emoties als woede en angst. De partijen in het conflict ontmenselijken de tegenstander,¹ en vereenzelvigen leiders, militairen en bevolking.

Toch moeten onze strategische denkers stilstaan bij de fase na de oorlog. Bij strategie gaat het immers niet om individuele emoties of persoonlijke belangen, maar om de verschuiving in de relatieve verdeling van macht en invloed tussen (niet-)statelijke actoren ten gunste van de actor die de strategie uitvoert.

Dit conflict op het Europese continent is meer dan oorlog tussen twee staten. Ook de NAVO, EU-lidstaten, China en Iran spelen een rol, net als internationale organisaties, bedrijven of sympathisanten. Naast een scala aan actoren woedt 'de oorlog' ook op een veelheid aan terreinen: gas, graan, wapenverdragen en uitbuiting van strijdige interpretaties van het internationale recht.

Na de oorlog zullen we de relatie met Rusland wel weer op moeten pakken. Dit is immers de oorlog van president Vladimir Poetin en zijn handlangers, en niet *per se* van het Russische volk. Een vereenzelving die begrijpelijk is, maar ook gevaarlijk. De valkuil is dat wij ons laten inpalmen door onze eigen wraakgevoelens jegens Rusland, waarmee een 'Versailles 2.0' in de maak is.

Het is dus zaak om nu al, tijdens deze oorlog, na te denken over de toekomst. Hoe dan? Tonen wij ons empathisch naar Rusland? Rusland voelt zich kwetsbaar en om die gepercipieerde dreiging tegen te gaan heeft het behoefte aan strategische diepte en bufferzones. Daarnaast voelt Rusland zich miskend als grootmacht. Houden we rekening met de Russische perceptie, met daarbij de vraag hoe reëel die eigenlijk is? Of volharden we in onze eigen principes, waaronder het internationale recht, dat Rusland zo flagrant heeft geschonden?

Lastig? Dat valt best mee. Meedeinen met autoritaire leiders is geen optie; sterker nog, wij moeten niet langer zelfgenoegzaam in vrede leven,² maar accepteren dat in vrede leven constante actie vereist. De enige uitdaging die rest is om onze oorlogse emoties in te ruilen voor strategisch denken. Want als we onze wraakgevoelens laten prevaleren dan zal de vrede een voorzetting van de oorlog met andere middelen zijn: een fout die we een dikke eeuw geleden ook al hebben gemaakt. ■

1 Timothy Snyder, 'Ukraine Holds the Future. The War Between Democracy and Nihilism', *Foreign Affairs*, 6 september 2022.

2 Ervin Staub, 'The psychology of bystanders, perpetrators, and heroic helpers', in: Ervin Staub, *The Psychology of Good and Evil. Why Children, Adults, and Groups Help and Harm Others* (Cambridge, Cambridge University Press, 2003) 291-324.

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

Igen b.d. ir. R.G. Tieskens (hoofdredacteur)
drs. A. Alta
kol Marns drs. G.F. Booij EMSD
ltkol drs. 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
drs. R. de Winter

BUREAU-REDACTIE

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: Zr. Ms. Zeven Provinciën
vaart de haven van New York binnen,
oktober 2022

Foto: MCD, Aaron Zwaal



FOTO: MCD, HERMAN ZONDERLAND

Minder fossiele brandstoffen gebruiken vraagt technische en militaire innovatie

Marcel Hendriks Vettehen

Het heeft er alle schijn van dat Defensie geen serieus werk maakt van de eigen doelstelling om in 2050 70 procent minder fossiele brandstoffen te gebruiken.

Essay: Waarom de NAVO niet zonder Turkije kan

Niels van de Ven

Tegenstanders van het Turkse NAVO-lidmaatschap gebruiken normatieve argumenten, terwijl voorstanders militaire en geopolitieke standpunten innemen.



Cyber-enabled Influence Operations

Peter Schrijver and Paul Ducheine

The case of the Belarusian Cyber Partisans shows that conceptual frameworks for analyzing operations in cyberspace are not universally applicable.

Mensen, materieel en financiën bij Defensie

Tine Molendijk en Robert Bertrand

Bedrijfskundig academisch onderzoek van het Research Centre Military Management Studies draagt bij aan duurzame investeringen in mensen en middelen bij Defensie.

EN VERDER

EDITORIAAL	Oekraïne: en hoe nu verder?	273
VERSLAG	'Maybe Russia cannot be deterred'	307
TEGENWICHT	Vertrouwen	318
COLUMN SERGEI BOEKE	Train the trainer: leren van de Oekraïners	320
BOEKEN	<i>The Road Less Traveled</i>	322
RETROSPECTATOR	'Zekerheidsneurose mag niet leiden tot pietepouterige controle op alle details'	324

Minder fossiele brandstoffen gebruiken vraagt technische en militaire innovatie

M.G.M. Hendriks Vettehen*

Europa moet klimaatneutraal worden en Defensie wil in 2050 zeventig procent minder afhankelijk zijn van fossiele brandstoffen ten opzichte van 2010. Hoe dat moet weet niemand, maar de tijd dringt; Defensie investeert immers in wapensystemen die dertig jaar mee gaan. Tegelijkertijd moet het behoud van de gevechtskracht voorop blijven staan. Defensie moet ingrijpend veranderen om beide doelstellingen – terugdringen gebruik fossiele brandstoffen en handhaven gevechtskracht – mogelijk te maken. Daar is niet alleen technische innovatie voor nodig, maar vooral ook militaire vernieuwing. Dit artikel geeft daartoe een aanzet.

Defensie heeft als doelstelling in 2030 twintig procent minder afhankelijk te zijn van fossiele brandstoffen, en in 2050 zeventig procent minder dan in 2010.¹ Aanvankelijk alleen om bij te dragen aan de nationale inspanningen om klimaatverandering tegen te gaan, maar nu ook ingegeven door zorgen over energiezekerheid.² Dat is actueel nu Rusland olie en gas inzet om de Europese steun aan Oekraïne te ondermijnen, maar concreet is er tot nu toe nog weinig bereikt.

Dat is op zich niet zo verwonderlijk, want net zo min dat we ons een klimaatneutraal Europa kunnen voorstellen in 2050, kunnen we ons voorstellen hoe de krijgsmacht zijn werk kan doen met slechts dertig procent van de diesel, kerosine en scheepsbrandstof die nu wordt gebruikt. En waar halen we die brandstoffen vandaan, als ze door de rest in de ban zijn gedaan? Wat is er operationeel en technisch-

* M.G.M. Hendriks Vettehen is kapitein-ter-zee van de technische dienst (b.d.).

1 'Defensie Energie en Omgevingsstrategie', Tweede Kamer vergaderjaar 2019-2020, 33 763, nr. 152.

2 Ministerie van Defensie, 'Nieuwe Energie in de Organisatie', juli 2020.

Prototype van een hybride quad. Defensie heeft als doelstelling in 2030 twintig procent en in 2050 zeventig procent minder afhankelijk te zijn van fossiele brandstoffen ten opzichte van 2010

FOTO MCD, PAUL TOLENAAR



logistiek mogelijk? Voor welke ingrepen staat Defensie?

Dit artikel maakt onder andere gebruik van het HCSS-rapport 'Lessen uit het Landgevecht'.³ Soms sluiten de bevindingen aan bij wat er nodig is om '2050' mogelijk te maken, soms wringt het.

Koninklijke Marine

Fregatten

Het grootste deel van de scheepsbrandstof, 26 procent van het totaal van de door Defensie gebruikte brandstof,⁴ wordt gebruikt door fregatten.

In 2050 is de maritieme tijd-afstand-nexus nog te complex om op grote schaal onbemande oorlogsschepen in te zetten. De marine heeft daarom nog steeds bemande fregatten voor wereldwijde inzet. Bijna alle alternatieve niet-fossiele brandstoffen zijn echter minder geschikt of zelfs ongeschikt: ze hebben méér bunkercapaciteit nodig en ze zijn giftiger en/of gevaarlijker dan de huidige brandstoffen. Biobrandstoffen zijn als 'drop-in-fuels' gelukkig wel geschikt, maar de beschikbaarheid zal beperkt zijn wanneer de mobiliteitssector daar 'en masse' op overgaat. Nucleaire voorstuwing is mogelijk maar voor een relatief kleine marine vooralsnog financieel en organisatorisch onhaalbaar; dit kan hooguit in samenwerking met bondgenoten.

Kunnen toekomstige fregatten substantieel bijdragen aan het terugdringen van het gebruik van fossiele brandstoffen? Ja, maar dan moet de maximale vaart terug naar 20 knopen en moet de trendmatige groei van de waterverplaatsing worden gekeerd. Een S-fregat verplaatste in de

jaren tachtig nog 3.500 ton, tegenwoordig is dat bijna het dubbele. Een aanzienlijk lagere maximale vaart opent ook de mogelijkheid om met één schroef te varen, in plaats van twee zoals nu gebruikelijk is. Dit is eventueel aan te vullen met een elektrisch in- en uitschuifbaar 'thuiscomfortje'.

Gaan dat soort veranderingen de inzet raken? Geleide wapens zijn tegenwoordig zo snel en accuraat en hebben zoveel reikwijdte dat 'hoge vaart' relatief weinig toevoegt. Fregatten hoeven in principe niet veel harder te kunnen varen dan het bevoorradingsschip waarvan ze afhankelijk zijn. Daar waar het de inzet toch zou kunnen raken, moet gezocht worden naar sensoren, wapensystemen en andere wijzen van opereren, om die 'delta' te overbruggen.

Amfibische schepen

Het HCSS-rapport 'Lessen uit het landgevecht' heeft ook een interessante observatie over amfibisch optreden. De ondergang van de Russische kruiser Moskva heeft aangetoond hoe kwetsbaar onder de kust varende schepen zijn voor vanaf het land afgevuurde raketten. Dat geldt qualitate qua ook voor het gebruik van Nederlandse LPD's zoals de Zr.Ms. Rotterdam en Zr.Ms. Johan de Witt. Defensie denkt daarom ook na over een nieuw type schip dat de beide amfibische schepen en de vier patrouilleschepen moet combineren.⁵ Wat de gevolgen zijn voor het brandstofverbruik van de vloot is op dit moment moeilijk in te schatten.

Koninklijke Luchtmacht

De luchtmacht is met 59 procent veruit de grootste gebruiker van fossiele brandstoffen. Dat zal de komende jaren eerder toe- dan afnemen. De F-35 verbruikt immers ongeveer 1,6 keer meer brandstof dan zijn voorganger, de F-16.⁶ Als er één krijgsmachtdeel moet bijdragen aan de doelstelling 2050, dan is het de luchtmacht. Waar liggen mogelijkheden?

Het HCSS-rapport wijst op de sleutelrol van de grondgebonden luchtverdediging waarmee vliegtuigen en drones tot op zeer grote hoogtes

³ Frederik Mertens et al, 'Lessen uit het Landgevecht. Eén jaar oorlog in Oekraïne', HCSS, januari 2023.

⁴ Ministerie van Defensie, 'Roadmap Energiëtransitie, operationeel materieel', januari 2023.

⁵ Ministerie van Defensie, *Defensienota 2022*, juni 2022.

⁶ 'Forsvarets nye jagerfly vil øke utslippene med 207 prosent', *Dagavisen*, 15 oktober 2019.



Apaches worden volgetankt. De luchtmacht is de grootste gebruiker van fossiele brandstof: waar liggen mogelijkheden?

FOTO MCD, SJOERD HILCKMANN

het luchtruim wordt ontzegd. Het rapport wijst natuurlijk ook op de opvallende en succesvolle wijze waarop drones worden ingezet. Hoe kunnen deze ontwikkelingen bijdragen aan de noodzaak veel minder kerosine te gebruiken en tegelijkertijd de gevechtskracht waarborgen?

Jachtvliegtuigen

Moderne jachtvliegtuigen gebruiken grote hoeveelheden brandstof. Zo gebruikt de F-35 op uurbasis gemiddeld drie keer méér brandstof dan een fregat.⁷ Daar komt de brandstof bij van de tankervliegtuigen om de F-35 in de lucht te houden. De afgelopen decennia zijn motoren voor jachtvliegtuigen, door de noodzaak ze compact te bouwen, ook nauwelijks energie-efficiënter geworden. De Amerikanen werken al jaren aan Adaptable Versatile Engine Technology om het verbruik te verminderen. Of die technologie ooit technisch en financieel de markt gaat halen, is onzeker.

Technisch kan worden gevlogen op Sustainable Aviation Fuel (SAF). Maar vliegen op SAF gaat slechts in beperkte mate bijdragen aan de 2050-doelstelling. De grondstoffen voor het maken van biokerosine (bijvoorbeeld afgewerkte frituurolie) zijn kwantitatief onvoldoende beschikbaar en de productie op zich vergt veel

energie. Als die energie zelf niet duurzaam is, wordt het paard achter de wagen gespannen.⁸

De F-35 weegt zonder brandstof en munitie ongeveer 13 ton. Een deel van dat gewicht wordt ingenomen door de piloot, zijn/haar uitrusting, de schietstoel en de intrinsiek met de piloot verbonden systemen. Daarnaast worden snelheid, wendbaarheid en detecteerbaarheid voor een belangrijk deel bepaald door het belang om het vliegtuig en de piloot weer veilig terug te krijgen. Onbemand kan een vliegtuig kleiner, lichter, langzamer en *spendable* zijn, en toch de gewenste militaire uitwerking hebben. Dat is niet alleen veel goedkoper, maar kost ook veel minder brandstof.

Grote landen en bedrijven lopen zich al warm voor de ontwikkeling van een nieuwe generatie jachtvliegtuigen: het zogenaamde Future Combat Air System (FCAS). Daar gaat helaas de komende jaren nog veel geld aan verspild worden, want de toekomst is aan de onbemande systemen. Als Defensie enig zicht wil houden

7 Marcel Hendriks, 'Maken méér JSF's de wereld veiliger? Nou nee, tenzij...', *Energie voor inzet*, 8 juni 2022. Zie: <https://www.energievoorzet.nl/jsf>.

8 European Parliamentary Research Services, 'Sustainable aviation fuels', november 2020.



De landmacht is de kleinste gebruiker, maar heeft wel veel logistiek en force protection nodig om de brandstof te krijgen waar die nodig is

FOTO MCD, SJOERD HILCKMANN

op de doelstelling van 2050 dan is de F-35 het laatste bemande jachtvliegtuig.

Luchtmobiel

Met een waaier aan lange- en kortereafstands-systemen slagen de Oekraïners erin de getalmatig superieure Russische luchtmacht op afstand te houden. Ook een aanzienlijk deel van de kruisvluchtwapens wordt uit de lucht geschoten. De levering van méér geavanceerde westerse systemen zal die luchtverdediging nog succesvoller maken.

Het snel door de lucht achter de linies kunnen inzetten van troepen heeft op papier meerwaarde. Of dat in een grootschalig conflict verschil maakt, is nog maar de vraag. Door effectieve luchtafweer zijn de risico's voordat de grond wordt bereikt ook veel groter dan vroeger: vliegende transportmiddelen zijn van nature nu eenmaal groot en langzaam. Inzet in een *contested area* lijkt daarom bij voorbaat kansloos

en onverantwoord. De analogie met het amfibisch optreden, zoals het HCSS-rapport vaststelt, dringt zich op.

Na de val van de Berlijnse Muur was luchtmobiel het politiek-militaire antwoord op het ontspannen van de veiligheidssituatie. Nu dat beeld weer gekanteld is, is het de vraag of de kosten nog opwegen tegen de baten. Door het opheffen van luchtmobiele capaciteit kan Nederland zijn luchtvloot aanzienlijk inkrimpen. Dat bespaart niet alleen heel veel geld, maar ook een enorme sloot brandstof. De ontwrichting van het vijandelijke achterland, een taak van luchtmobiel, kan beter worden overgelaten aan precisieartillerie met lange dracht.

Koninklijke Landmacht

De landmacht is met vijftien procent de kleinste gebruiker binnen de krijgsmacht. Maar opera-

tioneel wel de meest kwetsbare, omdat de landmacht anders dan de marine en luchtmacht minder makkelijk kan terugvallen op eigen voorraden. Er is veel logistiek en *force protection* nodig om de brandstof te krijgen waar die nodig is. Waar liggen de mogelijkheden voor de landmacht om bij te dragen aan de doelstellingen voor 2030 en 2050?

Compounds

Op een compound moet in 2030 de helft van de elektrische energie duurzaam worden opgewekt. Een werkgroep van bedrijfsleven, kennisinstellingen en Defensie heeft aangetoond dat dat nu al kan: door minder te gebruiken, meer duurzame energie op te wekken en bestaande systemen energie-efficiënter te maken. Met middelen die nu al op de markt zijn en zich al onder extreme omstandigheden hebben bewezen.⁹

Maar om '2030' te realiseren moet er wel tegelijkertijd worden geïnvesteerd in energie-opwekking en opslag, transport en accommodatie, koeling en verwarming, en voeding en sanitair. Het incrementeel verwerven, zoals dat nu gebeurt, van dieselgeneratoren en tenten levert onvoldoende op en kan zelfs averechts werken. Het is onduidelijk welke organisatorische en financiële hindernissen Defensie belemmeren hierin door te pakken.

In 2050 moet op een compound zelfs alle elektrische energie duurzaam worden opgewekt. Dat is een enorme uitdaging omdat er ook elektrische gevechtsvoertuigen komen. Wind- en zonne-energie alleen kunnen daarin onmogelijk voorzien. Duurzaam geproduceerde waterstof die met brandstofcellen elektriciteit opwekt, kan uitkomst bieden. Dat is echter alleen haalbaar wanneer waterstof veel veiliger dan nu (onder hoge druk of cryogeen vloeibaar) kan worden vervoerd en opgeslagen. Er wordt gelukkig onderzoek gedaan naar nieuwe opslagtechnieken die dat mogelijk moeten maken.

Gepantserde voertuigen

Het HCSS-rapport wijst op de waarde van de wapensystemen uit de vorige eeuw zoals tanks en artillerie, mits goed toegepast. In lijn daar-

In de wedloop tussen antitank en pantser zullen de platformen steeds zwaarder worden en navenant meer diesel nodig hebben

mee is het een goede zaak dat het Westen Oekraïne ook helpt met tanks. Maar oorlog voeren doe je met de wapens die je op dat moment hebt. Ze zijn hopelijk succesvol in 2023, maar dat zegt niet veel over wat je in 2050 nodig hebt om te winnen.

Landstrijdkrachten maken in tegenstelling tot de andere krijgsmachtonderdelen nog gebruik van bepantsering. Maar moderne antitankwapens worden steeds effectiever. In de wedloop tussen antitank en pantser zullen de platformen daarom steeds, tenzij er goede actieve bescherming komt, zwaarder worden en navenant meer diesel nodig hebben. Gepantserd materieel heeft dus te maken met een tweesnijdend zwaard: steeds betere antitankwapens en een steeds hoger brandstofverbruik.

De steun aan Oekraïne bestaat niet voor niks voor een belangrijk deel uit antitankwapens

9 NIDV Platform Operationele Energie, 'Een duurzaam kamp? Ja dat kan!', Themadag Energie en Duurzaamheid, Rijswijk, 2 maart 2017.

en langeafstandartillerie om ook Russische brandstofdepots uit te schakelen. Vooralsnog lijkt dat succesvol. De Russische overmacht aan zwaar materieel heeft nog geen verschil kunnen maken.

Het ligt daarom voor de hand dat de landmacht op den duur alleen nog gepantserd materieel gebruikt waar dat echt niet anders kan, zoals voor commandovoering, gewondentransport, transport van essentiële non-combattanten, et cetera. Bij zware voertuigen waar ‘massa’ fysiek niet kan worden gemist, zoals voor de genie en voor geschut, heeft pantser natuurlijk ook nog steeds toegevoegde waarde.

Wat moet ervoor in de plaats komen? Momenteel onderzoekt de landmacht het gebruik van Robotica en Autonome Systemen (RAS), nu nog voor verkenning en als kleine wapendrager.¹⁰ Maar doorontwikkeling naar platformen met meer vuurkracht is te verwachten. Bij onbemande systemen is er geen pantser nodig om de bemanning te beschermen, hooguit om de sensoren te laten blijven werken. Met kleinere en lichtere onbemande gevechtsvoertuigen komt elektrische tractie ook binnen handbereik.

Ook bij het gebruik van infanteriegevechtsvoertuigen (IGV) lijkt een volgende stap mogelijk. De bescherming die pantser nu biedt kan worden vervangen door bescherming door ‘ongemerkt en ongezien’. Militairen die zich verplaatsen met elektrische tweewielers en quads, waarbij de directe omgeving steeds met drones wordt verkend, lopen waarschijnlijk minder risico dan wanneer ze zich verplaatsen in een IGV, en ze kunnen zich ook sneller ontplooiën.

Koninklijke Marechaussee

Van de krijgsmachtdelen gebruikt de Koninklijke Marechaussee ongetwijfeld de minste fossiele brandstof. Uit de jaarrapportages van Defensie wordt echter niet duidelijk hoeveel precies. Beleidsmatig is dit ook minder relevant, omdat de voertuigen van de marechaussee voor een groot deel kenteken-geregistreerd zijn en dus de gewone wet- en regelgeving moeten volgen. Voor investering in nieuw materieel is het relevant dat de Europese Unie in 2035 geen verkoop meer wil van personenauto’s en kleine transportmiddelen met een verbrandingsmotor.

Militaire innovatie

De hiervoor beschreven oplossingen staan mogelijk op gespannen voet met inzichten hoe de gevechtskracht versterkt moet worden: een sine qua non voor de krijgsmacht. Maar de huidige inzichten zijn gebaseerd op de premisse dat fossiele brandstoffen onbeperkt beschikbaar zijn en bijna niets kosten. Dat is niet langer zo en dat dwingt Defensie niet alleen om na te denken over technische, maar ook over militaire innovatie.

Militaire innovatie is zelfs belangrijker dan nieuwe technologie. Want energietechniek is gebonden aan de wetten van de thermodynamica. Met het Carnotdiagram – waarbinnen alle verbrandingsprocessen zich afspelen – valt niet te sjoemelen. Wachten tot de techniek Defensie aan ‘70 procent minder’ helpt, is de hond in de pot vinden. Defensie moet daarom op zoek naar operationele concepten die middelen vragen die inherent minder brandstof gebruiken dan de huidige platformen.

De strategische noodzaak om minder afhankelijk te worden van fossiele brandstoffen dwingt Defensie tot het maken van keuzes. Langer uitstellen kan niet, de tijd dringt. Wapensystemen die nu worden aangeschaft, zullen immers nog in 2050 operationeel zijn. Om die urgentie te onderstrepen zei secretaris-generaal van de NAVO Jens Stoltenberg op 28 juni 2022 bij de opening van een congres over

¹⁰ Ministerie van Defensie, ‘Vecht landmachtmilitair straks zij aan zij met een robot?’, 14 oktober 2022. Zie: <https://www.defensie.nl/actueel/nieuws/2022/10/14/vecht-landmachtmilitair-straks-zij-aan-zij-met-een-robot>.



De NAVO test 'smart energy'-technologie. NAVO-chef Jens Stoltenberg onderstreepte het belang van verminderde afhankelijkheid van fossiele brandstof voor de resilience van strijdkrachten

FOTO NAVO

klimaat en veiligheid terecht: 'The most resilient armed forces will be those that don't rely on fossil fuel.'

Bijna tien jaar na vaststelling van de noodzaak om in 2050 zeventig procent minder afhankelijk te zijn van fossiele brandstoffen is er slechts weinig bereikt. Begin dit jaar publiceerde Defensie de 'Roadmap Energietransitie, operationeel materieel'. Dit is een document met gepolijste bespiegelingen, uiteenzettingen, voornemens, verkenningen en ideeën, maar het bevat helaas opnieuw geen enkel concreet plan,

aanknopingspunt of perspectief op het halen van '2050'.

Het heeft er alle schijn van dat Defensie de eigen doelstelling voor 2050 niet haalbaar acht en dat de organisatie er daarom ook maar geen serieus werk van maakt. Dat kan de Tweede Kamer natuurlijk niet zijn ontgaan. Maar er is blijkbaar geen urgentie om Defensie daarover eens flink aan de tand te voelen. Zo'n 'don't ask, don't tell'-situatie schaadt uiteindelijk Defensie en de politiek. Het is beter om duidelijkheid te scheppen met elkaar. ■

Cyber-enabled Influence Operations

The case of the Belarusian Cyber Partisans

Peter Schrijver MA and Prof. Dr. Paul Ducheine*

The Belarusian Cyber Partisans (BCP) have opposed the authoritarian government of Belarus since 2020 through cyber attacks. They have hacked government and police databases, revealing sensitive information about government personnel. One notable event was their hack of the Belarusian railway system in early 2022, which disrupted the Russian military build-up to the large-scale invasion of Ukraine. To this day, the Cyber Partisans continue to challenge the regime of President Lukashenko and Russian presence and influence in Belarus. An analysis offers more conceptual clarity on the effects sought by non-state groups like the BCP, and thereby on how the Cyber Partisans should be labelled.



One month before the full-scale Russian invasion of Ukraine on 24 February 2022, Belarusian railway workers posted a message on their Telegram-channel @belzhd_live in which they reported the arrival in Belarus of trains carrying military equipment and personnel of the Russian Federation Armed Forces for the joint Belarus-Russian exercise Allied Resolve. ‘The total number of trains that will arrive in Belarus – 200 military echelons – is an outrageous figure’, the message read, also noting that during the earlier joint strategic exercise ZAPAD 2021 ‘only 29 military echelons’ had been sent to Belarus.¹ The message was preceded by what has been called the largest Russian military deployment in Belarus since the end of the Cold War. According to press reports, by the beginning of February 2022, 30,000 Russian troops had arrived in Belarus for joint military exercises.² Some of the units deployed to Belarus came from places as far as Lake Baikal in Russia’s Eastern Military District.³

Then, on Monday 24 January 2022, a group calling itself the Belarusian Cyber Partisans posted messages on their social media channels Twitter (13,500 followers) and Telegram (63,000 followers), claiming to have encrypted the Belarus Railways (BR) servers, workstations and databases.⁴ According to the Cyber Partisans, the direct aim of this operation was to disrupt the activities of BR as a sign of protest because President Aleksandr Grigorjevitsj Lukashenko of Belarus had allowed ‘occupying troops to enter our land’.⁵ The Belarusian Cyber Partisans have found themselves at loggerheads with the Belarus regime since August 2020 when, after

fraudulent presidential elections, Lukashenko refused to cede power to the opposition and crushed a popular revolt by using harsh measures towards protesters, exiling opposition leaders and detaining thousands of opposition members.

Operations in cyberspace by non-state actors against state actors are not a new phenomenon.⁶ For more than a decade the hacker collective Anonymous, an important benchmark for these type of action, has not hesitated to attack governments and firms in cyberspace for alleged misdoings.⁷ The Anonymous ‘group’ has claimed responsibility for several website defacements, information leaks and distributed denial of service (DDOS) attacks.⁸

In the analysis of these operations frameworks can be used such as the ‘(unified) cyber kill chain’.⁹ This operational framework focusses heavily on the techniques, vectors, vulnerabilities and exploits used to seek effects with the cyber operations. These frameworks, however, offer little insight into motives and focus primarily on so-called ‘hacking’ or ‘hard cyber operations’. But is this label appropriate for the activities of the Belarusian Cyber Partisans or are other, more precise, definitions possible?

* Major Peter Schrijver is PhD-researcher at the Netherlands Defence Academy (NLDA). Brigadier-general Paul Ducheine is Professor of Cyber Warfare at the NLDA. This article is based on a Master Military Strategic Studies research paper.

- 1 @belzhd_live (Belarusian railway workers, Telegram channel), ‘Live. Сообщество Железнодорожников Беларуси’. https://t.me/belzhd_live/1257.
- 2 Pavel Polityuk and Sabine Siebold, ‘NATO Says Russia to Have 30,000 Troops on Drills in Belarus, North of Ukraine’, *Reuters*, 3 February 2022.
- 3 Michael Sheldon, ‘Russian Military Equipment Spotted in Belarus as Tensions Heighten with Ukraine’, @DFRLab, 18 January 2022.
- 4 @cpartisans_bot (Telegram channel Belarusian Cyber Partisans) ‘Кибер-Партизаны’. <https://t.me/cpartisans/625>.
- 5 ‘Why the Belarus Railways Hack Marks a First for Ransomware’, *Wired.com*, 25 January 2022.
- 6 R.J. Buchan, Cyberspace, ‘Non-State Actors and the Obligation to Prevent Transboundary Harm’, *Journal of Conflict & Security Law*, 21 (3) (2016) pp.429-453.
- 7 Paulo Shakarian, Jana Shakarian and Andrew Ruef hakarian, *Introduction to Cyber-Warfare. A Multidisciplinary Approach* (London, Syngress, 2013) p.79.
- 8 Johan Sigholm, ‘Non-State Actors in Cyberspace Operations’, *Journal of Military Studies*, 4 (1) (2013) 3.
- 9 See i.a. Paul Pols, *The Unified Kill Chain. Raising resilience against advanced cyber attacks through threat modeling*: www.unifiedkillchain.com.

A photo made available by the Belarusian government shows Russian military vehicles arrive for the joint military exercise ‘Allied Resolve’ in Belarus, 18 January 2022. The Belarusian Cyber Partisans claimed to have encrypted the Belarus Railways servers, aiming to disrupt such transports

PHOTO ANP/EPA/BELARUS DEFENCE MINISTRY

Belarusian Cyber Partisans: resistance in cyberspace

The Belarusian Cyber Partisans hacker collective emerged in 2020 in response to the controversial presidential elections and following crackdown on civil liberties in Belarus. The group consists of Belarusian activists, hackers and IT professionals who use their skills to challenge the regime of President Aleksandr Lukashenko and support the pro-democracy movement.

The cyber partisans rose to prominence in August 2020 when they launched a massive cyber-attack against government propaganda websites and leaked sensitive information about the country's security services. The group has claimed responsibility for several high-profile cyber-attacks, including in 2022 on systems of Belarusian Railways to disrupt incoming Russian military transports.

The group operates in secrecy, using an enhanced variant of the messaging app Telegram to evade detection and retaliation by authorities. Belarusian cyber activism has received widespread support from the international community and has been praised for its efforts to promote human rights and democracy in Belarus. However, their actions also angered the Belarusian government, which called them 'terrorists' and threatened them with severe punishment if caught. Overall, the Cyber Partisans represent a form of activism that uses technology and digital tools to challenge authoritarian regimes.

Sources: Andrea Peterson, 'Cyber Partisans hacktivists claim credit for cyberattack on Belarusian Railways', *The Record*, 24 January 2022; Andrew Roth, 'Cyberpartisans' hack Belarusian railway to disrupt Russian buildup', *The Guardian*, 25 January 2022; Dalton Bennett and Robyn Dixon, 'How Belarus's 'Cyber Partisans' exposed secrets of Lukashenko's crackdowns', *The Washington Post*, 15 September 2021

Aim and Relevance

This article firstly aims to enhance insight into the activities of the Belarusian opposition in cyberspace. This contributes to the understanding of the dynamics in the information environment in Belarus, which borders on Lithuania where a Netherlands company within the NATO enhanced Forward Presence (eFP) mission is stationed. In particular, it will shed light on the context of the cyberspace activities against the Belarus regime since 2020. Although the actions of the Belarusian cyber group succeed in increasing media attention, little is known about the background of this group, which aligns itself with the Belarusian opposition leadership.¹⁰

Secondly, apart from gaining more operational insight into the modus operandi of the various operations described to (or claimed by) the Cyber Partisans, this article also aims to offer more conceptual clarity on effects sought by these non-state groups, and thereby on how the Belarus Cyber Partisans should be labelled.

Structure

This article limits itself to examining the context of the activities of the Belarusian Cyber Partisans (BCP) in cyberspace against the Belarus regime during and after 2020. It will therefore offer a conceptual framework for influence operations first. It will then describe the Cyber Partisans activities against the Belarus regime. Subsequently, the various activities will be analysed using the model presented.

Conceptual framework

Traditionally, cyber operations are divided into the broad categories of hard and soft cyber power.¹¹ According to Joseph S. Nye, an example of hard power in cyberspace is when states or non-state actors organise a DDOS-attack to paralyse the internet system of an opponent.¹² An example of soft power in the cyber domain is persuading a group of programmers to adhere to a new software standard.¹³ In that sense the Stuxnet Operation, which targeted the centrifuges of Iran's uranium enrichment plants, using

10 'Belarusian Cyber-Partisans Want to Overthrow the Regime through Hacking', *Deutsche Welle*, 3 September 2021.

11 Joseph Nye Jr, *Cyber Power* (Cambridge, Harvard Kennedy School/Belfer Center for Science and International Affairs, 2010) p.6.

12 *Idem*, p.5.

13 *Ibidem*.

stealthy software to disrupt industrial control systems would be classed as hard cyber power and the interference with the US elections in 2016 through influence operations in cyberspace as soft cyber power.¹⁴

Sean Cordey of the Swiss ETH Center for Security Studies (CSS) approaches cyber operations from the generic angle of influence operations, which were already a characteristic of pre-conflict and conflict phases long before there even was a mention of cyber operations and/or cyberspace.¹⁵ The ETH CSS definition of cyber influence operations is as follows: 'the term cyber influence operations (CIOs) refers to illegitimate (sometimes illegal) activities that are run in cyberspace, leverage the distributed vulnerabilities of cyberspace, and rely on cyber-related tools and techniques to affect an audience's choices, ideas, opinions, emotions or motivations, and interfere with its decision-making processes'.¹⁶

Based on the means and ways applied his definition is then subdivided into two separate spheres.¹⁷

First, Cyber-enabled Technical Influence Operations (CeTIO) disturb 'cyberspace through intrusive means to gain unauthorized access to networks and systems in order to destroy, change, steal or inject information with the intention of influencing attitudes, behaviors, or decisions of target audiences'.¹⁸ Basically, this definition refers to the hacking of computer systems.

Secondly, Cordey then goes on to explain Cyber-enabled Social Influence Operations (CeSIO), which 'target and attack the semantic layer of cyberspace (i.e. information content) through a wide variety of tools and techniques in order to support and amplify various political, diplomatic, economic, and military pressures'.¹⁹ This definition is tied to influence operations, for example the distribution of disinformation via social media channels.

According to these definitions, DDOS-attacks or hacking into IT-systems – which are traditionally labelled hard cyber operations – belong to the sphere of cyber-enabled influence operations. The ETH CSS argues these DDOS-attacks on



Belarusian Cyber Partisans: 'Russian war machine, leave Belarus and Ukraine. We have not even started'

institutions in Estonia in 2007 had the ultimate goal of undermining trust in the Estonian government and should therefore not be called hard cyber operations but be considered as Cyber-enabled Technical Influence Operations.²⁰ Actions which sow and amplify disinformation via cyberspace with the goal of undermining trust in institutions are not soft cyber operations but Cyber-enabled Social Influence Operations.²¹

Hence, the ETH CSS postulates that cyber operations aiming to influence persons, communities and even regions or countries should thus be labelled as cyber-enabled influence operations. The modus operandi used to influence will, subsequently, be further categorised as either technical (e.g. hacking) or social (e.g. spread of disinformation on Twitter).

14 Petere Pijpers and P.A.L. Duchaine, 'Influence Operations in Cyberspace – How They Really Work' (September 24, 2020), Amsterdam Center for International Law No. 2020-31, Available at SSRN: <https://ssrn.com/abstract=3698642> or <http://dx.doi.org/10.2139/ssrn.3698642>.

15 Sean Cordey, 'Cyber Influence Operations: An Overview and Comparative Analysis', (ETH Zürich, October 2019) p.6.

16 Cordey, p.11.

17 Which is similar to the Russian division between information technological warfare and information psychological warfare, see: Keir Giles, *Handbook of Russian Information Warfare*, NATO Defence College 9, no. November (2016): pp.1-90, 9.

18 Cordey, p.15.

19 Cordey, p.16.

20 Cordey, p.15.

21 Cordey, p.17.

1. Preparation/ Reconnaissance	2. Execution cyber-related activities		3. Exploitation/ Objective
<ul style="list-style-type: none"> • Political intent • Strategic narrative • Identify fissures • Map and segment audience • Framing • Creation (websites, content) 	<p>Cyber-enabled Technical Influence Operations</p> <ul style="list-style-type: none"> • DDos/DOS • Defacement • Hacks 	<p>Cyber-enabled Social Influence Operations</p> <ul style="list-style-type: none"> • Cognitive hacking • Social hacking • Disinformation • Doxing • Forging & leaking • Potemkin villages • Deceptive identities • Bots/botnets • Trolling & flaming • Humor & memes 	<ul style="list-style-type: none"> • Disrupt activities – sense of insecurity • Control/reinforce/redirect narrative • Undermine trust in institutions/media/allies • Demoralise/encourage • Sow division/polarise • Discredit/support individuals

Figure 1 Framework derived from Pijpers, ETH CSS Zürich and CSET, for the purpose of identifying different types of cyber-enabled influence operations (IO)

To bring operational and conceptual clarity in the activities of the Belarusian Cyber Partisans in cyberspace against the Belarus regime as of 2020, a combination of frameworks/analytical models is used.^{22, 23, 24} A possible model could be figure 1 shown above.

Activities in cyberspace against the Belarus Regime since 2020

This section gives an overview of the cyberspace activities against the Belarus Regime since 2020. It will give a chronological summary starting with activities executed shortly after the fraudulent presidential elections in August 2020 and ending with the claim of the Belarusian Cyber Partisans to infringe the systems of the

Russian internet and media regulator Roskomnadzor in November 2022. In 2021, Operation Heat was the most notable example of the capabilities of the Cyber Partisans. However, they had already given hints of their expertise as of September 2020, with the defacement of government websites²⁵ and the interruption of internet news programmes by state TV channels *Belarus 1* and *ONT* by showing clips of police brutality instead of regime-censored news.²⁶

Summer of 2020: fraudulent elections followed by a harsh crackdown

After the elections in August 2020, despite almost openly fraudulent actions, Lukashenko began his sixth term as President of Belarus since 1994. Though elections had been rigged before and despite the regime’s effort before the elections to crack down on the opposition by jailing its leaders and banning their candidacies, this time it was different. Not least since Svyatlana Tsikhanouskaya – the wife of candidate Syarhei Tsikhanousk – stepped in. Tsikhanousk was a well-known video blogger who had been imprisoned after leading an enormously popular – though not very subtle – campaign called ‘Stop the Cockroach’.²⁷ Along with Tsikhanouskaya, the wives of other jailed politicians and campaigners united in one opposition front, which, according to exit poll

22 Pijpers, ‘Influence Operations in Cyberspace’.
 23 Cordey, ‘Cyber Influence Operations: An Overview and Comparative Analysis’.
 24 Katerina Sedova et al, ‘AI and the Future of Disinformation Campaigns’ (Center for Security and Emerging Technology, December 2021) p.2.
 25 ‘Lukashenka’s Regime Confused about Belarusian Cyber-Partisans’ Activity’, @DFRLab, 1 October 2020.
 26 Belarus Free Theatre, ‘Cyber Partisans in #Belarus Hacked the Websites of the Main State TV Channels, Instead of the Government Propaganda They Showed the Beatings and Arrests of Protestors in the Live TV Section. See: <https://T.Co/GMqpvvKESR>’.
 27 ‘Stop the cockroach’: protests rattle Belarus President Lukashenko before election’, Reuters, 2 June 2020.



Riot police clash with protesters in Minsk, capital of Belarus, after President Lukashenko denied to step down after fraudulent elections in 2020

Photo Picture Alliance/Anadolu Agency

data collected by various online platforms, would presumably have won the elections.²⁸ From that moment on mass protests began to break out in the capital Minsk and in other Belarusian cities. The regime increasingly resorted to excessive violence and mass detentions to crack down on the peaceful manifestations. The regime imprisoned more than 30,000 persons, mostly on trivial charges such as displaying symbols related to the opposition, presence at a demonstration or even a single social media post that was critical of the regime.²⁹ These events caused opposition leaders such as Tsikhanouskaya to go into exile in neighbouring Poland and Baltic states Lithuania and Latvia. Progressively, the security apparatus succeeded in suppressing open rebellion against the regime of President Lukashenko and in the winter of 2020/2021, mass protests on the streets of the cities in Belarus slowly stopped.³⁰

Operation Heat

However, this was not the end of the resistance against Lukashenko's regime. In a series of hacks in the summer of 2021 the Belarusian

Cyber Partisans, which reportedly consists of 10 to 15 Belarus IT experts,³¹ managed to penetrate deeply into government databases.³² Contrary to what a casual observer might think, Belarusian IT-expertise is traditionally one of the trademarks of the Belarusian economy. Already during the era of the Soviet Union, Belarus developed into a hub of the then emerging IT sector.³³ Belarusian IT skills are still sought after on the global market.³⁴

28 'It's outrageous: Belarus election result sparks night of defiance and violence', *The Guardian*, 10 August 2020.

29 Human Rights Watch, 'Belarus'. See: <https://www.hrw.org/europe/central-asia/belarus>.

30 Deutsche Welle, 'Belarus'. See: <https://www.dw.com/en/belarus/t-38384925>.

31 'Details Emerge on Hack of Belarusian Railways and the Group behind It. The hackers posted 'proof' of their hacks, and researchers have started to dig in', *Cyberscoop*, 26 January 2022.

32 Andrei Soshnikov et al., 'Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data', *Current Time*, 4 August 2021.

33 Foreign Policy Research Institute, 'How Belarus' Soviet Past Led to its Modern-Day IT Success', See: <https://www.fpri.org/article/2020/12/how-belarus-soviet-past-led-to-its-modern-day-it-success/>.

34 Rest of World, 'The tech workers exiled from Europe's last dictatorship', See: <https://restofworld.org/2023/belarus-tech-exile-lukashenko/>.

The BCP managed to retrieve 5.3 million recordings of tapped telephone conversations from databases of the Belarus Interior Ministry

This high level of home grown IT-knowledge in Belarus may have helped the BCP in the summer of 2021, when the group managed to retrieve 5.3 million recordings of tapped telephone conversations from databases of the Belarus Interior Ministry.³⁵ Dimitri Alperovitch, an American cyber security specialist posted a message on Twitter: 'This is as comprehensive of a hack of a state as one can imagine.'³⁶ The American Center for European Policy Analysis (CEPA) qualified it as 'the most successful cyber-attack in the history of Belarus, involving entry to the regime's most secret and sensitive data vaults', describing the scale of the hack as unprecedented.³⁷

The Cyber Partisans released a phone call from their trove which had been recorded just after the elections in August 2020, in which a subordinate, asking how to handle a group of peaceful protestors – mainly women in Minsk –

received a reply from a colonel of the Interior Ministry's Minsk department of the Public Security Police that he should arrest them and beat them.³⁸

The Cyber Partisans published the call on multiple (social) media channels, exposing the ruthless tendencies of those loyal to the regime. Apart from police brutality, other released phone recordings showed similar behaviour from officers responsible for security in Belarusian cities, including one officer in Brest who stated that 'the more of his 500 detainees [...] sent to hospital after rough treatment, the better'. In August 2020 the BBC already reported on police firing live rounds at protestors in Brest.³⁹ To this day, the BCP regularly leak recorded phone calls between security and/or government personnel from the mid-2021 hack.⁴⁰

Operation Scorching Heat 2022

The next operation through which BCP managed to attract attention worldwide, was a hack into the IT systems of Belarusian Railways. On 24 January 2022, the group posted the following message on several social media channels: 'At the command of the terrorist Lukashenko #Belarusian Railway allows the occupying troops to enter our land. We encrypted some of BR's servers, databases and workstations to disrupt its operations'.⁴¹ The group stressed that in order to prevent dangerous railway conditions, BR's safety systems were not affected by the attack. The group claimed that it would be willing to release its grip on the BR systems when its demands, namely the release of fifty political prisoners and a halt to the influx of Russian troops, had been met.⁴² Just before the hack, the BR railway workers union had placed a message on its Telegram channel stating that BR was set to receive record numbers of trains in Belarus carrying Russian military equipment as part of the Russian-Belarus joint exercise Allied Resolve.⁴³

The visible result of the hack by the BCP, coined Operation Scorching Heat, was the interruption of the electronic ticket system for passengers.⁴⁴ The group itself claimed that it was easy to access the BR network due to obsolete IT

35 Dalton Bennett and Robyn Dixon, 'How Belarus's 'Cyber Partisans' Exposed Secrets of Lukashenko's Crackdowns', *The Washington Post*, 15 September 2021.

36 Dmitri Alperovitch, 'This Is as Comprehensive of a Hack of a State as One Can Imagine', *Twitter*, 2 September 2021.

37 CEPA, 'Lukashenko's Secrets: Not So Secret Anymore', See: <https://cepa.org/article/lukashenkas-secrets-not-so-secret-anymore/>.

38 You Tube channel Cyber Partisans, See <https://www.youtube.com/watch?v=fPsiabcDiPU>.

39 BBC News, 'Belarus election: Police use live fire on protesters in Brest', See: <https://www.bbc.com/news/world-europe-53748748>.

40 Bennett and Dixon, 'How Belarus's "Cyber Partisans" Exposed Secrets of Lukashenko's Crackdowns', *The Washington Post*, 15 September 2021.

41 Greenberg, 'Why the Belarus Railways Hack Marks a First for Ransomware'.

42 ZD NET/tech, 'Belarusian activists launch ransomware attack in protest of dictatorship, Russian troop surge', See: <https://www.zdnet.com/article/belarusian-activists-launch-cyberattack-against-railway-in-protest-of-dictatorship-russian-troop-surge/>.

43 @belzhd_live (Belarusian railway workers, Telegram channel), 'Live. Сообщество Железнодорожников Беларуси 🇧🇪'.

44 Dan Goodin, 'Hactivists Say They Hacked Belarus Rail System to Stop Russian Military Buildup', *Ars Technica*, 24 January 2021.

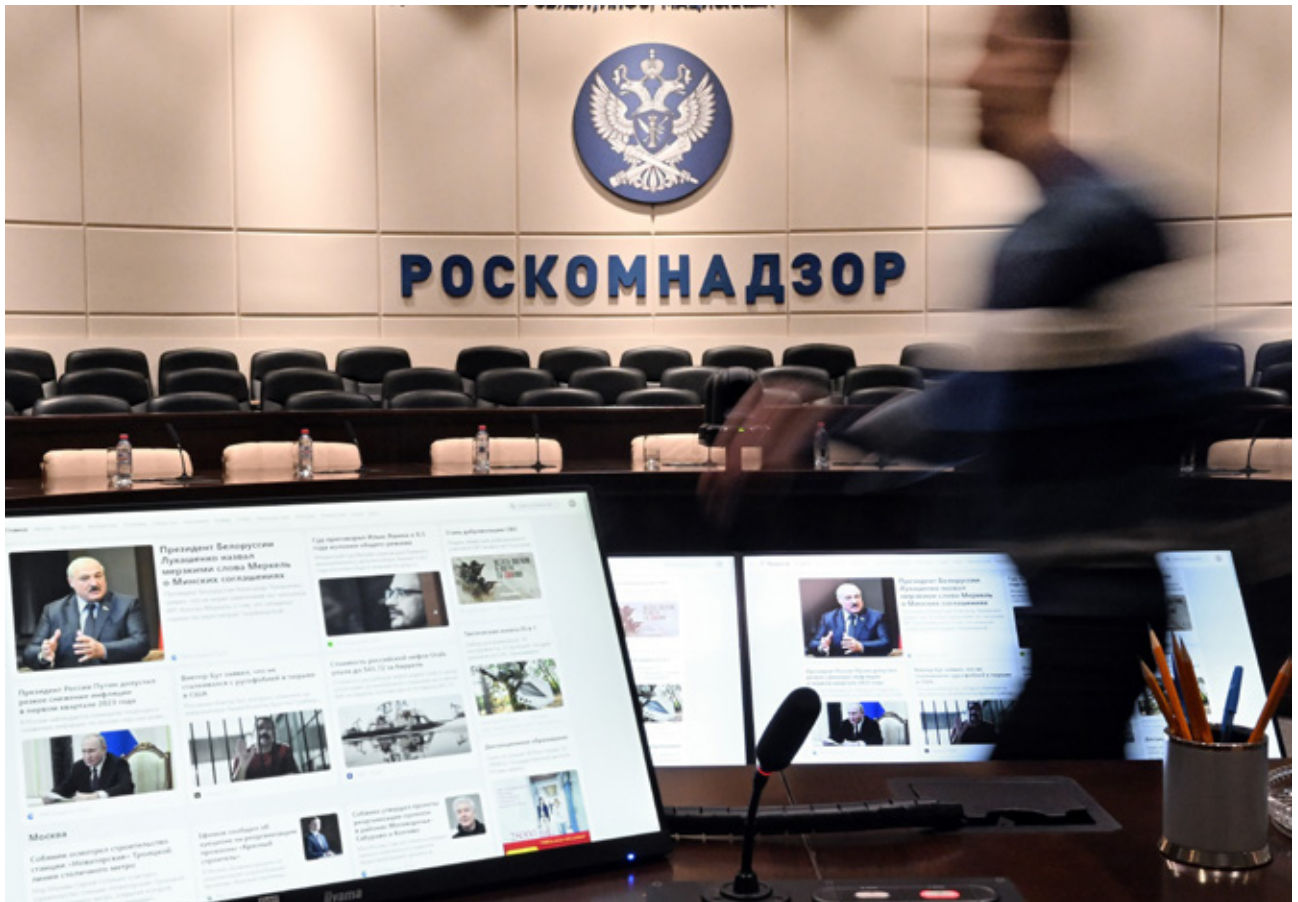


PHOTO: ANP/ANATOLIY ZHDANOV/KOMMERSANT/SIPA USA

In November 2022 the BCP said they had infringed the systems of Roskomnadzor, responsible for monitoring online content in Russia, claiming to have obtained a large amount of data

infrastructure and published several internal BR documents as proof of their breaching success.⁴⁵ The Cyber Partisans indicated that they had gained access to the BR systems because they were aware that BR personnel were using illegal software, which needs so-called ‘cracks’ or ‘crack software’ in order to run. These ‘cracks’ can be downloaded from shady websites.⁴⁶ Access to the BR network may have been gained after a BR employee unwittingly downloaded a possibly tailored piece of ‘crack software’ from such a website via a computer connected to the BR network, which enabled the installation of malware.⁴⁷

Several private US based cyber security agencies commented on the credibility of the Scorching Heat hack. SentinelOne stated that it was ‘unable to confirm the ransomware attack but

that the images provided appeared to confirm someone gained privileged access to Belarus Railway’s network’.⁴⁸ The phrase ‘images provided’ refers to several screenshots of documents from BR databases captured by the Cyber Partisans. These screenshots, published on Twitter, showed recent documentation of communications between BR and Russian

45 James Beardsworth, ‘“Hacktivist” Cyber Disruption Could Spread to Russia, Experts Believe’, *The Moscow Times*, 1 February 2022.

46 Belarusian Cyber Partisans, ‘Screenshots Taken during a #ScorchingHeat Cyberattack on the #belarus Railroad Reveal That Employees Frequently Used Pirated Software. Do You Think It’s Connected to How They Got Hacked? 🤔🤔🤔’ <https://t.co/De2R6W4Jt3>.

47 Hypothesis by authors after conversation with forensic cyber expert (NLD Army reservist).

48 Goodin, ‘Hacktivists Say They Hacked Belarus Rail System to Stop Russian Military Buildup’.

railway IT personnel, and an internal BR document requesting that outdated workstations running on Windows XP be replaced.⁴⁹

In the course of 2022 the BCP continued their campaign to put pressure on the Belarusian regime. The BCP gained access to passport data of all Belarusian citizens. Although these data were not extensively released to the public, interested parties were offered non-fungible tokens (NFT) of President Lukashenko's passport as a publicity stunt and fundraising campaign to continue actions against the government.⁵⁰ The BCP follow a pattern of not only breaching into government databases but, subsequently, the organisation also seeks ways to maximise publicity around their hacks by providing journalists and research collectives, e.g. Bellingcat access to acquired material.⁵¹ In November 2022 the BCP once again were able to hit international headlines after they had infringed the systems of Roskomnadzor, responsible for monitoring online content in the Russian Federation.⁵² BCP claimed to have obtained large amount of data, including emails and other documents, totalling over two terabytes.⁵³ It was also reported that the hacktivist group encrypted certain workstations and damaged the domain controller. Roskomnadzor acknowledged the breach but attributed it to the exploitation of a previously unknown vulnerability.⁵⁴

Failure and success of Operation Scorching Heat

With regard to the Scorching Heat attack of January 2022 and later attacks that year, it must be assessed that the original demands of the Belarusian Cyber Partisans were not met: it appears that the regime did not release political prisoners and did not halt the influx of Russian military and personnel into Belarus. In fact, in February 2022 Russian troops located on Belarusian territory were tasked to take the Ukrainian capital Kyiv. In this respect, the ransomware attack on BR was of little or marginal effect, besides the disturbance of electronic ticketing, the capture of internal BR documentation and the claimed encryption of servers, workstations and databases. Although this caused considerable damage to BR daily operations, the BR activities seemingly proceeded to continue as usual.⁵⁵ Thus, the operation could be considered as a minor success. However, amplified by the worldwide interest being paid to the Russian military build-up around Ukraine during the winter of 2021/2022, the January hack by the Cyber Partisans into the BR network gained worldwide media attention. Around the time of the hack (24-25 January 2022), approximately 6,000 articles appeared in press and media in which the BCP were mentioned.⁵⁶ The hacking of the Belarusian passport data records and the Russian internet regulator Roskomnadzor also received attention in global media outlets.⁵⁷ The earlier data hack (Operation Heat) into the Belarus Interior Ministry in mid-2021, which was of a much larger scale, attracted less attention in the international press.

Exposing the regime

Worldwide media attention set aside, the Belarusian Cyber Partisans have repeatedly stated that the overall goal of their actions is to expose the Belarusian regime⁵⁸ and take away the cloak of anonymity of government employees responsible for human rights abuses of Belarusian citizens.⁵⁹ The BCP explained that they wanted 'to stop the violence and repression from the terroristic regime in Belarus and to bring the country back to democratic principles and rule of law'.⁶⁰ To do so, the data, including details of security personnel which the Cyber

49 'Details Emerge on Hack of Belarusian Railways and the Group behind It'.

50 A.J. Vicens, 'Belarusian Hacktivists Try NFTs to Support Antigovernment Campaign', *Cyberscoop*, 31 August 2022.

51 Christo Grozev [@christogrozev], 'We First Noticed Her Thanks to a Super Useful Database Shared with Us by @cpartisans: The Border Crossing Records of Belarus. We Knew the Passport Ranges of GRU and FSB Spies, so We Decided to Search in That Data-Set by Partial Matches, Leaving the Last 3 Digits out as Wildcards.'

52 Daryna Antoniuk, 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator', *The Record*, 22 November 2022.

53 Gintaras Radauskas, 'Russian Censors Suffer Another Massive Hack', *Cybernews*, 21 November 2022.

54 Antoniuk, 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator'.

55 'Details Emerge on Hack of Belarusian Railways and the Group behind It'.

56 Unit, 'A Web Interface for the GDELT Project'. Source: <https://www.gdeltproject.org/>.

57 'Belarusian Hacktivists Claim to Breach Russia's Internet Regulator'.

58 Antoniuk, 'Hacktivist Group Shares Details Related to Belarusian Railways Hack'.

59 Soshnikov et al., 'Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data'.

60 Patrick Howell O'Neill, 'Hackers Are Trying to Topple Belarus's Dictator, with Help from the Inside', *MIT Technology Review*, 26 August 2021.



PHOTO PICTURE ALLIANCE/EPUSJUN ANDEMIR/ANAODLU AGENCY

Svyatlana Tsikhanouskaya speaks during the 2020 Sakharov Award Ceremony in Brussels: the European Parliament considers Tsikhanouskaya and other opposition leaders to be the true legitimate representatives of Belarus

Partisans collected during Operation Heat in 2021, are also shared with other activists. On the Telegram channel 'Black Book of Belarus' and the website Blackbook.org, data are published that identify members of the Belarus security services. Yanina Sazanovich, an editor of the Telegram channel, argues: 'In this war, we don't have any weapons. We have truth and 'de-anonymization' and this is our power and we will use it'.⁶¹ The government of Belarus rarely comments on the attacks carried out by the BCP or pretends to be unaware of them.⁶² Pro-Lukashenko Telegram channels *Belaruskaya Kuhnya* and *#InfoSpecNaz Belarusii* have branded the Cyber Partisans as 'employees of NATO cyber centers carrying out information and psychological attacks'.⁶³

The aim of the Belarusian Cyber Partisans is to stop the violence and 'to bring the country back to democratic principles and rule of law'.⁶⁴ The BCP influence activities do not solely affect the

cognitive dimension. In the physical dimension, real-world information (personal data) is provided on the home addresses of regime members. In the virtual dimension, hack operations result in the disturbance of IT systems such as the Belarus Railways ticketing system or the defacement of websites. Physical and virtual activities add up to effects in the cognitive dimension, including activities outside Belarus, such as the promotion of anti-regime protest in European capitals in the physical dimension.

The combined activities in all three dimensions are designed to undermine the resilience of the Belarus regime with the aim of ending it, which is one of the stated goals of the BCP.

61 'How Belarus's 'Cyber Partisans' Exposed Secrets of Lukashenko's Crackdowns'.

62 'Lukashenko's Regime Confused about Belarusian Cyber-Partisans' Activity'.

63 @DFRLab.

64 O'Neill, 'Hackers Are Trying to Topple Belarus's Dictator, with Help from the Inside'.

Belarusian Railway was once again the target of a hack in an attempt to slow down the transfer of occupying forces and give the Ukrainians more time to repel the attack

Defining the operations of the Belarusian Cyber Partisans

In this section the BCP operations of the Cyber Partisans are analysed against the conceptual framework used for the analysis of cyber-enabled influence operations, which encompass three consecutive phases of preparation/reconnaissance, execution of cyber-related activities and exploitation. The model (figure 1) offers an opportunity to assess whether the operations of the Belarusian group fit in the ETH CSS categorisation of Cyber-enabled Technical or Social Influence Operations.

Outcome

Nearly all activities of the Belarusian Cyber Partisans can be placed in a framework (figure 2) defining cyber-enabled influence operations. As such, the specific input provided by ETH CSS is helpful in categorising activities which involve the influencing of audiences and the input increases understanding of (non-state) activities in cyberspace. The analysis also shows that while a conceptual categorisation of cyber-activities can be made, to gain cognitive effect in or via cyberspace both operational avenues (technical and social) to influence are used. Hence, actors in cyberspace – including BCP – should not upfront be labelled as hard- or soft cyber operators.

Though the ETH CSS definition of cyber-enabled influence operations is helpful, there is also a flaw with this type of labelling as ‘the term cyber influence operations (CIOs) refers to illegitimate (sometimes illegal) activities’ only.⁶⁵ It is outside the scope of this article to determine when influence operations are unlawful.⁶⁶ However, while the Belarusian regime regards the activities undertaken by the Belarus Cyber Partisans as illegitimate, Poland and Lithuania harbouring sizeable contingents of Belarusian exiles, and the European Parliament, all consider the Belarusian opposition to be the true (legitimate) representatives of Belarus.⁶⁷ In sum, conceptual frameworks are useful in assessing the nature of the operations in cyberspace, but some prudence must be taken since the frames will not be universally applicable. ETH CSS’ definition, for instance, places the emphasis on rogue actors using cyber-enabled influence operations, hence, lacks an inclusive approach.

Conclusion and epilogue

In this article the activities of the Belarusian Cyber Partisans against Lukashenko’s regime during and after 2020 were addressed offering operational insights. The organisation presents itself as a non-state actor which supports the Belarus opposition by executing cyber operations aimed at undermining the Belarus regime. To provide conceptual clarity for their operations, a framework for the appraisal of cyber-enabled influence operations was used, based on work of scholars such as Pijpers and of the research institutes CSET and ETH CSS.

The article focused on the context of the activities in cyberspace. Cyber operations by the BCP are meant to influence an actor or actors, in this case primarily the Belarusian regime (undermine its resilience), but also the Belarusian population itself as well as foreign governments and populations. This aim or purpose – to influence audiences – is the main criterion for labelling the activities. Subsequently subdividing these by operational means and ways (technical or social) into cyber-enabled social and technical

65 See footnote 22.

66 On this topic see e.g. Peter B.M.J. Pijpers, *Influence Operations in Cyberspace. On the Applicability of Public International Law during Influence Operations in a Situation Below the Threshold of the Use of Force* (Thesis, University of Amsterdam, 2021).

67 ‘Lithuania Gives Belarusian Opposition Official Status’, *Radio Free Europe*, 5 July 2021.

1. Preparation/ Reconnaissance	2. Execution cyber-related activities		3. Exploitation/ Objective
<p>Intent: Bring Belarus to democracy and return rule of law</p> <p>Narrative(s): Lukashenko's regime is undemocratic</p> <p>'We have no weapons'</p> <p>Stop repression by regime</p> <p>Release political prisoners</p> <p>Russian troops in Belarus are not welcome</p> <p>Regime is negligent of infrastructure ('hacking into IT-systems is easy')</p>	<p>Cyber-enabled Technical IO Website defacement of Belarus TV-stations</p> <p>Content replacement in government-related websites</p> <p>Hack into sensitive databases of the Interior Ministry</p> <p>Access to footage of surveillance cameras</p> <p>Hack into license plate database service</p>	<p>Cyber-enabled Social IO Doxing of government personnel and security officers</p> <p>Leaking details from official sensitive documentation</p> <p>Social engineering (making use of inside knowledge /weaknesses</p> <p>Humor & memes</p>	<p>Disrupt activities – sense of government not in control</p> <p>Reinforce narrative about regime being undemocratic</p> <p>Russian troop movements in Belarus are illegal</p> <p>Undermine trust in infrastructure</p> <p>Demoralise security personnel government</p> <p>Deanonymisation (actions of regime personnel are noted and recorded)</p> <p>Discredit government-related individuals</p>

Figure 2 Activities of the Belarusian Cyber Partisans outlined in a framework to identify different types of cyber-enabled influence operations

influence operations is helpful in understanding the true nature of these actions, instead of using the more generic terminology of hard and soft cyber operations.

Given the current situation in which the Belarusian regime is inclined to strengthen its ties with the Russian Federation, Operation Heat and Operation Scorching Heat proved not to be the final activities of the BCP for the world to notice. On 24 February 2022 the group announced on its social media channels that it would contribute to the defence of Ukraine.⁶⁸ Since then, the BCP reached out to cooperate with groups such as the IT Army of Ukraine.⁶⁹ Shortly after Russia's invasion the Cyber Partisans stated that the state company Belarusian Railways was once again the target of a hack in an attempt to 'slow down the transfer

of occupying forces and give the Ukrainians more time to repel the attack'.⁷⁰ As such, the BCP moved from influence operations seeking cognitive effects to physical impact operations too. ■

68 Belarusian Cyber Partisans, '#Ukrainians and #belarusians Have a Common Enemy: Putin, Kremlin, the Imperial Regime. We Call on Everyone to Share This Info and Contact Us If Any Volunteers Want to Join Our Group. Please Support, Many Resources Are Still Needed: Bc1qv5jeswp0tu9s7kuf5uzjges49gnf0637asa8!'.
 69 Stefan Soesanto, 'The IT Army of Ukraine. Structure, Tasking, and Eco-System' (ETH Zürich, June 2022) p.27.
 70 'Belarusian hackers launch another attack, adding to chaotic hacktivist activity around Ukraine', *Cyberscoop*, 28 February 2022.

Mensen, materieel en financiën bij Defensie

Het Research Centre Military Management Studies van de Nederlandse Defensie Academie

Tine Molendijk en Robert Bertrand*

De militaire organisatie opereert in constant veranderende, onzekere omstandigheden waarin zij geconfronteerd wordt met complexe organisatievraagstukken, bijvoorbeeld rond technologische ontwikkelingen of ethisch leiderschap. Deze vraagstukken hangen bovendien met elkaar samen. Het Research Centre Military Management Studies, in 2020 opgericht door de Faculteit Militaire Wetenschappen (FMW) van de Nederlandse Defensie Academie (NLDA), doet hier onderzoek naar. Dit artikel bespreekt de achtergrond, de positie en het onderzoek van dit Research Centre.¹

Mensen, materieel en financiën

Hoe kan de defensieorganisatie de momenteel sterk vergrote financiële ruimte omzetten in duurzame investeringen in mensen en middelen? Wat is de invloed van nieuwe technologische ontwikkelingen op het functioneren van militaire eenheden? Wat zijn technologische en ethische vraagstukken rond *human enhancement*? Welke invloed heeft informatietechnologie (IT) op de informatievoorziening en de inrichting van de defensieorganisatie? Hoe zijn ethisch

* Dr. Tine Molendijk is een interdisciplinair georiënteerde antropoloog gespecialiseerd in de thema's geweld, militaire cultuur, ethiek en geestelijke gezondheid, met name morele verwonding. Ze is universitair docent aan de Nederlandse Defensie Academie en bestuursvoorzitter van het Research Centre Military Management Studies. Kolonel dr. Robert Bertrand RA RC RO is een interdisciplinair geschoold historicus, bedrijfsseconoom en auditor. Zijn onderzoek richt zich op auditing, compliance, internal control en ethiek. Hij is universitair hoofddocent aan de Nederlandse Defensie Academie en bestuurslid van het Research Centre Military Management Studies.

¹ Prof. dr. Lonneke Peperkamp is hoofd van het Research Centre Military Management Studies. Daarnaast maken prof. dr. Jeroen Klomp en dr. Jori Kalkman deel uit van het bestuur.



leiderschap en *just cultures* in de krijgsmacht te bevorderen? Wat is de rol van organisatiefactoren in morele verwonding, en welke rol heeft het thuisfront in werk en welzijn? Hoe kan samenwerking met civiele partners buiten de krijgsmacht verbeterd worden? En hoe kan de implementatie van exportcontroleregels zo goed mogelijk plaatsvinden?

De hedendaagse krijgsmacht staat voor een scala aan vraagstukken op strategisch, operationeel en tactisch niveau. Militairen – en dus ook de militaire organisatie als zodanig – opereren in constant veranderende, onzekere omstandigheden waarin zij geconfronteerd worden met complexe situaties die ingrijpende gevolgen kunnen hebben, zowel in vredessituaties als in

*Militairen lossen materieel van een trein.
Het Research Centre Military Management
Studies (RC MMS) doet onderzoek naar
organisatievraagstukken binnen de krijgsmacht*

FOTO MCD, SJOERD HILCKMANN



Met de implementatie van nieuwe technologie ontstaan nieuwe organisatorische, ethische en psychologische uitdagingen

crisisomstandigheden. De vraagstukken die dit oplevert zijn dus ook organisatievraagstukken. Binnen het Research Centre Military Management Studies (RC MMS) wordt hier onderzoek naar gedaan. In 2020 werd dit onderzoekscentrum opgericht door de Faculteit Militaire Wetenschappen (FMW) van de Nederlandse Defensie Academie (NLDA), samen met de onderzoekscentra War Studies en Military Technology.

Op het eerste oog hebben bovengenoemde vraagstukken misschien niet veel met elkaar te maken, maar niets is minder waar. Zo heeft de implementatie van nieuwe technologie onvermijdelijk invloed op hoe militaire eenheden georganiseerd worden en opereren, waardoor nieuwe sociale, ethische en psychologische uitdagingen kunnen ontstaan. Denk bijvoorbeeld aan de toevoeging van onbemande verkenningsvliegtuigen aan eenheden. Dit betekent niet gewoonweg de adoptie van extra sensoren of 'ogen', maar heeft gevolgen voor de personele inrichting van die eenheden, de verhoudingen binnen en tussen die eenheden, en dus voor de aard van het werk voor al het betrokken personeel. Zo ontstaan nieuwe sociale verhoudingen, ethische dilemma's en psychische stressoren. Bovendien roept het nieuwe vragen op rondom wat informatiegestuurd optreden

(IGO) precies inhoudt en hoe dat zich verhoudt tot andere wijzen van militair optreden.

Het is daarom zowel van belang te onderzoeken hoe militairen beter kunnen worden voorbereid (onder meer door selectie, opleiding en training) en moreel weerbaarder gemaakt kunnen worden, als om te kijken naar verbetermogelijkheden in bijvoorbeeld de organisatie van die eenheden, de interactie tussen mensen en middelen, en de samenwerkingsverbanden met andere partners. Militaire bedrijfswetenschappen vormen het vakgebied dat dit soort kwesties in samenhang onderzoekt. Dit onderzoek vormt de basis voor advies over verbeteringen in effectiviteit en efficiency aan beleidsmakers, commandanten, en eenheden. Dit maakt de militaire bedrijfskunde een unieke discipline met direct praktische relevantie.

In de zomer van 2022 publiceerden collega's van het War Studies Research Centre een informatief artikel in de *Militaire Spectator* over de geschiedenis en activiteiten van hun onderzoekscentrum.² Op vergelijkbare wijze bespreekt dit artikel de achtergrond, de positie en het onderzoek van het RC MMS. Eerst wordt een beknopte schets gegeven van de discipline militaire bedrijfswetenschappen en de unieke positie van het RC MMS in de militaire context. Deze schets bevat ook een toelichting op de positie van het onderzoekscentrum binnen Defensie en de notie van militairen als 'reflective practitioners' waarin onderzoek een grote rol speelt. Hierna volgt een bespreking van de doelstellingen, onderzoeksactiviteiten en meerwaarde van het RC MMS voor de militaire organisatie. Tot slot bespreken we hoe de drie onderzoekscentra in gezamenlijkheid zich gaan richten op overstijgende thema's als data science, ruimtetehnologie en IGO.

Bedrijfswetenschappen binnen de unieke militaire context

De krijgsmacht is nagenoeg de eerste organisatie in de geschiedenis die grootschalig optreden organiseerde. Dit optreden was bovendien al vroeg in de geschiedenis zeer complex. De

2 G. Frerks, M.W.M. Kitzen, F. Remmits, S.J.H. Rietjens en T. Sweijts, 'Mars voorwaarts en voorwaarts mars. Het War Studies Research Centre van de Nederlandse Defensie Academie', *Militaire Spectator* 191 (2022) (7/8) 398-408.



Napoleon spreekt zijn troepen toe bij de brug over de Lech bij Augsburg. In de 19e eeuw groeiden militaire eenheden in omvang

AFBEELDING VERSAILLES

zogenoemde civilisatieprocessen in onze geschiedenis, zoals beschreven door Norbert Elias, hebben tot steeds meer sociale standaarden en gedragsregels geleid. Zelfs in oorlog. De 19e eeuw bracht verklaringen en verdragen, terwijl intussen militaire eenheden in omvang groeiden en steeds verder werden verspreid over de wereld. Militair geweld werd gemonopoliseerd, geprofessionaliseerd en zo 'geciviliseerd', met een bijbehorende scherpe civiele controle van de krijgsmacht en militaire discipline.³

Veel moderne managementtheorieën, -concepten en -praktijken zijn in de meer recente geschiedenis ontstaan uit militaire lessen uit de Tweede Wereldoorlog.⁴ Rond die tijd ontstond ook hernieuwde belangstelling voor ervaringen van eerdere oorlogen, en groeide het besef dat naast krijgswetenschappelijk ook bedrijfswetenschappelijk onderzoek cruciaal is voor ons begrip van oorlog en militair optreden. Als gezegd was de krijgsmacht een van de eerste organisaties die grootschalig optrad, wat alleen mogelijk is met voldoende financiële middelen, logistieke

ondersteuning, productie van militaire wapensystemen, en uiteraard getraind en gezond personeel.⁵ Veel hedendaagse bedrijfskundige praktijken kunnen dan ook teruggevoerd worden op de kenmerkende organisatie van krijgsmachten in verschillende historische tijdvakken. Huidige bestuurs- en besluitvormingsstructuren in het civiele bedrijfsleven zagen we bijvoorbeeld voor het eerst in de Romeinse legers.⁶ In ons eigen land maakten de militaire hervormingen van prins Maurits (met name op het gebied van tactiek, logistiek, onderwijs en bedrijfsvoering) het in het begin

3 S. Lone, *Japan's first modern war army and society in the conflict with China, 1894-5* (Springer, 1994).

4 D. Ahlstrom, D. Lamond en Z. Ding, 'Reexamining some management lessons from military history', *Asia Pacific Journal of Management* 26 (2009) (4) 617-642; D.A. Wren en A.G. Bedeian, *The Evolution of Management Thought* (John Wiley & Sons, 2020).

5 Voor een historische beschrijving van de ontwikkeling van de organisatie van krijgsmachten en determinanten van succes zie onder andere M. van Creveld, *Command in war* (Harvard University Press, 1985) en E.H. Kramer en H. Kuipers, 'Flexibiliteit en starheid in krijgshistorisch perspectief', *Militaire spectator* 172 (2003) (9) 454-472.

6 B. Campbell, *The Roman army, 31 BC-AD 337: a sourcebook* (Routledge, 2006).



Figuur 1 De militaire bedrijfswetenschappen en de samenhangende vraagstukken die ze bestuderen. Geïnspireerd door figuur 6 uit E-H. Kramer, *De Militaire Bedrijfswetenschappen in Tien Stellingen: Een Sociotechnisch Perspectief*, 34

van de zeventiende eeuw mogelijk om de strijd op te kunnen nemen tegen het machtige Spaanse wereldrijk.⁷ Later tijdens de Napoleontische oorlogen⁸ zagen we bovendien een nog altijd inspirerende aandacht voor gedegen planning met kwantitatieve en kwalitatieve analyses

- 7 P. Paret, G.A. Craig, en F. Gilbert (red.), *Makers of modern strategy from Machiavelli to the Nuclear Age* (Oxford University Press, 1986); C.J. Rogers (red.), *The military revolution debate: readings on the military transformation of early modern Europe* (Westview Press, 1995); O.V. Nimwegen, 'Het Staatse leger en de militaire revolutie van de vroegmoderne tijd', *BMGN-Low Countries Historical Review* 118 (2003) (4) 494-518.
- 8 P.A. Talbot, 'Management organisational history – a military lesson?', *Journal of European Industrial Training* 27 (2003) (7) 330-340.
- 9 B. Baack en E. Ray, 'The Political Economy of the Origins of the Military-Industrial Complex in the United States', *The Journal of Economic History* 45 (1985) (2) 369-375.
- 10 D. Ahlstrom, D. Lamond en Z. Ding, 'Reexamining some management lessons from military history', *Asia Pacific Journal of Management* 26 (2009) (4) 617-642.
- 11 H.E. Eccles, 'The study of military management', *Naval Research Logistics Quarterly* 13 (1966) (4) 437-445.
- 12 V. Nutton, 'Medicine and the Roman army: a further reconsideration', *Medical History* 13 (1969) (3) 260-270; P. Olsthoorn, *Military Ethics and Virtues: An Interdisciplinary Approach for the 21st Century* (Londen en New York, Routledge, 2010); J. Soeters, P.C. van Fenema en R. Beeres (red.), *Managing Military Organisations: Theory and Practice* (Londen en New York, Routledge, 2010).
- 13 E-H. Kramer en T. Molendijk, *Violence in Extreme Conditions: Ethical Challenges in Military Practice* (Springer Cham, 2023).

gecombineerd met een flexibele houding vanuit het motto 'On s'engage, puis on voit' ('We engageren, en daarna zien we verder'). Een andere bevinding uit deze tijd is het belang van sociale cohesie voor de verhoging van het collectieve moreel. Ontegengelijk gaven de Eerste en daarna de Tweede Wereldoorlog een enorme impuls aan ontwikkelingen binnen het militair-industriële complex.⁹ Nog altijd vormt de krijgsmacht een inspiratie voor civiel management. Denk alleen al aan militaire metaforen zoals positionering, *blue ocean strategy*, de *war room* en de frontlinie, en *fighting the last war*.¹⁰

Militaire bedrijfswetenschappen gaan in brede zin over het managen van alle processen die plaatsvinden binnen militaire organisaties, inclusief het personeels-, financieel, materieel en IT-management, training en alles wat daarom heen nodig is. De bedrijfskundige discipline houdt zich traditioneel bezig met alle zaken die een militair manager moet beheersen ('to control'), zodat effectief optredende militairen kunnen worden gevormd en ingezet. De term 'management' is dan ook nauw verbonden met termen als bestuur, bedrijfsvoering (personeel, financieel en materieel beheer), *command-and-control*, IT, logistiek, personeelszorg en crisis-beheersing.¹¹ Tegelijkertijd gaan militaire bedrijfswetenschappen (eveneens al sinds de Romeinse tijd) over effectief leiderschap, de versterking van moreel en cohesie, medische verzorging van fysiek en mentaal verwond personeel, geestelijke bijstand aan militairen en handhaving van ethische standaarden.¹²

Toch zijn militaire bedrijfswetenschappen niet gewoonweg de toepassing van algemeen bedrijfswetenschappelijke inzichten op een specifieke militaire context. De krijgsmacht is immers een unieke organisatie. Ze voert complexe operaties uit in steeds nieuwe omstandigheden en soms dreigende omgevingen met een door de samenleving toevertrouwd geweldsmonopolie. Hoewel het gevecht allang niet meer de enige vorm van militair optreden is, blijft Defensie in essentie een gewelds-organisatie.¹³ Het bestaansrecht van de krijgsmacht heeft als basis de bescherming van

ationale en internationale vrede en veiligheid, en daarvoor heeft zij het politieke mandaat van een geweldsmonopolie, wat de grote verantwoordelijkheid met zich meebrengt van geëlitimeerd gebruik van geweld.

Als zodanig krijgt de militaire organisatie meer dan de meeste andere organisaties te maken met complexe vraagstukken. Bijvoorbeeld over de inrichting van de organisatie bij optreden in crisissomstandigheden, dynamische economisch-logistieke vraagstukken, technologische vernieuwing en de inzet van personeel in gevaarlijke omstandigheden. Daarbij heeft de krijgsmacht direct te maken met internationale veiligheidskwesties, politieke aansturing, (inter)nationale juridische kaders, ethische, psychologische en sociologische vraagstukken, en de inbedding in een vaak kritische samenleving.¹⁴ Figuur 1 is een weergave van enkele van de onderling samenhangende thema's die de militaire bedrijfswetenschappen bestuderen (de lijst is niet uitputtend).

Zoals de recente defensienota's beschrijven wil de militaire organisatie excelleren in het omgaan met al deze vraagstukken, om zo de hoofdtaken van Defensie zo goed mogelijk te kunnen uitvoeren. De organisatie wil snel inzetbaar zijn op alle geweldsniveaus, flexibel en adaptief zijn, technologisch hoogwaardig, divers en inclusief, en samen kunnen werken zowel met defensieorganisaties van andere landen als met civiele organisaties. Dit vraagt veel van het organisatievermogen, zeker onder de huidige geopolitieke omstandigheden. Op zijn beurt vraagt dit om multi- en interdisciplinair onderzoek naar actuele ontwikkelingen en mogelijke *best practices*. Neem het genoemde voorbeeld over de samenhang tussen technologische innovatie, organisatieverandering en nieuwe ethische en psychologische uitdagingen. In het bijdragen aan discussies over deze ontwikkelingen vanuit een integrale visie ligt de meerwaarde van militaire bedrijfswetenschappen.¹⁵

Het RC MMS maakt deel uit van de FMW, die zowel het wetenschappelijke onderwijs van officieren in spe verzorgt als wetenschappelijk onderzoek verricht. Zoals helder besproken in

Veel elementen uit moderne managementtheorieën vinden hun oorsprong in militair optreden vanaf de Romeinse tijd

het eerdergenoemde stuk over de geschiedenis van het War Studies Research Centre is de oprichting van onderzoekscentra te zien als 'de bezegeling van de groeiende wetenschappelijke oriëntatie' in militaire organisaties nationaal én internationaal.¹⁶ Stimuli in deze ontwikkeling in Nederland zijn de oprichting van de Koninklijke Militaire Academie (KMA) en het Koninklijk Instituut voor de Marine (KIM) in het begin van de 19e eeuw, de officiële erkenning van de Faculteit Militaire Wetenschappen als een wetenschappelijke instelling in 2011, de accreditering van de opleidingen als wetenschappelijke bachelors en masters in de jaren erna, en dus de oprichting van onderzoekscentra in 2022. Deze ontwikkelingen vertonen grote gelijkenis met die in ons omringende landen en in de Verenigde Staten en Canada. Ook elders in Europa zijn de militaire bedrijfswetenschappen inmiddels een geïnstitutionaliseerde component in militair wetenschappelijk onderwijs en onderzoek. Voorbeelden zijn het Defence Studies Department aan King's College in het Verenigd Koninkrijk, het Defensiecollege aan de Koninklijke Militaire School in België, de

14 E-H. Kramer, *De Militaire Bedrijfswetenschappen in Tien Stellingen: Een Sociotechnisch Perspectief*, oratie (Breda, Nederlandse Defensie Academie, 2020) 1-54.

15 Kramer, *De Militaire Bedrijfswetenschappen in Tien Stellingen*, 1-54.

16 Frerks, Kitzen, Remmits, Rietjens en Sweijs, 'Mars voorwaarts en voorwaarts mars', 398.

Fakultät Management aan de Führungsakademie der Bundeswehr in Duitsland, het Centre for Military Studies aan de Universiteit van Kopenhagen in Denemarken en de École Spéciale Militaire de Saint-Cyr (ESM) in Frankrijk. Resultaten van wetenschappelijk onderzoek worden gepubliceerd in academische tijdschriften met een gevestigde reputatie, waaronder krijgsmachtgerichte tijdschriften zoals *Defense and Peace Economics*, *Peace Science and Public Policy*, *Armed Forces & Society*, *Military Psychology* en *Journal of Military Ethics*. Door resultaten van academisch onderzoek in deze tijdschriften te publiceren dragen onderzoekscentra bij aan het valideren, delen, groeien en bestendigen van kennis. Vanuit het RC MMS kan vooral de Nederlandse onderzoeksbijdrage aan de militaire bedrijfswetenschappen zichtbaarder worden gemaakt.

De FMW hanteert het paradigma van *thinking soldiers*. Dit zijn enerzijds academische denkers die in staat zijn relevante kennis te absorberen, selecteren en exploiteren en anderzijds praktische doeners die die kennis in de praktijk kunnen brengen. Bedrijfskundig opgeleide officieren zijn dus academische professionals die door toepassing van wetenschappelijke inzichten in staat zijn oplossingen te bedenken en gebruiken voor de bedrijfskundige vraagstukken uit het militaire werkveld. Binnen de militaire bedrijfswetenschappen wordt het concept van de reflective practitioner als nadere duiding gebruikt. De reflective practitioner reflecteert constructief kritisch op de eigen praktijk en gebruikt theorie voor complexe praktijkproblemen. Reflective practitioners werken daarom ook interdisciplinair: ze verbinden inzichten uit verschillende bedrijfskundige disciplines om vraagstukken uit het veld in hun complexe samenhang op te lossen.¹⁷

Met de oprichting van het RC MMS wordt kritisch en direct relevant onderzoek gewaarsborgd naar het functioneren van de militaire organisatie. Dit is cruciaal voor een unieke

organisatie als de krijgsmacht die complexe processen moet organiseren in constant veranderende en soms dreigende omstandigheden, en noodzakelijk voor een organisatie die als 'instrument van de staat' en met een mandaat van de samenleving optreedt binnen en buiten onze nationale grenzen.

Het Research Centre Military Management Studies

De vakgroep Militaire Bedrijfswetenschappen heeft een zestal leerstoelen die verschillende disciplines vertegenwoordigen: Militaire Ethiek en Leiderschap, Militair Management en Organisatie, Civiel Militaire interactie, Militaire Logistiek, Defensie Economie en Arms Export Control. Vaak is het bedrijfswetenschappelijk onderzoek thematisch georiënteerd en daardoor leerstoeloverstijgend. Er wordt vanuit integraal perspectief onderzoek verricht op de volgende disciplinaire kruispunten, ofwel interdisciplinaire *hotspots*.

Mens en organisatie in extreme omstandigheden

Politieke opdrachten, sociale en culturele contexten, innovatieve technologie en organisatiestructuren plaatsen de militair voor vragen en dilemma's die ingrijpende consequenties kunnen hebben. Bijvoorbeeld op het gebied van ethiek, leiderschap en identiteit, morele, psychische en sociale dimensies van het militaire beroep, vorming, en systeemveiligheid. Binnen het RC MMS vindt onderzoek naar deze kwesties plaats vanuit geïntegreerde psychologische, filosofische, bedrijfswetenschappelijke en sociaalwetenschappelijke perspectieven, alsook vanuit geschiedkundige, economische en technologische expertise. Dit gebeurt op zowel het niveau van het individu en de groep als dat van de organisatie en de (internationale) samenleving, met expliciete aandacht voor de wendbare, onzekere, complexe en ambigue omstandigheden waarin hoog-risicoberoepen vandaag de dag opereren.

Lopend onderzoek richt zich bijvoorbeeld op de rol van organisatiefactoren in morele stress en verwonding, het creëren van een *just culture* in de

¹⁷ Opleidingsbestuur MBW Nederlandse Defensie Academie, *Zelfevaluatie rapport Opleiding Militaire Bedrijfswetenschappen* (Breda, Nederlandse Defensie Academie, 2022) 1-40.



Lopend onderzoek van het RC MMS richt zich bijvoorbeeld op de rol van het thuisfront in werk en welzijn

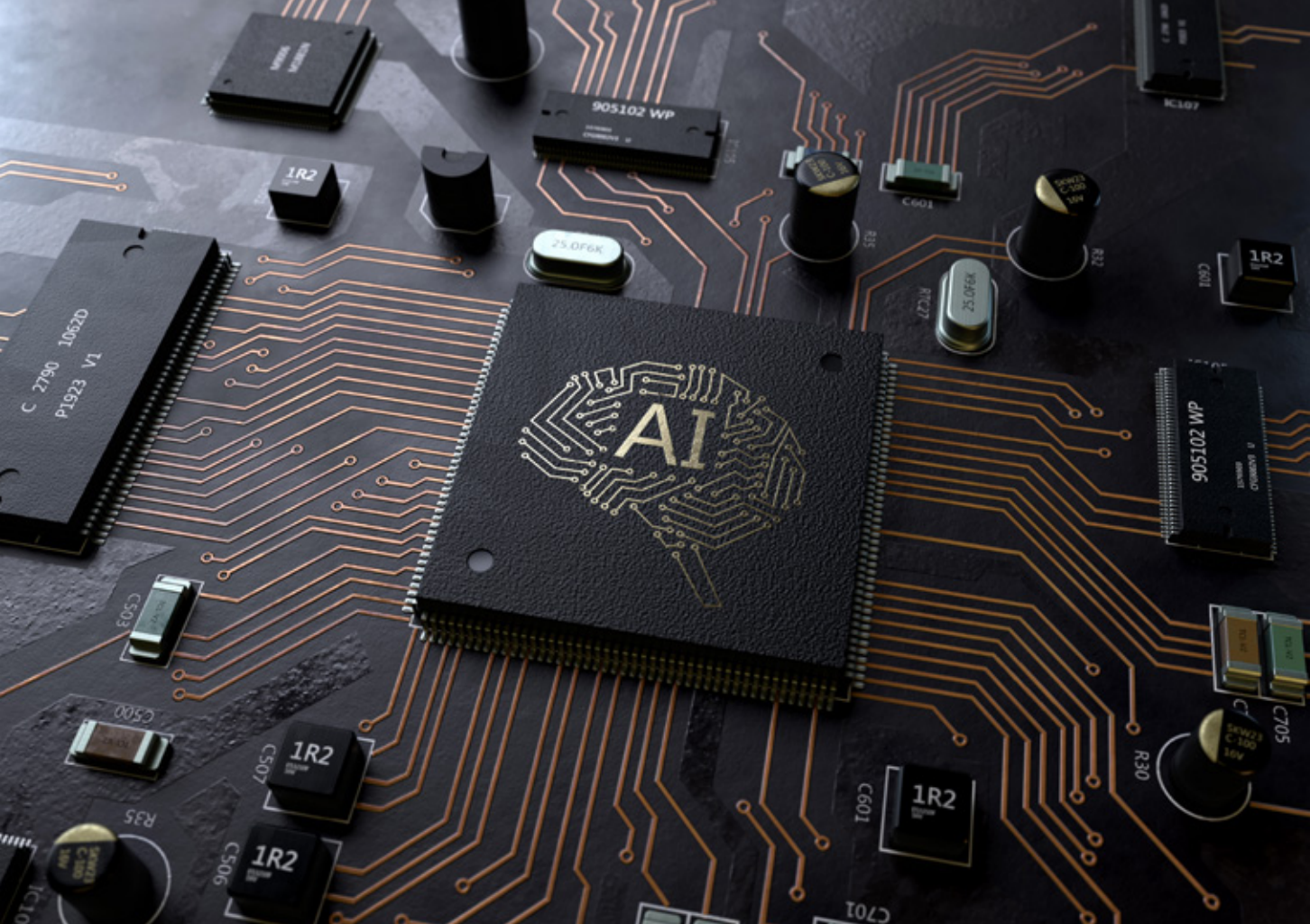
FOTO MCD, KEESNAN DOGGER

organisatie, ethisch leiderschap, de zorgbehoeftes van vrouwelijke veteranen en de rol van het thuisfront in werk en welzijn. Ook wordt speciale aandacht besteed aan de mogelijkheden van verschillende innovatieve technologieën, alsook aan de implementatie van die technologie in de organisatie. Vanuit het perspectief van militair medisch personeel wordt gewerkt aan een moreel-ethisch kader van toepassing op *soldier enhancement*. Dit helpt te bepalen wat de mogelijkheden zijn ten aanzien van het kunstmatig verbeteren van de fysieke of mentale menselijke capaciteiten, bijvoorbeeld door middel van medicatie of technische toepassingen. Daarnaast worden de psychologische en ethische dimensies van het werken met robotica en steeds autonomer werkende systemen onderzocht. In meer algemene zin wordt aandacht besteed aan AI-toepassingen in het militaire domein, bijvoorbeeld algoritmevalidatie en de ethische dilemma's die voortvloeien uit het gebruik van (semi)autonome wapensystemen. Op dit deelthema wordt eveneens onderzoek verricht naar de betekenis van klassieke militaire deugden in het licht van nieuwe manieren van oorlogvoering, naar effectief leiderschap in een hoogtechnologische

organisatie en naar de verhouding tussen innovaties en de sociale systemen waarin deze worden geïmplementeerd.

Innovatie en verbetering van de militaire bedrijfsvoering

Om de ambities van de Nederlandse krijgsmacht in termen van inzetbaarheid (*deployability*) en voortzettingsvermogen (*sustainability*) te realiseren, is het nodig dat bij besluitvorming de verschillende aandachtsgebieden in samenhang worden gezien. Om deze besluitvorming te monitoren worden prestatie-meetsystemen ontwikkeld en geïmplementeerd. Deze houden de organisatie 'op koers'. Digitale innovaties bieden nieuwe mogelijkheden voor inrichting. Binnen het RC MMS wordt fundamenteel en toegepast onderzoek verricht op het gebied van *performance management*. Dit onderzoek is gericht op diverse vraagstukken, onder andere ten aanzien van personele, materiele gereedheid en geoefendheid, materieel- en personeelslogistiek, maar ook financiën, de invloed van bezuinigen op de *deployability* en *sustainability* van de krijgsmacht, de implementatie van Vraag-Aanbod Management (VAM), Single Service Management (SSM) en Assortimentsgewijs werken (AGW) in



De krijgsmacht wil de wetenschappelijke kennisbasis van data science en AI versterken. Onderzoek van het RC MMS kan hieraan bijdragen

FOTO DARPA

een organisatie als de krijgsmacht. Ook wordt de implementatie van export control-regels onderzocht, strategische handelsregulering in relatie tot de inzetbaarheid van de krijgsmacht, en innovatie en management op het gebied van samenwerkingsrelaties met onder meer leveranciers.

Moderne defensieorganisaties ontwikkelen zich naar nieuwe manieren om in control te zijn. Zij combineren drie manieren van control en passen digitale innovatie geïntegreerd toe, gericht op proactieve bedrijfsvoering: controlprocessen over de lagen van hiërarchische niveaus waarbij sturingsinformatie en dashboards de juiste lagen met de juiste proactieve informatie betrekken; controlprocessen in de zin van ketenprestatie-management waarin deelprestaties zichtbaar en beheersbaar worden; en externe control met leveranciers en andere partners (smart contracts). Daarbij spelen moderne bedrijfsvoeringsconcepten, ERP-systemen, data analytics-projecten, en control towers een steeds

prominentere rol. Diverse onderzoeksprojecten werken deze thematiek uit.

De toekomst van werk en organisatie in het informatietijdperk

Op diverse terreinen is de militaire organisatie bezig met het ontwikkelen en implementeren van geavanceerde technologie. Veel digitale en informatietechnologie komt zowel terug in nieuwe wapenplatformen en communicatiemiddelen als in het ontwerp van ondersteunende systemen en processen. De toepassing van nieuwe technologie creëert enerzijds nieuwe mogelijkheden en vraagt om nieuwe manieren van organiseren. Anderzijds zijn (organisatie) keuzes bepalend voor de inzet (en gevolgen) van technologische toepassingen. Binnen het RC MMS worden diverse onderzoeksprojecten verricht, bijvoorbeeld op het gebied van tijd- en plaats-onafhankelijk werken in de militaire organisatie, de invloed van nieuwe technologische platformen op het functioneren van groepen en eenheden, data driven-procedures en

samenwerking binnen de krijgsmacht en met (civiele) partners buiten de krijgsmacht.

In het kader van ‘the future of work’ wordt bijvoorbeeld een onderzoekslijn ontwikkeld die zich richt op het vraagstuk van sociotechnische innovatie. Centraal hierin staat het vraagstuk van samenhang. Als technologie nieuwe mogelijkheden creëert, dan heeft het volgens dit perspectief potentieel invloed op strategie, operationele concepten, organisatiestructuur, groeps- en taakontwerp, maar ook op ethiek en de vormgeving van de bredere *governance*-netwerken waarin innovatieprojecten zijn ingebed. Nieuwe technologische mogelijkheden kunnen zo leiden tot vraagstukken op het gebied van organisatieontwerp en -ontwikkeling. Dit maakt innovatieprojecten potentieel bijzonder complex. Op dit moment wordt in verkennend onderzoek bestudeerd tegen welke typerende vraagstukken de krijgsmacht aanloopt als het gaat om het beheersen van de complexiteit die uit deze samenhang voortkomt.

Nieuwe ontwikkelingen: data science, ruimtetechnologie, IGO

Naast deze drie thema's zetten de drie onderzoekscentra gezamenlijk en in samenwerking met andere onderzoeksinstellingen in op onderzoek naar de meest actuele ontwikkelingen binnen Defensie en daarbuiten. Deze ontwikkelingen raken de krijgsmacht op alle vlakken en worden daarom ook vakgroepoverstijgend benaderd. Dit betekent zowel theoretische als methodologische kruisbestuiving, met onder meer de empirische datagerichtheid van Military Technology, de multidisciplinaire benadering van War Studies, en het holistische perspectief van Military Management Studies.¹⁸

Nieuwe ontwikkelingen in data science en kunstmatige intelligentie (AI) bieden kansen voor Defensie maar stellen ook hoge eisen aan onze organisatie. Het kan de manier waarop wij werken ingrijpend veranderen. Voor het behalen van de ambities uit de *Defensievisie 2035* wil de krijgsmacht de wetenschappelijke kennisbasis van data science en AI versterken. Hieraan kan ons onderzoek bijdragen. Tegelijkertijd is het belangrijk dat wij als onderzoekscentra kritisch

Het research centre verricht interdisciplinair, innovatief onderzoek op het gebied van militaire bedrijfsvoering, informatietechnologie en de mens in de organisatie

durven kijken naar technologische innovatie en de ambities op dit gebied. Dit betekent een open blik bij vraagstukken rondom ‘mogen, willen, kunnen’, waarbij de verkenning van technologische mogelijkheden samengaat met blijvende aandacht voor de mens.

Een andere belangrijke ontwikkeling vindt plaats in de ruimte. De ruimte is van cruciale waarde voor het civiele leven alsook voor het functioneren van moderne krijgsmachten. Ruimtetechnologie is een sleuteltechnologie die gebruikt wordt ten behoeve van onder andere omgevingsbewustzijn en het verzamelen van inlichtingen, en voor logistiek, navigatie en de geleiding van wapens. Daarnaast verwordt de ruimte zelf meer en meer een internationaal strijdtoneel. De NAVO erkent de ruimte tegenwoordig officieel als operationeel domein en meerdere landen experimenteren met wapens waarmee satellieten, de grondstations en/of de communicatielinks daartussen verstoord of uitgeschakeld kunnen worden. Zijn er daarom nieuwe spelregels nodig voor de ruimte? Hoe kan Defensie samenwerken met partners om optimaal gebruik te kunnen maken van ruimtetechnologie? Hoe kunnen wij onze systemen en die van bondgenoten beschermen tegen allerhande dreigingen?

Een laatste hier te noemen thema is informatie-gestuurd optreden (IGO). De defensieorganisatie moet weerbaar zijn tegen desinformatie van tegenstanders, en wil defensief en offensief kunnen optreden in het cyberdomein. Ook

¹⁸ Zie ook de nog te verschijnen *NL ARMS 2022*, waarin prof. dr. Robert Beeres ingaat op de methodologische verschillende en complementariteit van de verschillende onderzoekscentra.

wordt steeds meer gebruik gemaakt van sensoren om in het inzetgebied zicht te krijgen op de omgeving. Door die operationele data te verwerken tot informatie en gericht te delen met elkaar krijgen militaire eenheden snel een zo volledig mogelijk beeld. Een voorbeeld is het werkveld van Communication & Engagement, waarbij inzichten in de psychische, sociale, culturele en historische achtergronden van relevante actoren en de kenmerken van de civiele omgeving gebruikt worden voor meer militaire slagkracht binnen een operatie. Maar wat is IGO nu precies, en wat is het niet? Hoe kunnen we het effectief toepassen, hoe mogen we het inzetten, en hoe willen we dat doen? Het toegenomen aanbod van informatiebronnen levert namelijk niet alleen kansen, maar ook risico's op: niet alles wat technisch kan, is wenselijk. Welke juridische en ethische kaders zijn hier van toepassing, en hoe kunnen die vertaald worden naar concrete richtlijnen voor IGO?

Het Research Centre als samenwerkingsforum en platform

Natuurlijk verricht het RC MMS zijn onderzoek in dialoog en samenwerking met andere partijen, waarbij onderzoeksbevindingen niet alleen via academische kanalen maar ook op veel andere manieren worden gedeeld, zoals via congressen, Kamercommissies, beleidsadvies, informatiedagen van militaire eenheden, militair onderwijs, vakbladen, nieuwsmedia, social media, enzovoorts. Om deze redenen is het RC MMS te zien als een *forum* en een *platform*. Specifiek heeft het RC MMS de volgende doelstellingen:

- Bieden van een *forum* voor kennisuitwisseling en dialoog op het gebied van onderzoeksprojecten, actuele ontwikkelingen en relevante onderzoeksthema's. Dit gebeurt binnen de faculteit en in dialoog en/of samenwerking met het werkveld en andere onderzoeksinstellingen.
- Bieden van een *outreachplatform* voor delen van het onderzoek – en van de expertise die het RC MMS in huis heeft in bredere zin – met het academische en militaire werkveld, en met politiek en samenleving. Dit is allereerst een belangrijk doel op zichzelf, omdat het onder-

zoekscentrum op deze manier belanghebbenden en geïnteresseerden informeert over onderzoek en aldus bijdraagt aan de valorisatie van bevindingen. Daarnaast draagt het delen van onderzoek en expertise bij aan de opbouw en versteviging van relaties met het militaire en academische werkveld, en politieke en maatschappelijke actoren. Het doel hiervan is om het forum te verstevigen waarop verdere kennisuitwisseling en gezamenlijk onderzoek kan plaatsvinden.

- Onderzoek ontwikkelen en uitvoeren dat relevant is voor de opleiding van toekomstige officieren, en dit onderzoek ook vertalen naar academisch en beroepsonderwijs aan de NLDA. Zoals gezegd worden hier reflectieve practit ioners opgeleid die inzichten uit verschillende bedrijfskundige disciplines kunnen toepassen om vraagstukken uit het veld in hun samenhang op te lossen. De complexiteit van de militaire beroepspraktijk vraagt immers om reflectie en kritisch denken ten aanzien van wat het betekent om complexe processen te organiseren, van de rol die de officier inneemt in het militaire geheel, en van de verantwoordelijkheden die dat met zich meebrengt.
- Fungeren als een loket voor onderzoekers binnen het RC MMS en vragen en ideeën rondom onderzoek.

Slot

Juist nu door recente internationale ontwikkelingen een adequaat toegeruste krijgsmacht nog eens te meer van belang is en de Nederlandse regering onze krijgsmacht daarvoor langjarig een forse verhoging van financiële middelen heeft toegewezen is het de taak van die krijgsmacht haar potentieel te ontwikkelen en benutten, zodat deze investering in bedrijfs-economische zin haar rendement laat zien. De geschiedenis laat zien dat dat mogelijk is. Relevant bedrijfskundig academisch onderzoek kan bijdragen aan onder meer duurzamer investeren, betere control, betere civiel-militaire samenwerking en verantwoorde inzet van nieuwe technologie in defensieorganisaties. Daarmee kan ook beter worden voldaan aan maatschappelijke verwachtingen. ■

'Maybe Russia cannot be deterred'

Baltic perspectives on European security at the Lennart Meri Conference

Maarten Katsman MA

On NATO's eastern flank 'the threat is tangible', the *Militaire Spectator* reported after last year's Lennart Meri Conference in Tallinn, Estonia.¹ A year on, despite Russia's military setbacks and failure to reach its objectives in Ukraine, that is still the case. General Martin Herem, Commander of the Estonian Defence Forces, stated during the 2023 edition of the conference: 'Maybe Russia cannot be deterred.'² However, he added, 'the war in Ukraine teaches us that Russia can be beaten in our own home.' Despite suffering significant casualties — many more than during the Soviet Union's failed invasion in Afghanistan — the Russian military fights on with dogged determination. Therefore, to defend against a Russian invasion of Estonia or any other NATO Ally 'we should be prepared to kill each and every invader', General Herem said rather grimly.

General Martin Herem (r),
Commander of the Estonian
Defence Forces

PHOTO ICDS, ARNO MIKKOR



The opening panel of the 2023 Lennart Meri Conference (entitled ‘Incipit Vita Nova – So begins New Life’, hereafter LMC) featured the Prime Ministers of the three Baltic states, EU Commissioner Margrethe Vestager, and renowned historian Timothy Garton Ash. ‘We should have listened to Estonia earlier. Unfortunately, there’s nothing like real personal experience’, Garton Ash said about the Baltic states’ and Poland’s warnings concerning Russia’s malign intentions. Estonian Prime Minister Kaja Kallas added that ‘For Western Europe the peace after the end of the Second World War meant liberty and prosperity. The countries on the wrong side of the Iron Curtain also had peace, but we were not free and we suffered from severe oppression. Western European nations cannot understand what this was like.’

During a side event of the LMC, an Estonian official stressed the unity in his country with regard to the war in Ukraine. Even though the Riigikogu, the Estonian Parliament, is strongly divided about many domestic issues, a rather hawkish text on NATO-Ukraine relations received overwhelming support: 95 of the 101 Riigikogu members spoke out in favour. This can be explained by Estonia’s history and experience with Russia. ‘We know Russia very well’, the official said. ‘Nothing about Russia has surprised us for years, Moscow’s path has been extremely predictable. This war is an existential issue for Estonia because the outcome will determine new norms for European security.’ Prime Minister Kallas emphasised this existential threat from a different angle: ‘For a small country like ours, war means destruction and suffering. For empires (like President Vladimir Putin’s regime still perceives Russia to be, ed.) it means glory.’

‘Listen to the Baltics’

Kallas, labelled by some as Europe’s ‘new Iron Lady’, is on a mission to support Ukraine as much as possible. She has, for example, initiated the EU plan for joint procurement of ammunition. Kallas also called for a legal framework to try Russia in court: ‘When aggression pays off even a little bit, it is an invitation for more aggression.’ Therefore, ‘Russia must be held accountable. There can be no impunity, no immunity.’ The International Criminal Court can prosecute the Russian military for war crimes they committed but, Kallas said, ‘Before the military perpetrated those war crimes, the Russian leadership first committed a crime of aggression. We need a special tribunal to address that.’

Germany indeed experienced total defeat in 1945, making it possible for the victors to hold it to While Prime Minister Kallas refrained from saying out loud to Western Europe ‘we told you so’, some other speakers at the LMC did so vocally and continued to issue warnings. ‘The West invested in its own potential enemies, and with regard to China it might be making the same mistake again’, said one speaker, implying, ‘Listen to the Baltics, follow their example’. Poland has ambitious plans to set such an example. Warsaw wants to acquire no less than 1,600 modern tanks, as was outlined in one of the LMC discussion panels, and it aims to have the most powerful land force in Europe. With capabilities like that, in the event of a Russian attack against Poland, the Polish military could bring the fight to ‘the Russians’ own area, which is the only way they can be stopped’, one speaker said, echoing General Herem’s comments.

Total defeat?

Over the course of the conference and side events, several speakers alluded to the need for internal change in Russia. Unlike Germany after 1945, Russia, after the collapse of the Soviet Union was never forced to account for the crimes of its former dictatorial regime. Looking

1 Dr. Frans van Nijnatten, ‘The threat is tangible’, *Militaire Spectator*, June 12, 2022. See: <https://militairespectator.nl/artikelen/threat-tangible>.

2 The Lennart Meri Conference was held on 12-14 May in Tallinn, Estonia. Most of the sessions were subject to Chatham House Rules, so many speakers’ names and affiliations will not be mentioned in this article. See: <https://lmc.icds.ee/>.



NATO exercise in Sweden, with, among others, participation from Estonian forces. General Herem: 'We need to prepare for war, with supplies and mentality'

PHOTO NATO

forward into the future, Latvian Prime Minister Krišjānis Kariņš proclaimed that 'To have true peace in Europe, profound defeat of Russia is needed. But we also need Russia to change so we wouldn't be coming back to this place again.' Some way or other the West will eventually have to deal with Russia again. It may take several generations, however, to establish a relationship built on trust, and only if Russian society goes through a process of fundamental change. Regaining trust is not impossible, as evidenced by NATO's eastern members' call for German leadership and strength in the current crisis, something that had long been unthinkable in the post-WWII era.

Germany indeed experienced total defeat in 1945, making it possible for the victors to hold it to account for its heinous actions before and during the war. Such circumstances do not apply to Russia today, so real change has to come from the Russian people itself. In fact it is 'Russia's tragedy', said historian Timothy Garton Ash, 'that it cannot suffer a defeat like Germany did.'

That defeat is the foundation upon which Germany's freedom, democracy and prosperity are built.' In the spirit of the LMC's theme ('So Begins New Life'), Garton Ash added that the war in Ukraine 'provides opportunities for a better Europe.' But in order to achieve this, 'we must put the illusion of a post-war Europe behind us and support Ukraine until it wins a clear, decisive military victory.' He continued: 'To seize this chance we have to prepare actively for the second great, double eastward enlargement of the geopolitical West: EU and NATO, both. The Western Balkans, Ukraine, Moldova, Georgia, all of them should be on the path to membership in both organisations. To expand the frontiers of a Europe "whole and free" is a strategic goal.'

Until then, in case Russia may not be deterred from further aggression, Western Europe should listen to the Baltics. To conclude with Estonia's Defence Chief General Herem: 'We need to prepare, and really prepare for war. With supplies and mentality.' ■

Waarom de NAVO niet zonder Turkije kan

Niels van de Ven MSc*

Turkije maakt sinds 1952 deel uit van de NAVO en door de jaren heen heeft dat voor bepaalde spanningen gezorgd in het bondgenootschap. Turkije, dat na de VS de grootste krijgsmacht van de alliantie heeft, probeert op te treden als een (zelfstandig opererende) regionale grootmacht en vaart hierdoor een koers die niet altijd aansluit bij de belangen van zijn NAVO-partners. Tegenstanders van het Turkse lidmaatschap voeren vaak normatieve standpunten aan, terwijl voorstanders vooral kijken naar de militaire en geopolitieke gevolgen van een eventuele Turkse uittreding. Welk kamp heeft de meest doorslaggevende argumenten?



Turkse militairen die deel uitmaken van de Very High Readiness Joint Task Force van de NAVO tijdens de oefening Steadfast Defender 2021

FOTO NAVO

In 1952 werd Turkije lid van de NAVO, waarmee het al langer onderdeel uitmaakt van het bondgenootschap dan bijvoorbeeld (West-) Duitsland (1955) en Spanje (1982). De toetreding kwam voor velen niet als een verrassing, aangezien Turkse militairen enkele jaren eerder in de Koreaoorlog (1950-1953) al zij-aan-zij hadden gevochten met verschillende westerse landen tegen China, Noord-Korea en de Sovjet-Unie. Tijdens de Koreaoorlog maakte de getoonde moed van de Turkse militairen, van wie er uiteindelijk zeventien sneuvelden en enkele duizenden gewond raakten, veel indruk op de bondgenoten.^{1, 2} Niet alleen het Turkse

optreden in de Koreaoorlog, maar ook de Koude Oorlog, die op dat moment in volle gang was, speelde een rol in de toetreding van Turkije tot de NAVO. Voor het Westen – en de Verenigde Staten in het bijzonder – maakte de strategische ligging Turkije tot een interessante partner.

* Niels van de Ven is werkzaam bij het ministerie van Defensie. Dit artikel is een bewerking van een essay dat is geschreven voor het vak Internationale Veiligheid Studies (IVS) tijdens de Middelbare Defensie Vorming (2022).

1 HistoryNet Staff, 'Korean War: 1st Turkish Brigade's Baptism of Fire', 6 december 2006. Zie: <https://www.historynet.com/korean-war-1st-turkish-brigades-baptism-of-fire/>.

2 Francesco Bongiovanni, 'Turkey: The Nato Alliance's Wild Card', *Turkish Policy Quarterly* 17 (2) (2018) 53-62: blz. 54.



Zo hoopte het Westen Turkije te kunnen gebruiken als een buffer tussen de Sovjet-Unie en landen in het Midden-Oosten enerzijds en het oostelijk deel van de Middellandse Zee anderzijds, om zo te voorkomen dat het communisme zich ook naar die gebieden zou verspreiden. Bovendien konden er ook strategisch belangrijke militaire basissen op Turks grondgebied gevestigd worden.³

Hoewel Turkije vanaf de jaren 50 lange tijd een gewaardeerde partner in het bondgenootschap was, zijn er sinds 2011 langzaam scheuren ontstaan in de relatie met de overige lidstaten en de NAVO als geheel.⁴ De hoofdoorzaak van deze spanningen is dat Turkije probeert op te treden als een (zelfstandig opererende) regionale grootmacht en hierdoor een koers vaart die niet altijd aansluit bij de belangen van zijn NAVO-partners.⁵ Zo leeft Turkije al sinds jaar en dag op

gespannen voet met buurland en NAVO-lidstaat Griekenland en lopen deze spanningen de laatste jaren steeds verder op, onder meer als gevolg van de Turkse assertiviteit rond de Egeïsche zee.⁶ Het Turkse optreden in Syrië – waar de Turkse krijgsmacht rond het Turks-Syrische grensgebied optreedt samen met door Turkije gesteunde rebellengroepen – zorgt ook voor wrevel bij NAVO-partners, waaronder de VS.⁷ Daarnaast onderhoudt Turkije als een van de weinige NAVO-lidstaten ook een vriendschappelijke relatie met Rusland. Zo kocht Turkije een geavanceerd luchtafweersysteem (de S400) van Rusland⁸ en is Turkije een van de weinige Europese landen die Moskou geen sancties heeft opgelegd naar aanleiding van de inval in Oekraïne in februari 2022.⁹ Op de achtergrond spelen ook nog andere wrijvingen, zoals de diplomatieke spanningen tussen Nederland (en Duitsland) en Turkije in 2017,¹⁰ spanningen met Frankrijk¹¹ en de erkenning van de Armeense genocide door de VS.¹² Daarnaast maken meerdere NAVO-bondgenoten zich ook zorgen om de situatie in Turkije zelf, onder meer op het gebied van mensenrechten.¹³ Dergelijke spanningen hebben de relatie tussen de overige NAVO-lidstaten en Turkije geen goed gedaan.

Als gevolg van de fricties met Turkije wordt in het publieke debat met enige regelmaat geopperd dat het land uit de NAVO zou moeten worden verwijderd.¹⁴ Hoewel dergelijke *statements* vanuit de emotie wellicht te begrijpen zijn, zou de NAVO mijns inziens een gigantische (strategische) blunder begaan als zij ertoe besluit Turkije daadwerkelijk uit het bondgenootschap te weren. In dit betoog zal ik verder toelichten waarom een vertrek van Turkije uit de NAVO de positie van de alliantie ernstig zou verzwakken.

Argumenten voor een Turks lidmaatschap van de NAVO

Een Turks vertrek zou onder meer pijn doen omdat Turkije, na de VS, de grootste krijgsmacht in de NAVO heeft en daarmee ook de grootste krijgsmacht van de alliantie op het Europese continent. De Turkse krijgsmacht beschikte in 2021 over ongeveer 750.000 actief dienende

- 3 Ayşe Atmaca, 'The Geopolitical Origins of Turkish-American Relations: Revisiting the Cold War Years', *All Azimuth A Journal of Foreign Policy and Peace* 3 (1) (2014) 19-34.
- 4 Yaprak Gürsoy en Ilke Toygür, 'Turkey in and out of NATO? An instance of a turbulent alliance with Western institutions', *Elcano Royal Institute*, 11 juni 2018) 2.
- 5 'The Erdogan Doctrine: Turkey's regional strategy', *Al Jazeera*, 15 oktober 2020. Zie: <https://studies.aljazeera.net/en/policy-briefs/erdogan-doctrine-turkey%E2%80%99s-regional-strategy>.
- 6 'Turkey opens new dispute over sovereignty of east Aegean islands', *Al Jazeera*, 8 februari 2022. Zie: <https://www.aljazeera.com/news/2022/2/8/turkey-opens-new-dispute-over-sovereignty-of-east-aegean-islands>.
- 7 Elettra Pelino, 'The 2018 Turkish Military Operation in Northern Syria: Turkey's Ambiguous Realpolitik Between the USA and Russia', *I Report dell'IsAG* (december 2018) 5.
- 8 'Russia starts delivery of S-400 missile system to Turkey, setting up standoff with US', *CNN*, 12 juli 2019. Zie: <https://edition.cnn.com/2019/07/12/europe/turkey-russia-missiles-intl/index.html>.
- 9 'Turkey will not join Western sanctions against Russia – foreign minister', *TASS*, 13 maart 2022/. Zie: <https://tass.com/politics/1421411>.
- 10 'Dit weten we over de diplomatieke rel tussen Nederland en Turkije', *NU.nl*, 11 maart 2017. Zie: <https://www.nu.nl/dvn/4533696/weten-we-diplomatieke-rel-tussen-nederland-en-turkije.html>.
- 11 Tim Ogden, 'It's time to expel Turkey from Nato', *The Spectator*, 30 oktober 2020. Zie: <https://www.spectator.co.uk/article/it-s-time-to-expel-turkey-from-nato/>.
- 12 'Biden erkent Armeense genocide, tot woede van Turkije', *RTL Nieuws*, 24 april 2021. Zie: <https://www.rtlnieuws.nl/nieuws/buitenland/artikel/5227297/armeense-genocide-biden-erkenning-turkije-woede-herdenking>.
- 13 'EU en VS waarschuwen Turkije mensenrechten te respecteren', *Trouw*, 18 juli 2016. <https://www.trouw.nl/nieuws/eu-en-vs-waarschuwen-turkije-mensenrechten-te-respecteren~b5a9e452/>.
- 14 Zie bijvoorbeeld Tim Ogden, 'It's time to expel Turkey from Nato'; Alon Ben-Meir, 'Time To Kick Turkey Out Of NATO', *The Jerusalem Post*, 8 november 2017. Zie: <https://www.jpost.com/blogs/above-the-fray/time-to-kick-turkey-out-of-nato-513757>; Geert Willders, 'Kick Turkey out of NATO!', zie: <https://twitter.com/geertwilderspvv/status/1310285712038789120>.



De Amerikaanse president Joe Biden overlegt tijdens de NAVO-top in Madrid in 2022 met zijn Turkse ambtgenoot Recep Tayyip Erdogan

FOTO WITTE HUIS, ADAM SCHULTZ

militairen.¹⁵ Ook leverde Turkije een kleine duizend militairen voor NAVO-missies in 2021,¹⁶ speelt het een belangrijke rol in de Very High Readiness Joint Task Force (VJTF)¹⁷ en levert het een bijdrage aan de vredesoperatie van de NAVO in Kosovo.¹⁸ Bovendien heeft de Turkse krijgsmacht zich de afgelopen jaren bewezen in onder meer Syrië en Irak.¹⁹ Daarnaast heeft Turkije een relatief grote defensie-industrie,²⁰ die ook steeds vaker haar meerwaarde toont, bijvoorbeeld in het conflict om Nagorno-Karabach²¹ en op dit moment in Oekraïne.²² Een NAVO-lidstaat met een dergelijke capaciteit kan van enorme toegevoegde waarde zijn voor het westerse bondgenootschap, terwijl het juist problematisch kan worden op het moment dat Turkije de alliantie zou verlaten. Bovendien zou de NAVO de toegang tot verschillende in Turkije gelegen basissen verliezen, zoals de luchtmachtbasissen in Incirlik en Konya.^{23, 24} Incirlik is van cruciaal belang bij operaties door het bondgenootschap of NAVO-lidstaten in het

- 15 International Institute for Strategic Studies, *The Military Balance 2021* (Londen, Routledge, 2021) 152.
- 16 Atlantic Council, 'NATO allies contribute to a variety of missions. Here's a look at how each country chips in', 11 juni 2021. Zie: <https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-allies-contribute-to-a-variety-of-missions-heres-a-look-at-how-each-country-chips-in/>.
- 17 De VJTF is een eenheid die in permanente staat van paraatheid verkeert en daardoor meteen en als eerste kan worden ingezet bij dreiging tegen de soevereiniteit van de NAVO.
- 18 Mehmet Yegin, 'Turkey between NATO and Russia: the failed balance. Turkey's S-400 purchase and implications for Turkish relations with NATO' (Berlijn, Stiftung Wissenschaft und Politik, 2019) 2.
- 19 Karagiannis, E. (2020). Five reasons why the West will lose Turkey. BESA Center Perspectives Paper: p. 2
- 20 Ferhat Gurini, 'Turkey's unpromising defense industry' (Carnegie Endowment for International Peace, 9 oktober 2020).
- 21 Kareem Fahim, 'Turkey's military campaign beyond its borders is powered by homemade armed drones', *The Washington Post*, 29 november 2020. Zie: https://www.washingtonpost.com/world/middle_east/turkey-drones-libya-nagorno-karabakh/2020/11/29/d8c98b96-29de-11eb-9c21-3cc501d0981f_story.html.
- 22 'Turkey is the arms industry's new upstart', *The Economist*, 12 februari 2022. Zie: <https://www.economist.com/europe/2022/02/12/turkey-is-the-arms-industrys-new-upstart>
- 23 Yegin, 'Turkey between NATO and Russia', 2.
- 24 Dorith Kool, Patrick Bolder en Murat Dogan, *Turkey's Recalcitrance and NATO's Nuisance* (Den Haag, The Hague Centre for Strategic Studies, 18 februari 2021) 9.

Midden-Oosten, bijvoorbeeld in de strijd tegen Islamitische Staat in Syrië en Irak. Daarnaast liggen er op de basis ook nucleaire wapens van de VS opgeslagen²⁵ en dienen de Turkse basissen als afschrikingsmechanisme richting zowel Rusland als Iran.²⁶

Een vertrek van Turkije uit de NAVO zou Rusland in de kaart spelen. Niet alleen zou het NAVO-bondgenootschap verzwakt zijn, maar het kan er ook toe leiden dat Turkije in de armen wordt gedreven van Moskou. Hoewel Turkije probeert op te treden als regionale grootmacht, zal het zich immers ook realiseren dat het bij een vertrek uit de NAVO niet bij machte is om

unilateraal de eigen veiligheid te garanderen. Zodoende zou uittreding van Turkije niet alleen de NAVO verzwakken; het zou ertoe kunnen leiden dat de NAVO ineens een machtig Russisch-Turks bondgenootschap aan haar oostgrens heeft.²⁷ Daarnaast kan ook niet worden uitgesloten dat Turkije bij een vertrek uit de NAVO de toch al aangehaalde banden met een andere systeemrivaal van het Westen, China, verder versterkt.²⁸

Daarnaast is Turkije, naast Albanië, de enige NAVO-lidstaat met een overwegend islamitische bevolking. Voor de NAVO biedt het Turkse lidmaatschap daarmee ook een bepaalde toegang tot de Arabische en islamitische wereld²⁹ en het lidmaatschap zorgt er ook voor dat interventies door het bondgenootschap op meer begrip kunnen rekenen in de islamitische wereld. Zonder de Turkse presentie wordt het voor de NAVO waarschijnlijk moeilijker om dergelijke interventies te 'verkopen' buiten het Westen.³⁰ In het verlengde hiervan kan ook gesteld worden dat de assertievere geopolitieke rol van Turkije juist een kans is voor het Westen. Terwijl het Westen zich steeds verder terugtrekt uit het Midden-Oosten en Afrika probeert Turkije hier juist voet aan de grond te krijgen. Zo is Turkije actief in Somalië,³¹ Libië³² en Djibouti.³³ Juist in Noord-Afrika en de Hoorn van Afrika liggen ook veel (veiligheids)belangen voor het Westen.^{34, 35} Via Turkije of door Turkse bemiddeling kunnen westerse landen alsnog proberen hun belangen in dergelijke landen veilig te stellen, juist in een periode dat het Westen aan invloed verliest in de regio's.^{36, 37}

Het belang van de geografische ligging van Turkije mag ook niet onderschat worden. Door de ligging van Turkije vormt het land in feite een buffer tussen Europa, Rusland en de Arabische landen in het Midden-Oosten.³⁸ Ook ligt Turkije aan de Zwarte Zee en kan het dankzij het Verdrag van Montreux andere landen de toegang tot deze strategische wateren ontzeggen³⁹ door landen te verbieden de door Turkije gecontroleerde zeestraten Bosporus en Dardanellen te bevaren,⁴⁰ zoals het bijvoorbeeld op dit moment doet als gevolg van de Russische inval in Oekraïne.⁴¹

- 25 'Why are US military bases in Turkey so crucial for Washington?', *TRT World*, 16 december 2019. Zie: <https://www.trtworld.com/magazine/why-are-us-military-bases-in-turkey-so-crucial-for-washington-32243>.
- 26 Kool, Bolder en Dogan, *Turkey's Recalcitrance and NATO's Nuisance*, 3.
- 27 Bongiovanni, 'Turkey: The Nato Alliance's Wild Card' 59.
- 28 Kool, Bolder en Dogan, *Turkey's Recalcitrance and NATO's Nuisance*, 6.
- 29 Ibrahim Aoudé, 'Turkey and its immediate Arab neighbors in the twenty-first century', *Arab Studies Quarterly* 42 (1-2) (2020) 91-108: blz. 92.
- 30 Muge Kinacioğlu, 'NATO-Turkey Relations. From Collective Defence to Collective Security', in: Pinar Ercan (red.), *Turkish Foreign Policy. International Relations, Legality and Global Reach* (Londen, Palgrave Macmillan, 2017) 83-103: blz. 98.
- 31 'A decade of Turkey's rise in Somalia', *TRT World*, 25 augustus 2021. Zie: <https://www.trtworld.com/magazine/a-decade-of-turkey-s-rise-in-somalia-49451>.
- 32 Idem.
- 33 'Djibouti seeks greater Turkish presence in country', *Daily Sabah*, 14 maart 2019. Zie: <https://www.dailysabah.com/diplomacy/2019/03/14/djibouti-seeks-greater-turkish-presence-in-country>.
- 34 'Veiligheid van Europa in het geding door onstabiel Noord-Afrika', HCSS, 1 februari 2013. Zie: <https://hcss.nl/news/veiligheid-van-europa-in-het-geding-door-onstabiel-noord-afrika/>.
- 35 Rijksoverheid, 'Notitie Geïntegreerde Buitenland- en Veiligheidsstrategie (GBVS) met bijlagen', 14 mei 2018. Zie: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs/Notitie+GBVS.PDF>.
- 36 Francis Ghilès, 'How France is losing influence across North Africa', *Middle East Eye*, 19 januari 2022. Zie: <https://www.middleeasteye.net/opinion/how-france-losing-influence-across-north-africa>.
- 37 Atlantic Council, 'The US risks losing its influence in the Horn of Africa. Here's how to get it back', 11 januari 2022. Zie: <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-us-risks-losing-its-influence-in-the-horn-of-africa-heres-how-to-get-it-back/>.
- 38 Bongiovanni, 'Turkey: The Nato Alliance's Wild Card', 61.
- 39 Zo vormt de Zwarte Zee voor Rusland de toegang tot de Middellandse Zee.
- 40 Nezihi Çakar, 'A strategic overview of Turkey. Perceptions', *Journal of International Affairs* 3 (2) (1998) 1.
- 41 'Turkey blocks Black Sea passage for Russian naval vessels', *Nikkei*, 1 maart 2022. Zie: <https://asia.nikkei.com/Politics/Ukraine-war/Turkey-blocks-Black-Sea-passage-for-Russian-naval-vessels>.



FOTO: US DEPARTMENT OF DEFENSE, DOMINIQUE PINERO

De Turkse chefstaf generaal Hulusi Akar en zijn Russische ambtgenoot Valery Gerasimov praten in 2017 in Antalya over operaties in Noord-Syrië: een vertrek uit de NAVO zou Turkije verder richting Moskou kunnen laten drijven

Argumenten tegen een Turks lidmaatschap van de NAVO

Zij die Turkije het liefst zien vertrekken uit de NAVO zullen stellen dat de nadelen die een vertrek van Turkije met zich meebrengt niet opwegen tegen de spanningen van het Turkse lidmaatschap, die het bondgenootschap ondermijnen.⁴² Maar juist een vertrek van Turkije uit de NAVO zou er toe kunnen leiden dat deze spanningen tot een kookpunt komen, terwijl het Turkse lidmaatschap er voor kan zorgen dat de spanningen juist binnen de perken blijven en diplomatiek opgelost worden. Zo heeft de Turkse en Griekse toetreding er juist voor gezorgd dat dergelijke spanningen op diplomatiek niveau besproken worden.^{43, 44} Gelet op de nog immer aanwezige frictie tussen beide landen zou een

vertrek van Turkije uit de NAVO er juist voor kunnen zorgen dat deze spanning (opnieuw) hoog oploopt. Hetzelfde geldt bijvoorbeeld voor (de strijd in) Noord-Syrië, waar bij een Turks vertrek uit het bondgenootschap escalatie op de loer ligt in het toch al sluimerende conflict tussen de door het Westen gesteunde groten-deels Koerdische People's Defense Units (YPG) enerzijds en Turkije en door Turkije gesteunde rebellengroepen anderzijds.

42 Ogden, 'It's time to expel Turkey from Nato'.

43 Aoudé, 'Turkey and its immediate Arab neighbors in the twenty-first century', 92.

44 Valentin Naumescu, 'Stability, ambiguity and change in the discourses of NATO allies in the Black Sea region: The cases of Romania, Bulgaria and Turkey', *Croatian International Relations Review* 23 (80) (2017) 187-209: blz. 189.

Tegenstanders van het Turkse lidmaatschap van de NAVO beroepen zich ook op meer normatieve argumenten, zoals dat Turkije alsmaar autoritairder wordt⁴⁵ en vanwege zorgen om persvrijheid⁴⁶ en de mensenrechtensituatie in het land.⁴⁷ Dergelijke argumenten hadden zeker hout gesneden wanneer deze betrekking hadden gehad op de Turkse toetreding tot de Europese Unie (EU), maar de argumenten slaan de plank mis als het gaat om het Turkse lidmaatschap van de NAVO. Niet alleen zijn er ook andere lidstaten waar (onder meer) de rechtsstaat en persvrijheid onder vuur liggen, zoals Hongarije en Polen,^{48, 49} ook is de NAVO in de eerste plaats een defensief militair bondgenootschap, gericht op de verdediging van het grondgebied van de alliantie.⁵⁰ Dit in tegenstelling tot de EU, waar (de verspreiding van) de Europese normen en waarden, zoals democratie, persvrijheid en een goed functionerende rechtsstaat ook centraal staan.⁵¹ Dat democratie, persvrijheid en de rechtsstaat in Turkije onder vuur liggen is absoluut betreurenswaardig, maar betekent niet dat het land niet langer deel uit kan maken van de NAVO.

Conclusie

Een vertrek van Turkije uit de NAVO zou het westerse bondgenootschap op verschillende manieren ernstig kunnen verzwakken. Allereerst zou de NAVO haar op een na grootste krijgsmacht verliezen en daarbij ook de toegang tot een aantal belangrijke militaire basissen die zich op Turks grondgebied bevinden. Daarnaast



FOTO NAVO

zou het Turkse vertrek ook de grote rivalen, Rusland en China, in de kaart spelen en zou het Westen zelfs het risico lopen dat Turkije in de armen wordt gedreven van deze twee landen. Verder zou het voor de NAVO bij een Turks vertrek ook moeilijker worden om te opereren met of in de islamitische wereld, terwijl het Westen in landen in deze regio (denk onder meer aan Noord-Afrika) wel zwaarwegende

45 Ogden, 'It's time to expel Turkey from Nato'.

46 Ben-Meir, 'Time To Kick Turkey Out Of NATO'.

47 'EU en VS waarschuwen Turkije mensenrechten te respecteren', *Trouw*.

48 Robert Tait, 'Media Freedom is 'in danger', survey in four central European countries finds', *The Guardian*, 26 april 2022. Zie: <https://www.theguardian.com/media/2022/apr/26/media-freedom-is-in-danger-survey-in-four-eastern-european-countries-finds>.

49 Judy Dempsey, 'What Ukraine Reveals About NATO and the EU', *Carnegie Europe*, 1 februari 2022. Zie: <https://carnegieeurope.eu/strategieurope/86325>.

50 Dempsey, 'What Ukraine Reveals About NATO and the EU'.

51 Naja Bentzen, 'Protecting, promoting and projecting Europe's values and interests in the world', *European Parliamentary Research Services, Ideas Paper Towards a more resilient EU*. PE 652.061, 12 september 2022. Zie: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652061/EPRS_BRI\(2020\)652061_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652061/EPRS_BRI(2020)652061_EN.pdf).



Turkije heeft met ongeveer 750.000 actief dienende militairen de de grootste krijgsmacht van de alliantie op het Europese continent

veiligheidsbelangen heeft. Daarnaast zouden de immer aanwezige spanningen tussen Griekenland en Turkije bij een Turks vertrek zomaar kunnen escaleren, net zoals de spanningen in Noord-Syrië. Argumenten tegen het Turkse lidmaatschap van de NAVO hebben voornamelijk een normatief karakter, maar gaan in het kader van een defensieve militaire alliantie niet op.

Hoewel Turkije voor spanningen zorgt in de NAVO heeft dit betoog aangetoond dat het bondgenootschap simpelweg niet zonder Turkije kan. Of, om met Francesco Bongiovanni te spreken: 'het enige dat erger is dan Turkije in de NAVO, is Turkije uit de NAVO'.⁵² ■

52 Bongiovanni, 'Turkey: The Nato Alliance's Wild Card', 58.

Vertrouwen

Frans Matser

Volgens een bekend gezegde komt vertrouwen te voet en vertrekt het te paard. Met die wijsheid in gedachten valt het mij op dat het bij een groot deel van het (gewezen) defensiepersoneel niet erg goed zit met het vertrouwen in de organisatie als werkgever. Dat valt onder meer op te maken uit een al jarenlange te hoge uitstroom, maar ook uit de populariteit van socialemediagroepen waar defensiemedewerkers op krachtige wijze hun beklag doen over het personeelsbeleid. Hoe is het toch gekomen, dat een in het verleden toch als zeer loyaal bekend staande groep zich tegenwoordig vooral kritisch uitlaat over haar (voormalige) werkgever?

Het begon natuurlijk allemaal met de bezuinigingen in de vorige eeuw. Mensen die jarenlang was verzekerd dat ze *lifetime employment* hadden, leken tot hun schrik prooi te worden van bezuinigingsgeneraals en hun projectgroepen die vanaf de jaren 80 met grote regelmaat de ene na de andere bezuinigingsoperatie lanceerden. Allemaal met één doel: zoveel mogelijk functies uit de organisatie te 'kloppen'. Het ene moment was je nog een gewaardeerd adjudant van de mariniers of majoor van de artillerie en het volgende moment was je gereduceerd tot lid van een overtolligheidscategorie. Duizenden kaderleden werden, met zachte of harde hand, uit de organisatie verwijderd. Dat kwam bij velen, ook degenen die uiteindelijk mochten blijven, als een flinke schok aan.

De relatie tussen werkgever en werknemer is volgens de organisatiepsychologie gebaseerd op een 'moreel contract'. Zo'n contract, dat niet noodzakelijkerwijs op papier hoeft te staan, schept naar twee kanten verplichtingen.

Plotseling echter trekt een van de partijen, eenzijdig, zich niets meer van die verwachtingen aan. Het is niet moeilijk te begrijpen dat hier de eerste kiem werd gelegd voor een vertrouwensbreuk tussen de defensieleiding en haar personeel.

Met werkonzekerheid hield het echter niet op. Tal van andere afspraken bleken plotseling niet zo hard als de werknemers hadden gedacht. Zo werden veel opleidingen ingekort door er vooral veel 'leuke' dingen uit te halen. Militaire rijbewijzen voor officieren en onderofficieren waren plotseling niet meer nodig. Gevechtscursus, de Vierdaagse en parachutespringen werden uit het opleidingscurriculum geschrapt. Voor veel mensen die geworven waren met die arbeidsvoorwaarden bleek het woord van de werkgever plotseling niet veel waard te zijn. Wat een sergeant-majoor van de wervingsorganisatie bij de voorlichting mondeling had beloofd, bleken beleidsmakers op het ministerie een jaar later met één simpele penningstreek te kunnen herzien. Natuurlijk, er moest bezuinigd worden en het personeel moest daaraan zijn bijdrage leveren. Wie niet wilde slikken... kon stikken.

Geleidelijk aan kwam ook de pensioenleeftijd in het vizier. Plotseling moesten mensen jaren langer gaan werken dan ooit met hen afgesproken was. En passant werd het tot dan toe waardevaste pensioen aan het ABP overgedaan, waarna al heel snel de jaarlijkse indexatie ophield. Ja, regels van het pensioenfonds hè! Sorry jongens, pech gehad.

Daarna kwamen de affaires met de Wet Uniformering Loonbegrip en het pensioengat, waarbij de werkgever, die altijd de



mond vol had gehad over de bijzondere positie van de militair, ineens de schouders ophaalde over financiële gevolgen die algemene wettelijke aanpassingen – geheel onbedoeld – voor defensiewerknemers hadden. Loyale mannen en vrouwen die al jaren bij ons werkten dreigden voor tienduizenden euro's gedupeerd te worden. En de werkgever? Die vond dat allemaal best. 'Niet ons probleem', klonk het uit de krochten van het ministerie, waar technocratische burgers van de algemene bestuursdienst al jaren de voeling met de basis van de organisatie volledig kwijt zijn. 'Moreel contract? Waar staat dat dan?'

Goed genomen kon dit door de werknemers van Defensie niet anders vertaald worden dan dat hun werkgever onverschillig stond tegenover elke aantasting van hun rechtspositie en zich laf verschool achter algemeen overheidsbeleid. Dat het pensioengat uiteindelijk werd gedicht was niet het gevolg van het tot inzicht komen van Defensie, maar te danken aan de bijna tien jaar durende strijd van één standvastig individu, LTZ b.d. Loek van den Heuvel, die zich vastbeet in deze zaak en via sociale media ruim 6000 medestanders wist te mobiliseren. Uiteindelijk wist hij via een zware juridische strijd en tal van politieke acties en demonstraties een (gedeeltelijke) oplossing af te dwingen. De boodschap was duidelijk: bij Defensie kan een fatsoenlijke behandeling niet anders dan met zware druk en juridische middelen voor de poorten van de ministeriële hel worden weggesleept. Zo iets blijft hangen.

Recentelijk startten andere activistische oud-medewerkers een actie om de 20 procent achtergebleven pensioenindexatie aan te pakken.¹ Binnen enkele weken werd met een crowdfundinginitiatief onder defensiemedewerkers zonder veel problemen de noodzakelijke 30.000 euro bij elkaar gebracht. Ruim 1300 (ex)defensiemedewerkers bleken bereid om bedragen variërend van enkele tientjes tot een paar honderd euro te doneren om een rechtszaak tegen hun (ex)-werkgever aan te spannen. Want één ding hadden de medewerkers inmiddels kennelijk geleerd: zonder keiharde juristen valt er met de werkgever Defensie niet te praten.

Bij Defensie kan een fatsoenlijke behandeling alleen met zware druk en juridische middelen voor de poorten van de ministeriële hel worden weggesleept

Ik kan zo nog wel even doorgaan, en dat terwijl er inmiddels in Europa een oorlog woedt, die meer dan ooit duidelijk maakt dat een land dat in vrede wil leven zich helaas permanent moet voorbereiden op een oorlog. Iets wat wij in Nederland in de afgelopen dertig jaar schromelijk hebben nagelaten; zowel op materieel- als op personeelsgebied.

Munitievoorraden zijn goed voor drie dagen oorlog voeren en veel noodzakelijke uitrusting is uit de organisatie verdwenen of zó sporadisch ingedeeld dat je er niets meer mee kunt en daarbovenop is er al jaren een groot tekort aan personeel in alle geledingen, behalve hogere burgers in de Bestuursstaf natuurlijk. Als het zittende personeel de eigen werkgever niet meer vertrouwt, dan is het volstrekt uitgesloten dat nieuw personeel zich in voldoende mate zal laten verleiden om dienst te nemen. Daarom is het verstandiger en goedkoper om eerst maar eens te investeren in het herwinnen van het vertrouwen van het zittende personeel, alvorens te proberen het vertrouwen te winnen van nieuwe mensen die in veel gevallen na jarenlange kostbare opleiding en training weer veel te snel teleurgesteld de organisatie verlaten.

Mooie reclamecampagnes met gelikte filmpjes over generatie-D veranderen daar niets aan. De defensieleiding zal de komende jaren eerst meer moeten investeren in het herstel van het vertrouwen van het eigen personeel. En ja, vertrouwen komt te voet, dus dat is geen proces dat binnen een paar maanden succes zal hebben, alle gebruikelijke mooie praatjes van de defensietop over het 'altijd loyale goud van de organisatie' ten spijt. ■

1 Zie: Servé Mullenders, 'Wij gaan voor Onvoorwaardelijke indexatie', <https://www.gofundme.com/f/wij-gaan-voor-onvoorwaardelijke-indexatie>.

Train the trainer: leren van de Oekraïners

Sergei Boeke

De westerse inspanningen om Oekraïense militairen te trainen zijn enorm. Voor februari 2022 werden Oekraïense Special Forces getraind door onder meer de VS, het VK en Canada, en mede hierdoor hadden de Russische konvooien ten noorden van Kyiv een groot probleem. Afgelopen jaar werden enkele grote trainingsprogramma's voor tactische vaardigheden opgezet. Eerst organiseerde het VK een groot trainingsprogramma voor 30.000 Oekraïense militairen; nu leidt de Europese EUMAM-missie een vergelijkbaar aantal troepen op.

Nederland nam/neemt aan beide deel. Hiernaast bestaat er een uitgebreid scala aan gespecialiseerde opleidingen. Oekraïne heeft immers onoverzichtelijk veel verschillende wapensystemen gekregen van het Westen – alleen al een dozijn verschillende types 155mm-houwitser. Elk wapensysteem vereist een eigen opleiding, om nog te zwijgen over onderdelen en onderhoud. Voor al deze opleidingen zou eigenlijk het concept Train the trainer leidend moeten zijn. Dit betreft het creëren van een netwerk van toekomstige trainers, die allemaal zelf gaan opleiden. In de praktijk blijkt het lastig om toekomstige trainers op te leiden, want de nood is hoog en de meesten worden gelijk naar het front gestuurd. Toch heeft het concept hier ook een andere betekenis. Eigenlijk zouden Oekraïense troepen opleidingen moeten geven aan westerse militairen. Zij hebben immers als enigen – nu al bijna anderhalf jaar – ervaring in het voeren van een grootschalig gevecht tegen een zogeheten *peer adversary*.

Opleidingen en trainingsinfrastructuur – en het verwerken van lessons learned – spelen al sinds het begin van het conflict in Oekraïne een cruciale rol. Vanaf 2014 werd Oekraïne dagelijks gedwongen lessen te trekken uit het gevecht. In februari 2022 mobiliseerde Oekraïne onmiddellijk, Rusland niet. De Russen zetten al hun professionele eenheden volledig in; die werden gelijk vermangeld in de strijd. De Russische mobilisatie-infrastructuur bleek de jaren ervoor verwaarloosd te zijn, en het kader om op te leiden is nu beperkt. Zowel Oekraïne als Rusland ervoer de pijnlijke les dat de eerste weken van een conflict met hoge intensiteit veel moderne wapensystemen – en helaas ook de aanwezige troepen – zal opbranden. Vervolgens moet men terugvallen op wat er nog in de opslag staat. De Russische wapenopslagen waren vol, maar door corruptie en wanbeheer waren de wapens slecht onderhouden en vaak ontdaan van cruciale componenten. Westerse en Nederlandse opslagen lagen er beter bij. Zo konden de YPR's redelijk snel naar Oekraïne, al moest men waarschijnlijk wat handleidingen afstoffen en enkele deskundigen benaderen die allang met pensioen waren. De westerse opslagen zijn inmiddels helemaal leeg – alles is in Oekraïne. Wat betreft het menselijk kapitaal heeft

Nederland nog de dienstplicht. Die is opgeschort, en niet afgeschaft, en kan in principe in tijd van oorlog zo weer geactiveerd worden. Helaas zijn wel de hiervoor benodigde kazernes en opleidingscapaciteit verdwenen.

Terwijl westerse militairen Oekraïense soldaten hebben



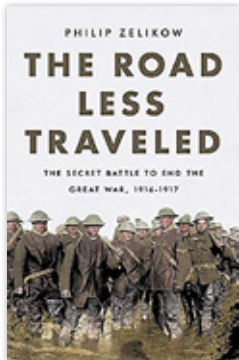
opgeleid, hebben de Oekraïners nu ruimschoots gevechtservaring. Hun lessons learned kunnen over de hele linie getrokken worden, van strategisch tot operationeel en tactisch niveau. Ook hebben ze ervaring hoe joint en combined optreden in de praktijk uitpakt. De Oekraïense krijgsmacht heeft zich volledig moeten aanpassen aan de harde realiteit. Dit is altijd een pijnlijk proces, maar in nood gaan innovatie en aanpassingsvermogen in een stroomversnelling. Bij de NAVO-landen bestaat geen vergelijkbare druk om de krijgsmacht te hervormen, en militairen (en organisaties in het algemeen) hebben een natuurlijke weerstand tegen al te rigoureuze veranderingen. Er is dus een groot risico dat het Westen uit het conflict in Oekraïne wat versnipperde conclusies trekt en geen geïntegreerde analyse maakt om deze vervolgens rigoureuze te implementeren. Drones zijn daar een voorbeeld van. Britse onderzoekers van het gerenommeerde Royal United Services Institute (RUSI) schatten in dat Oekraïne zo'n 10.000 drones per maand verliest. Dit getal is natuurlijk omstreden, en het is nogal wies dat NAVO-krijgsmachten meer moeten investeren in drones. De kernvraag is hoe deze capaciteit in te bedden in bestaande structuren. Of moeten bestaande structuren wellicht juist worden omgegooid om (goedkope en vervangbare) drones op pelotonsniveau te integreren? Uiteindelijk gaat het niet om de drones zelf, maar hoe een bepaald effect kan worden bereikt op het slagveld.

Elk domein, elk niveau en elke militaire specialiteit zal fundamentele lessen moeten trekken uit het conflict in Oekraïne. Vervolgens zullen deze allemaal moeten worden geïntegreerd, idealiter binnen de nieuwe doctrine van Multi Domain Operations. Sommige conclusies zullen op organisatorische weerstand stuiten en misschien moeten bestaande structuren, modellen en eenheden op de schop. Andere conclusies zullen politiek ongemakkelijk zijn. Als Oekraïense militairen overtuigd zijn dat de tank onontbeerlijk is voor het landgevecht, dan loont het om goed te luisteren. De lessons learned zullen ongetwijfeld grote gevolgen hebben voor de Nederlandse krijgsmacht. Misschien moeten binnen en tussen krijgs-

Als Oekraïense militairen overtuigd zijn dat de tank onontbeerlijk is voor het landgevecht, dan loont het om goed te luisteren

machtdelen andere prioriteiten worden gesteld, met grote financiële gevolgen. Het is goed dat er een *Defensievisie 2035* ligt, maar deze stamt wel uit oktober 2020, toen de wereld er anders uitzag.

Het lijkt eenvoudig om lessen te trekken uit het conflict in Oekraïne, maar dat is het niet. Om de krijgsmacht te kunnen aanpassen zullen eerst alle assumpties tegen het licht moeten worden houden die ten grondslag liggen aan een groot-schalig conventioneel gevecht. Het betekent vooral niet: we bestellen er een flink aantal drones en HIMARS bij, en klaar is Kees. Lessen trekken kan alleen met hulp van Oekraïense militairen. Hun krijgsmacht heeft zich immers razendsnel aangepast en staande gehouden. Ook de Russen trekken hun lessen, al lijkt dit proces aanzienlijk pijnlijker te verlopen. Zo zal de dreiging tegen de NAVO zich eveneens verder ontwikkelen en aanpassen. Oekraïne zal voorlopig nog een grote behoefte aan westerse militaire opleidingscapaciteit hebben, maar het is belangrijk om te beseffen dat wij op veel vlakken inmiddels meer van de Oekraïense krijgsmacht kunnen leren dan zij van ons. Momenteel hebben zij andere zorgen aan hun hoofd dan ons bijspijkeren in de kunst van het oorlogvoeren. Toch dienen Den Haag en de Operationele Commando's nu de voorbereidingen te treffen om geïntegreerde lessons learned van de frontlinies te vergaren. Implementatie van deze lessen zal de volgende stap zijn. Hier hoort een open houding bij, samen met de bereidheid om eigen stokpaardjes te offeren. Het motto *train as you fight* blijft leidend, en het zijn de Oekraïense militairen die momenteel dapper vechten. Ongeacht het resultaat op het slagveld mogen we hopen dat zij straks ook ons uitgebreid willen trainen. ■



The Road Less Traveled

The Secret Battle to End the Great War, 1916-1917

Door Philip Zelikow

New York (PublicAffairs) 2021

334 blz.

ISBN 9781541750951

€ 32,-

Een van de meest indrukwekkende liedjes over de Eerste Wereldoorlog is zonder twijfel 'The Green Fields of France'. Daarin wordt het lot bezongen van een jonge soldaat, Willy McBride. En dan die eerste zinnen: 'I can see by your gravestone that you were only nineteen, when you joined the great fallen in 1916. I hope you died well and I hope you died clean, or young Willy McBride, was it slow and obscene?' Hoeveel van die jonge mannen aan beide kanten zouden niet gesneuveld zijn als er al in 1916-1917 vrede was gesloten? Becijferen is moeilijk, maar het moet om miljoenen gaan, een hele generatie die in het trommelvuur van de Eerste Wereldoorlog om het leven kwam.

Over de 'Mutterkatastrophe' van de twintigste eeuw is onnoemelijk veel geschreven. Veel aandacht gaat daarbij uit naar de oorzaken van het conflict, de grote veldslagen, waarom de generaals zo lang vast bleven houden aan het offensief, en bovenal naar de schuldvraag: wie was er verantwoordelijk voor het uitbreken van de oorlog? Veel minder is er gepubliceerd over pogingen om het conflict eerder te beëindigen. En dat is niet terecht, stelt Philip Zelikow in zijn fascine-

rende *The Road Less Traveled. The Secret Battle to End the Great War, 1916-1917*. Waarom, zo vraagt hij zich af, mislukte 'the secret German peace move of 1916' (blz. 13), terwijl de Duitse ambassadeur in de Verenigde Staten in november 1916 verklaarde dat 'peace is on the floor waiting to be picked up!' (blz. 15)?

Complexe besluitvorming

Zelikow biedt een mooie schets van de enorme complexiteit van de besluitvorming, diplomatieke initiatieven en de brede waaier aan betrokkenen aan beide kanten. De auteur stelt dat de strijdende partijen tussen augustus 1916 en eind januari 1917 worstelden om een eind te maken aan de oorlog. In veel opzichten, zegt Zelikow, is de vraag waarom er *niet* gekozen werd om de oorlog te beëindigen veel interessanter dan de kwestie waarom de oorlog begon. Daar is wel het een en ander voor te zeggen, al blijft het – de auteur gaat er wat makkelijk aan voorbij – vooral speculeren hoe de geschiedenis eruit had gezien als de oorlog inderdaad eind 1916, begin 1917 gestopt was. Hij maakt wél duidelijk dat de Duitse regering in het geheim vrede zocht en bij de Amerikaanse president Woodrow Wilson aandrang op een vredes-

conferentie. Bovendien, zo stelt hij, moet dit initiatief serieus worden genomen: het was geen proefballonnetje, maar gecoördineerd met de geallieerden en politieke sleutelfiguren in Duitsland. Wilson nam het voorstel serieus, en dat gold ook voor de Britten en Fransen. En toch resulteerde het niet in vrede. Volgens Zelikow begreep Wilson nooit helemaal wat er mis was gegaan. Niettemin kwam er een einde aan 'America's historic neutrality and America embarked on a new course in world history' (blz. 10).

Volgens Zelikow waren de maanden tussen augustus 1916 en januari 1917 een 'window of opportunity', omdat alle partijen belang hadden bij een einde aan de vijandelijkheden. De Franse en Britse offensieven van dat jaar waren op niets uitgelopen en hadden miljoenen slachtoffers geëist, hetzelfde gold voor de Slag bij Verdun. Het Duitse keizerrijk en diens bondgenoot Oostenrijk-Hongarije zuchtten steeds meer onder de Britse blokkade en de eruit voortkomende tekorten aan grondstoffen en voedsel. Groot-Brittannië was er nauwelijks beter aan toe, en balanceerde op de rand van de financiële afgrond, al waren de Duitsers zich daar niet van bewust.

Zelikow maakt knap inzichtelijk dat er bij alle strijdende partijen – maar ook in het nog neutrale Amerika – sterk tegenover elkaar staande kampen en facties bestonden. In Groot-Brittannië was Herbert Henry Asquith jarenlang de premier geweest, en wel geneigd naar vredesonderhandelingen. Zijn collega en rivaal, David Lloyd George, was daarentegen voorstander van wat Zelikow noemt 'the all-out war effort' (blz. 42).

Aan Duitse zijde was de situatie minstens even complex, al was het maar omdat het parlement niks te zeggen had over defensie en buitenlandse zaken. Aan de andere kant van de Atlantische Oceaan stelde Wilson inderdaad een vredesconferentie voor, maar van Britse en Franse zijde kwam er weinig reactie: 'He [Wilson, M.L.] simmered with frustration. As the slaughter continued every day, he and House [Wilsons adviseur, M.L.] complained to each other about the foolish stubbornness on all sides, especially the British and French' (blz. 79). Dat was opmerkelijk, in de woorden van Zelikow: 'By August 1916, the warring countries were reaching their limits: limits to mass tolerance of the agony; limits in the number of men available to man front lines, factories, and farms; limits of money; and limits of food and other resources' (blz. 82).

De rol van Bethmann Hollweg en Wilson

Toch kwam er geen vrede en zouden nog miljoenen sterven en gewond raken. Wat ging er mis? Volgens Zelikow waren alle partijen ervan overtuigd dat alleen de Verenigde Staten in de positie waren een vredesinitiatief te ontwikkelen. Op 2 september 1916 stuurde de Duitse kanselier Bethmann Hollweg bijvoorbeeld een telegram aan zijn ambassadeur in Washington, waarin beknopt werd weergegeven hoe de Duitse leiding de oorlogssituatie inschatte: 'Hope to conclude peace before winter [...] would peace mediation by Wilson be possible and successful if we were to guarantee Belgium's conditional restoration?' (blz. 97). Zelikow kraakt een aantal

harde noten, bijvoorbeeld over Wilsons adviseur Edward House, die zich fel tegen vrede keerde. Wilson wilde vooral een praktische en simpele vredesconferentie, maar hij stelde er geen voorwaarden aan: 'Nor did it [de draft voor een vredesconferentie, M.L.] discuss the possibility of a cease-fire or the terms for an armistice' (blz. 169). In Duitsland had Bethmann Hollweg – deels verantwoordelijk voor het uitbreken van de Eerste Wereldoorlog – maanden gevochten om de weg naar vrede open te houden, maar de militaire leiding en conservatieven vonden dat hij zijn kans had gehad: 'Public opinion and political opinion in the Reichstag wanted to let the U-boats loose, to starve the enemy as Germans were being starved' (blz. 233). Zelikow wijst er terecht op dat het Duitse opperbevel twee fatale inschattingfouten maakte. Ten eerste de aanname dat de Britten (met Amerikaanse hulp) geen tegenmaatregelen zouden kunnen vinden tegen de U-Boote. De tweede aanname was catastrofaal: 'the underestimation of the United States' (blz. 252).

Hoe het ook zij, volgens Zelikow was de mislukking om de Eerste Wereldoorlog te beëindigen in 1916-1917 veel meer dan een menselijke tragedie van de miljoenen gesnevelde soldaten; het was een keerpunt in de geschiedenis. Zelikow stelt, in navolging van de Duitse historicus Robert Gerwarth, dat het geweld na 1917-1918 veel minder beheersbaar was: het werden existentiële conflicten om de vijand te vernietigen. Voeg daaraan toe het uitbreken van de Russische Revolutie

en de erop volgende burgeroorlog, de revoluties in Duitsland en de opkomst van het fascisme, en de tragedie van het niet bereiken van vrede wordt steeds groter. Zelikow wijt dat voor een groot deel aan Wilson: 'In the failure to make peace at the most opportune moment, no one failed, and failed the world, more than President Wilson. His was the most consequential diplomatic failure in the history of the United States' (blz. 271). Dat lijkt mij wat al te sterk – de Britten waren bepaald niet happig op vredesvoorstellen en dat gold ook voor een groot deel van de Duitse leiding – al is Zelikows beschrijving van Wilson als 'the rookie who sits down at the poker game and, dealt a hand with three kings, throws back two of them in the hope of getting better cards' (blz. 272) wel raak.

Zelikow gebruikt veel interessant archiefmateriaal en zijn vloeiende schrijfstijl maakt dit boek haast tot een *pageturner*. Hoewel niet overal overtuigend, is *The Road Less Traveled* een aanrader voor hen die geïnteresseerd zijn in diplomatieke geschiedenis en de Eerste Wereldoorlog. Zelikow verliest daarbij het menselijke drama gelukkig niet uit het oog. Of, zoals bezongen in 'The Green Fields of France': 'But here in this graveyard it's still no man's land, the countless white crosses stand mute in the sand. To man's blind indifference to his fellow man, to a whole generation that were butchered and damned'. ■

*Dr. Martijn Lak, Universiteit Utrecht/
Universiteit van Amsterdam*

‘Zekerheidsneurose mag niet leiden tot pietepenterige controle op alle details’

De *Militaire Spectator* publiceerde in 1984 de serie artikelen ‘Leiderschap op de korrel’. Twee docenten aan de Koninklijke Militaire Academie reflecteerden ter afsluiting op de rol van de ‘militaire manager’. ‘Voor hen die gewoon zijn de zaken door een militaire bril te zien, verdient het ongetwijfeld aanbeveling te lezen hoe dat zelfde eruitziet door eens anders bril’, schreef de redactie van het tijdschrift ter begeleiding.¹

In de serie kwamen eerder diverse functies aan bod om een beeld te schetsen van de verschil-

lende leiders in de militaire organisatie. De bataljonscommandant gold bijvoorbeeld als schakel tussen planning en uitvoering, en was om die reden een gewilde positie. In het geval van de compagniescommandant, vergeleken met het bedrijfsleven, ‘kunnen wij stellen dat het zoeken naar vergelijkbare aspecten op een overeenkomstig managementniveau op zo goed als alle punten mank gaat.’ Een jonge officier gaat namelijk eerst aan het werk als ‘chef’ en pas daarna als stafmedewerker, terwijl het carrièrepad voor een pas afgestudeerde in de civiele sector precies andersom verloopt.



FOTO: BEELDBANK NIMH

De KMA-docenten keken, als burger, door een andere bril naar de militaire manager. Alles moest in dienst staan van de primaire taak van de strijdkrachten: ‘productie van gevechtskracht [is] de centrale missie van de krijgsmacht. Om dat te bereiken moet het vrijwillig en onvrijwillig dienende personeel voortdurend de kans krijgen zich daarin te bekwamen.’ Dat leverde veertig jaar geleden analyses op die we nu nog steeds tegenkomen: ‘Toenemende technologische veranderingen, ingewikkelder wordende organisaties, onvoorspelbaarder optreden van de vijand, dat alles stelt hoge eisen aan het aanpassingsvermogen van de organisatie en haar medewerkers.’ Het antwoord hierop was volgens de docenten het creëren van een ‘zelflerende organisatie’.

De auteurs gaven aanbevelingen die tegenwoordig ook bekend in de oren klinken: ‘De zekerheidsneurose binnen de organisatie mag niet leiden tot pietepenterige controle op alle details.’ En: ‘Beloon durf en het nemen van berekenbare risico’s. Uitgesleten paden zijn er al genoeg.’ ■

Schietoefening met tanks. Productie van gevechtskracht is de centrale missie van de krijgsmacht. Militaire managers moeten een zelflerende organisatie creëren voor zoveel mogelijk effectiviteit

¹ J. Heijnsdijk en C.W. Vroom, ‘De militaire manager, door andermans bril gezien’, *Militaire Spectator* 153 (1984) (9) 392-395.

SIGNALERINGEN



Diensten met geheimen

Hoe de AIVD en MIVD Nederland veilig houden
Door Willemijn Aerdts
Amsterdam (Ambo|Anthos) 2023
256 blz.
ISBN 9789026354120
€ 22,99

In *Diensten met geheimen* concludeert Willemijn Aerdts dat spionageromans en series als *Homeland* en *The Americans* ver af staan van de werkelijkheid van de Nederlandse inlichtingen- en veiligheidsdiensten. Ze licht toe hoe de AIVD en MIVD zijn ontstaan en op welke manier de taken en werkwijzen sinds de Tweede Wereldoorlog zijn veranderd. Beide diensten hebben als doel de democratische rechtsstaat te waarborgen en geheimhouding kan daarbij van levensbelang zijn; tegelijkertijd heeft iedere burger recht op privacy en is toezicht noodzakelijk. Aerdts, verbonden aan het Institute of Security and Global Affairs van de Universiteit Leiden, beschrijft ook de dilemma's waarvoor de diensten zich gesteld zien.



The Crucible of War

Dutch and British military learning processes in and beyond southern Afghanistan
Door Martijn van der Vorm
Leiden/Breda (proefschrift Universiteit Leiden/NLDA) 2023
476 blz.
ISBN 9789493124202

Voor *The Crucible of War*, waarop hij onlangs promoveerde aan de Universiteit Leiden, onderzocht majoor Martijn van der Vorm de leerprocessen van de Nederlandse en Britse krijgsmachten tijdens hun inzet in Zuid-Afghanistan. Wat waren precies de lessons learned en lukte het om ze in de organisaties, die niet op counterinsurgency-operaties waren ingericht, te borgen? Zijn theoretisch kader over counterinsurgency en organizational learning in krijgsmachten laat Van der Vorm volgen door analyses van de Nederlandse inzet in Uruzgan en Britse operaties in Helmand. Financiële beperkingen en herijking naar conventionele oorlogvoering leidden er volgens de auteur toe dat cruciale lessen uit deze campagnes verloren gingen.



De oorlog en de toekomst

Door Rob Riemen (red.)
Nexus No. 92
Amsterdam (Nexus Instituut) 2023
168 blz.
€ 25,-

De oorlog en de toekomst is de neerslag van de conferentie *The War and the Future* die afgelopen november plaatsvond bij het Nexus Instituut. De discussie ging over de vraag waarom de geschiedenis gelittekend is door oorlogen en hoe het beschavingsideaal met zijn morele waarden, liberale traditie en het humanisme als leerschool hersteld kan worden. De bundel bevat bijdragen van onder meer defensie-expert Nicolas Baverez, voormalig Amerikaans onderminister van Defensie Mary Beth Long en Kishore Mahbubani van de Universiteit van Singapore, die de stelling poneert dat 'de eeuw van Azië' onvermijdelijk is en dat het continent zich in tegenstelling tot Europa voor de vrede heeft geprogrammeerd.



Heerschappij ter zee

Over de rol van theorie in de zee krijgskunde
Door Henk Warnar
Breda (occasional paper Nederlandse Defensie Academie) 2023
111 blz.
ISBN 9789493124332
Downloadbaar via:
www.faculteitmiltairewetenschappen.nl

KTZ Henk Warnar doet onderzoek naar het Nederlandse navalisme, ofwel de ontwikkeling van het marinedenken tussen 1892-1940 en schetst in zijn occasional paper *Heerschappij ter zee* zijn eerste bevindingen. Volgens Warnar heerst in de Nederlandse historiografie ten onrechte het beeld dat het marinedenken in de aanloop naar de Slag in de Javazee een theoretisch onjuiste strategie zou hebben opgeleverd. Hij analyseert welke rol theorie destijds speelde in de zee krijgskunde en komt tot de conclusie dat concepten als de Heerschappij ter Zee achteraf verkeerd begrepen zijn. Over het zeeoptreden voor de verdediging van Nederland en Nederlands-Indië vond een waardevol professioneel debat plaats onder marineofficieren.

