

MILITAIRE SPECTATOR

WARFIGHTING CAPABILITIES EN DIGITALISERING



- Space weather impacts in the Arctic
- Meaningful human control onder vuur
- Een schaalbare krijgsmacht in tijden van vergrijzing
- Waarom Rusland ontregelt, en wat dit van ons vraagt

FOTO MCD, JASPER VEROLME



In *Militaire Spectator* 11-2026 verschijnt onder meer: 'Strategische autonomie van de Europese defensie-industrie. Van ambitie naar realiteit' van prof. dr. Jeroen Klomp.

De Russische invasie van Oekraïne in februari 2022 vormde een geopolitieke schok die de structurele kwetsbaarheden van de Europese defensiearchitectuur scherp blootlegde. Europese strijdkrachten beschikten over beperkte strategische voorraden, sterk gefragmenteerde productiecapaciteiten en een diepe afhankelijkheid van externe leveranciers. Pogingen om Oekraïne snel en substantieel te ondersteunen leidden binnen enkele maanden tot het uitputten van Europese munitievoorraden, terwijl de defensie-industrie onvoldoende in staat bleek om de productie op korte termijn op te schalen. Deze capaciteitskloof weerspiegelde niet slechts tijdelijke tekortkomingen, maar wees op decennia van onderinvestering, inefficiënte marktstructuren en een gebrek aan strategische industriële coördinatie.

In plaats van volledige onafhankelijkheid kan Europa echter beter kiezen voor *managed autonomy* als analytisch en beleidsmatig realistischer alternatief: het nastreven van selectieve autonomie in strikt gedefinieerde strategische domeinen, terwijl trans-Atlantische samenwerking behouden blijft waar deze operationeel en economisch rationeel is. Dit impliceert een expliciete prioritering van capaciteiten waarin autonomie cruciaal is voor strategische handelingsvrijheid, zoals command-and-controlsystemen, cryptografie en cybercapaciteiten, kritieke software en datalagen, ITAR-vrije subsystemen en voldoende *surge capacity* in munitie- en onderdelenproductie. Voor andere capaciteiten – met name waar schaalvoordelen dominant zijn – kan internationale samenwerking efficiënter blijven, mits afhankelijkheden worden begrensd door *multiple sourcing* en interoperabele standaarden. ■

AANKONDIGING KVBK

De battlefieldtour van de KVBK naar onder meer Nijmegen en het Reichswald is uitgesteld. Op 21 november wordt het programma in en rond Nijmegen uitgevoerd. Het tweede deel van de battlefieldtour wordt opnieuw vormgegeven en zal in de tweede helft van 2027 plaatsvinden.

Scan de qr-code voor meer informatie over de najaarsactiviteiten van de KVBK.



Samen voorwaarts! Ja, maar hoe dan?

De defensienota 2026 is de derde nota in vier jaar. Het schijnt dat het regel is dat elk kabinet nu zijn eigen defensienota uitbrengt en dat we het moeten doen met korte nota's met daarin algemeen geformuleerde beleidsvoornemens van de regering. De trend van deze defensienota's nieuwe stijl begon in 2013 met de nota *In het belang van Nederland*, waarbij de defensienota niet meer het uitgebreide planningsdocument was waarin het vraagstuk van legervorming en inrichting van de krijgsmacht werd beantwoord. De laatste defensienota waarin dat wel stond dateert uit 2000.

De defensienota 2026 *Samen voorwaarts!* wijst er terecht op dat Defensie niet alleen de weerbaarheid van het land bepaalt, maar dat we dat samen met de samenleving moeten doen.¹ Maar als je samenwerkt met de weerbare samenleving dan moet je die samenleving ook laten weten wat je gaat doen en moet zij de kans krijgen daarover mee te praten, met andere woorden er is behoefte aan een maatschappelijk debat over de precieze rol en taak van de krijgsmacht. Op dat punt schiet deze defensienota net als de twee eerdere nota's uit 2022 en 2024 tekort. De strategische doelen uit de defensienota 2026 zijn helder en kunnen rekenen op breed maatschappelijk draagvlak. Maar ook deze nota laat na die doelen te vertalen in concrete acties en capaciteiten. Net als in 2024 zijn de doelstellingen niet vertaald naar SMART-subdoelen² en dat maakt het maatschappelijk debat erover lastig, zo niet onmogelijk.

De huidige nota kiest voor 'een pakket aan maatregelen dat het meest bijdraagt aan het militair vermogen dat Nederland nodig heeft om de vier strategische doelstellingen te realiseren', maar laat na te zeggen waaruit dat pakket aan maatregelen precies bestaat en welke keuzes daarbij zijn gemaakt. De nota komt niet verder dan een negental leidende principes die sterk doen denken aan een update van de tien inrichtingsprincipes uit de *Defensievisie 2035* en waar niemand op tegen kan zijn. Zomaar twee voorbeelden: 'De krijgsmacht moet wendbaar zijn en inspelen op nieuwe dreigingen': ja, maar hoe dan? 'Defensie investeert in digitale en innovatieve kracht van de krijgsmacht': ja, maar hoe dan? Elk van die principes roept zo de vraag op: ja, maar hoe dan? De antwoorden staan hopelijk in de vertrouwelijke bijlage, maar in elk geval niet in de defensienota zelf die daarover zegt dat 'de gemaakte keuzes vertrouwelijke informatie betreffen en daarom niet openbaar en in detail kunnen worden toegelicht'.

Het vraagstuk van legervorming en het inrichten van de krijgsmacht is zeer complex. Vroegere defensienota's (tot en met 2000) gingen daar uitgebreid op in. Nu laten wij de oplossing van het vraagstuk met de defensienota's nieuwe stijl volledig bij de experts van Defensie. Wij hebben er alle vertrouwen in dat daar iets goeds uitkomt, maar het is jammer dat de samenleving de mogelijkheid ontzegd wordt zich een goed oordeel te vormen over de toekomstige krijgsmacht. Gaan we hier dan niet samen voorwaarts? ■

1 *Defensienota 2026. Samen voorwaarts!* (Den Haag, ministerie van Defensie, 29 juni 2026).

2 'De devaluatie van de defensienota', editoriaal, *Militaire Spectator* 193 (2024) (11) 617.

UITGAVE

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

Secretaris en ledenadministratie

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

REDACTIE

Igen b.d. ir. R.G. Tieskens (hoofdredacteur)
Itkol mr. E.C. Bahler
briggen Marns drs. G.F. Booij EMSD
kol dr. L. Boskeljon-Horst
bgen prof. dr. A.J.H. Bouwmeester
kap dr. B.T.A. van den Broek
drs. K.S. Chafekar MA
dr. A. Claver
drs. P. Donker
cdre KLu b.d. F. Groen (plv. hoofdredacteur)
lkol A.L. Judge-Heijboer MSc
kltz dr. W.M. Ooms
lkol P. Schrijver MA
mr. dr. A. van Vark
dr. R. de Winter

BUREAU REDACTIE

M. Katsman MA (e-outreach)
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

Particulier lid € 30,-
Particulier lid buitenland € 30,-
+ € 15,- verzendkosten

Instellingen binnenland € 35,-
Instellingen buitenland € 35,-
+ € 15,- verzendkosten

Evenementenlid € 10,-

OPMAAK

Coco Bookmedia

DRUK

Wilco Amersfoort
ISSN 0026-3869
Nadruk verboden

Cover: Drones vormen een belangrijk
onderdeel van het versterken van
warfighting capabilities door digitalisering
Foto: MCD



FOTO MCD

Een schaalbare krijgsmacht in tijden van vergrijzing

Raymond Gradus

Het is beter om in te zetten op Europese samenwerking dan vast te houden
aan de voorgenomen versnelling naar een schaalbare krijgsmacht.

Waarom Rusland ontregelt, en wat dit van ons vraagt

Jan-Willem Maas

Als antwoord op de Russische ontregeling zijn negen verschuivingen nodig
voor het inrichten en laten optreden van militaire formaties.

536



Meaningful human control
onder vuur

Job Timmermans en Stas Kloos

Ondanks theoretische en beleidsmatige aandacht blijft praktische reflectie op Meaningful Human Control bij de operationale toepassing van AI achter.

Het versterken van
warfighting capabilities
door digitalisering

Peter van den Berg e.a.

Een analyse van recente conflicten laat zien hoe de krijgsmacht in een gewapend conflict doeltreffender kan optreden door de inzet van IT.

EDITORIAAL	Samen voorwaarts! Ja, maar hoe dan?	505
MICHAELA BRCHNELOVÁ AND ARIE VERHEIJ	Space weather impacts in the Arctic	548
GASTCOLUMN EDWIN ZONDERVAN	Waarom de krijgsmacht baat heeft bij chemische technologie	560
TEGENWICHT	De wapenwedloop achter het beeldscherm	562
COLUMN PIEN VAN DER HOEVEN	Zwerfvuul en pacifisme	564
BOEKEN	The Weapons of Word War III	566
RETROSPECTATOR	‘Goed georganiseerde weerdienst is een dringende eisch’	568

EN
VERDER

Een schaalbare krijgsmacht in tijden van vergrijzing

Raymond Gradus*

Volgens het coalitieakkoord zou er in 2030 een schaalbare krijgsmacht van minimaal 122.000 mensen moeten zijn. Als deze opschaling onvoldoende resultaat oplevert, wordt een selectieve opkomstplicht overwogen. Het ministerie van Defensie gaat uit van 102.000, zo blijkt uit de *Defensienota*. In tijden van schaarste en vergrijzing is dit al een enorme opgave. Ook de rekrutering in de rest van West-Europa en de VS geeft aan dat dit heel veel vraagt van de defensieorganisatie en van jongeren. Het is beter om in te zetten op een Europees leger of een vergaande samenwerking van de strijdkrachten in een kopgroep van Europese landen dan vast te houden aan deze ambitie.

In het coalitieakkoord 2026-2030, *Aan de slag: Bouwen aan een beter Nederland*, is de afspraak gemaakt dat het nieuwe kabinet in 2030 een schaalbare krijgsmacht van minimaal 122.000 mensen paraat heeft. Men wil daartoe het dienstjaar fors opschalen en als eerste stap een 'verplichte enquête' voor jongeren introduceren. Als de opschaling van de krijgsmacht onvoldoende vordert, worden 'andere stappen, waaronder de invoering van een selectieve opkomstplicht overwogen'.¹ Ook in het tussenverslag van D66-voorman Jetten en CDA-leider Bontenbal is dit punt onder *Bouwen aan de krijgsmacht van de 21^e eeuw* opgenomen.²

Dit is om twee redenen opvallend. Op de eerste plaats omdat het vorige kabinet in maart 2025 in

een brief aan de Tweede Kamer nog had aangegeven te streven naar een schaalbare krijgsmacht van 100.000 in 2030.³ In de *Defensienota 2026* is opgenomen dat 'Defensie bouwt aan een krijgsmacht van vooralsnog circa 102.000 mensen in 2030'.⁴ Een doelstelling in 2030 van net iets meer dan honderdduizend is al een stevige ambitie en het ministerie van Defensie zal alles op alles moeten stellen om dit te realiseren. Op de tweede plaats is de koppeling van deze (te) ambitieuze doelstelling met de opkomstplicht frappant. Terwijl Defensie inzet op vrijwillige deelname en realistisch plant wat dit betekent voor instructeurs en kazernes,⁵ gaat het coalitieakkoord daar wel al te gemakkelijk aan voorbij. Bovendien lijkt een (selectieve) opkomstplicht als een soort zwaard van Damocles weinig doordacht. In een Kamerbrief wordt juist aangegeven dat het instellen van een generieke opkomstplicht niet 'effectief' is.⁶ Het legt een enorm beslag op de capaciteit en de fysieke ruimte en het is de vraag of jongeren voldoende gemotiveerd zijn, terwijl men juist met een *vrijwillig* dienstjaar de motivatie en instroom wil vergroten.

Dit artikel schetst allereerst de personeelsontwikkeling bij Defensie in 2024 en 2025 en de raming voor 2026, om vervolgens een extrapolatie naar 2030 te doen. Hieruit blijkt dat het

* Prof. dr. Raymond Gradus is hoogleraar Bestuur en Economie van de Publieke en Non-profit Sector aan de Vrije Universiteit Amsterdam. De auteur dankt André Mol, Ana de Koning en de redactie voor commentaar bij een eerdere versie.

1 Bureau Woordvoering Kabinetsformatie, *Aan de slag, Bouwen aan een beter Nederland* (2025), Coalitieakkoord. Zie: <https://www.kabinetsformatie2025.nl/documenten/2026/01/30/aan-de-slag---coalitieakkoord-2026-2030>.

2 Bureau Woordvoering Kabinetsformatie, *Inhoudelijke en ambitieuze agenda van de fracties D66 en CDA* (2025), Tussenverslag informateur Buma, 13. Zie: <https://www.kabinetsformatie2025.nl/documenten/2025/12/02/tussenverslag>.

3 Ministerie van Defensie, *Onze mensen, onze toekomst; meer, beter en sneller*, Brief aan de Tweede Kamer, 24 maart 2025.

4 Ministerie van Defensie, *Defensienota 2026: Samen Voorwaarts!*, 58.

5 Ministerie van Defensie, *Onze mensen, onze toekomst*.

6 Ididem, 3.

Nederland zet in op een
schaalbare krijgsmacht,
onder andere door het aantal
reservisten te vergroten.
Is dit realistisch?



Defensie zal alles op alles moeten zetten om de doelstelling van iets meer dan honderdduizend mensen in 2030 te realiseren

nog een hele opgave zal zijn om dan 102.000 personeelsleden te hebben (inclusief een groter deel reservisten). Vervolgens wordt het aantal militairen gerelateerd aan het fit-voor-service deel van de beroepsbevolking, niet alleen voor Nederland maar ook voor andere Europese NAVO-landen. Daaruit blijkt dat Nederland niet onderdoet voor andere NAVO-landen, zeker als het aanzienlijke deel burgerpersoneel wordt meegenomen. Veel landen zetten in op de uitbreiding van krijgsmacht maar worden in toenemende mate geconfronteerd met een rekruteringsprobleem. Tot slot worden mede op basis daarvan enige conclusies getrokken en een slotopmerking gemaakt.

De ontwikkeling van de krijgsmacht en een extrapolatie naar 2030

Bij Defensie werken 79.323 beroepsmilitairen, burgers en reservisten (stand per 1 september 2025). Dit kan worden uitgesplitst naar 44.245 beroepsmilitairen, 8.510 reservisten en 26.568 burgerpersoneel (zie Tabel 1). Dit is ruim 5.000

meer dan in 2024. Vooral het aantal reservisten stijgt fors, met 13,7 procent. Deze cijfers sluiten aan bij de ambitie van Defensie om een schaalbare krijgsmacht te realiseren met meer reservisten. Bij beroepsmilitairen was de stijging 4,6 procent en bij burgerpersoneel 9,7 procent. Voor 2026 zijn volgens de Begrotingsstaat de volgende doelstellingen vastgesteld: 47.176 beroepsmilitairen, 26.065 burgers en 10.212 reservisten.⁷ Dit betekent een geraamde versnelling bij beroepsmilitairen tot 6,7 procent en bij reservisten tot 20 procent. Bij burgerpersoneel wordt in tegenstelling tot 2025 dit jaar een lichte daling verwacht.

In Tabel 1 zijn twee extrapolaties naar 2030 opgenomen. In de eerste wordt de gerealiseerde groei voor reservisten en beroepsmilitairen tussen 2024 en 2025 doorgetrokken naar 2030. Hierbij is aangenomen dat de hoeveelheid burgers de komende jaren een constante omvang van 26.000 heeft. Volgens deze berekening (afgerond op tientallen) heeft Defensie in 2030 91.950 werknemers. De tweede extrapolatie trekt de versnelling van 6,7 procent voor beroepsmilitairen en 20 procent voor reservisten door, zoals die wordt beoogd in 2026: dan bedraagt het aantal werknemers bij Defensie in 2030 98.470, net iets minder dan het streefgetal van 102.000.

In *Stand van Defensie: Bouwen aan een sterke en slimme krijgsmacht*, waarin de instroom van beroepsmilitairen in de eerste vijf maanden van 2025 in kaart is gebracht, wordt reeds aangegeven dat 'Hoewel de instroom toeneemt, leidt dit naar verwachting niet tot het behalen van de beoogde doelstelling voor geheel 2025'.⁸ De uitbreiding naar 102.000 vraagt veel van de defensieorganisatie, met name voor reservisten, die moeten worden opgeleid en getraind op een reguliere basis. Iedere defensiemedewerker moet beschikken over goede huisvesting en werkplek, de juiste uitrusting en voldoende oefenmogelijkheden en -ruimte. Opschaling naar 102.000 is dus al een enorme opgave.

Een opschaling naar een personeelsbestand van 'minimaal' 122.000 lijkt mij niet haalbaar. Behalve een nog grotere versnelling bij reser-

7 Ministerie van Defensie, *Beantwoording Feitelijke vragen aangaande Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) en Vaststelling van de begrotingsstaat van het Defensiematerieelbegrotingsfonds voor het jaar 2026*, Brief aan de Tweede Kamer, 12 november 2025.

8 Ministerie van Defensie, *Stand van Defensie: Bouwen aan een sterke en slimme krijgsmacht*, Openbare versie Najaar 2025, 17.

Soort	2024	2025	2026	2030 extrapolatie 1	2030 extrapolatie 2
Beroepsmilitairen	42.305	44.245	47.176	52.530	55.990
Burgers	24.212	26.568	26.065	26.000	26.000
Reservisten	7.483	8.510	10.212	13.420	16.480
Totaal	74.000	79.323	83.453	91.950	98.470

Tabel 1 Krijgsmacht in 2024, 2025 en 2026 en extrapolatie naar 2030. Bron: www.defensie.nl

visten betekent dit dat veel meer militairen en burgerpersoneel in dienst moeten komen. De *Defensienota* geeft aan dat ‘Defensie (na 2030) zal moeten doorgroeien naar 122.000 mensen om aan onze huidige (inter)nationale taken te voldoen’.⁹ Het beslag op de arbeidsmarkt daarvan is aanzienlijk, terwijl deze juist in het volgende decennium verder verkraapt.¹⁰ Het coalitieakkoord somt een groot aantal prioriteiten op, die om extra menskracht (vooral vakmensen) vragen. Hetzelfde coalitieakkoord geeft tevens aan dat ‘we nu al niet genoeg vakmensen hebben die onze huizen kunnen bouwen, zonnepanelen aanleggen en zorg verlenen’.¹¹ Ook in dit licht lijkt de voorgenomen versnelling bij de krijgsmacht weinig doordacht en gaat die wringen met de andere prioriteiten.

Internationale vergelijking defensiepersoneel

Er bestaan weinig recente internationale statistieken die de militaire slagkracht van personeel weergeven. Een uitzondering is Global Fire Power (GFP), dat in 2025 over de hele linie de slagkracht in kaart brengt en deze van een index voorziet.¹² Gebaseerd op GFP-data wordt de personele militaire slagkracht – zowel voor actieve militairen als voor reservisten – voor Rusland en de Europese NAVO-landen op een rij gezet (zie Figuur 1).¹³

In totaal heeft Rusland 1,3 miljoen militairen en de Europese NAVO-landen samen 2 miljoen. Turkije en Polen hebben de grootste legers van de Europese NAVO met respectievelijk ruim 350.000 en 200.000 militairen. Qua reservisten is de overmacht van Europa nog groter. De

Europese NAVO heeft 3,5 miljoen reservisten tegen 2 miljoen voor Rusland. Het Verenigd Koninkrijk en Finland kennen de grootste groep reservisten met respectievelijk 925.000 en 870.000. Vooral Finland is interessant, omdat het een beperkt aantal beroepsmilitairen heeft (24.000), maar dus een enorme hoeveelheid reservisten. Relevant is uiteraard dat in 1939 de toenmalige Sovjet-Unie Finland binnenviel en het in ruil voor beëindiging van de oorlog een aantal stukken grondgebied aan de Sovjet-Unie moest afstaan. Sindsdien is landsverdediging en ook de opbouw van reservisten een belangrijk thema in dit land.

Op basis van de GFP-data is eveneens een vergelijking van het aantal actieve militairen in het fit-voor-militaire-service deel van de bevolking mogelijk. Deze geschiktheid voor militaire dienst is gedefinieerd als het deel van de populatie dat theoretisch beschikbaar is bij een oorlogsinspanning.¹⁴ Figuur 2 geeft het aandeel weer van actieve militairen in de fit-voor-

9 Ministerie van Defensie, *Defensienota 2026*, 58.

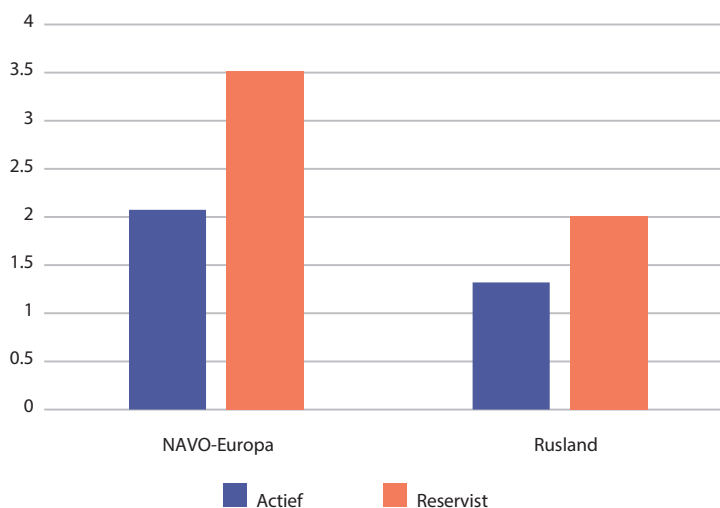
10 Centraal Planbureau, ‘Krappe arbeidsmarkt vraagt om keuzes’, 2024. Zie: www.cpb.nl. (2024).

11 Bureau Wordvoering Kabinetsformatie, *Aan de slag, Bouwen aan een beter Nederland*, 46.

12 Zie <https://www.globalfirepower.com/>.

13 Het betreft 29 landen (in alfabetische volgorde): Albanië, België, Bulgarije, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Italië, Kroatië, Letland, Litouwen, Luxemburg, Montenegro, Nederland, Noord-Macedonië, Noorwegen, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Turkije, het VK en Zweden. IJsland is niet opgenomen, omdat het geen eigen krijgsmacht heeft en voor Nederland heeft een actualisatie plaatsgevonden n.a.v. septembergegevens.

14 De website van GFP bevat geen exacte info hoe dit precies wordt bepaald. Op basis van de informatie voor Nederland kan worden aangenomen dat hiervoor een leeftijdsgrens wordt gehanteerd. Voor zover na te gaan heeft men in Nederland een leeftijdsgrens van 52 jaar genomen (die momenteel ook wordt gehanteerd voor reservisten).



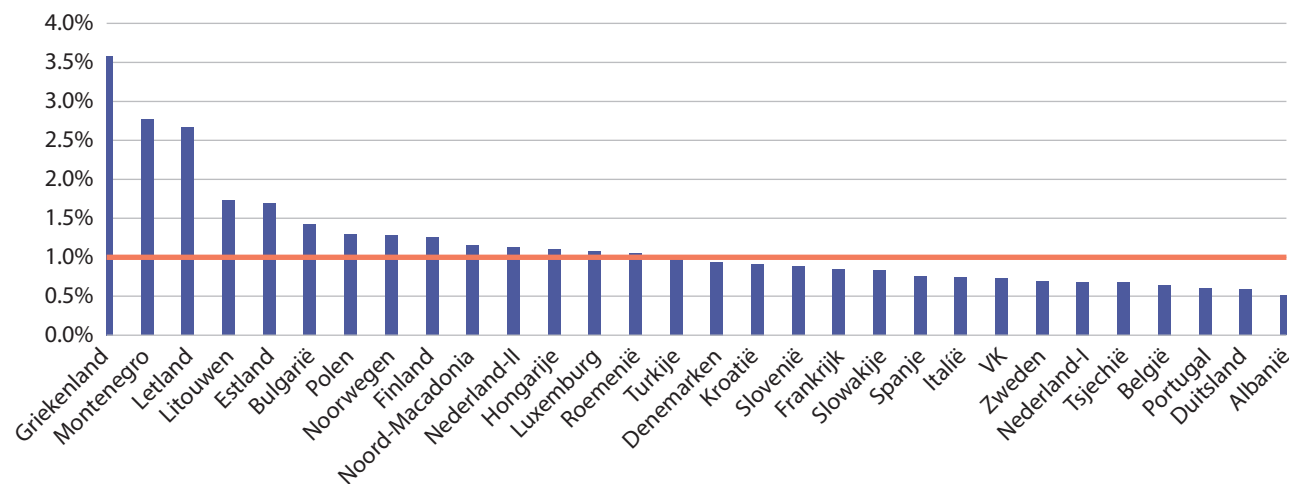
Figuur 1 Aantal militairen Rusland versus Europese NAVO (in miljoenen).

Bron: Global Fire Power

militaire-service bevolking van Europese NAVO-landen voor 2025.¹⁵

In het bijzonder springt Griekenland er uit met een aandeel van meer dan 3 procent. Gemiddeld is dit echter iets meer dan 1 procent, en 13 landen, voornamelijk Baltische en Scandinavische staten (behalve Zweden), hebben meer dan 1 procent. Nederland zit daar met 0,7 procent iets onder (Nederland-I). Nu past bij Nederland wel een kanttekening. Nederland kent relatief veel burgers bij Defensie, namelijk een derde van het personeel. In België is dit aanzienlijk lager, volgens het Belgische ministerie van Defensie slechts 6 procent.¹⁶

Voor het beslag op de arbeidsmarkt moet ook het burgerpersoneel worden meegenomen,



Figuur 2 Aandeel aantal actieve militairen in fit-voor-service-bevolking in 2025. Bron: Global Fire Power (voor Nederland-II inclusief burgerpersoneel)

omdat deze mensen niet elders inzetbaar zijn. In Figuur 2 is daarom voor Nederland ook het aandeel militairen plus burgerpersoneel berekend (Nederland-II). Dit gaat om 1,13 procent van de fit-voor-militaire-service bevolking. Dit is pakweg het gemiddelde van Europese NAVO-landen. Wanneer we er van uitgaan dat er in 2030 20.000 reservisten (met ook andere functie) zijn en dat de rest wordt aangevuld uit militairen en burgerpersoneel om de doelstelling van

¹⁵ Interessant zou zijn een vergelijking te maken met landen in Azië. Zo heeft China slechts een aandeel van 0,32 procent in de fit-voor-service bevolking en is het aantal Chinese militairen gedaald van 4 miljoen in 2000 tot 2,035 miljoen in 2025. Noord-Korea daarentegen kent 1,32 miljoen militairen uit een fit-voor-service-bevolking van 5,6 miljoen. De economische gevolgen van een zo'n groot beslag van militairen op de beroepsbevolking zijn dan ook enorm.

¹⁶ Zie Belgisch ministerie van Defensie, <https://www.mil.be/nl/>.

122.000 te halen, dan moet circa 1,75 procent van de Nederlandse fit-voor-service bevolking werkzaam zijn bij Defensie. Dit geeft ook aan dat de ambitie in het coalitieakkoord in internationaal opzicht hoog lijkt te zijn. Juist in een vergrijzende samenleving ligt het in de rede om meer in te zetten op een Europees leger of vergaande samenwerking van strijdkrachten in continentaal Europa.

Recruitment van jongeren

De defensie-recruitment richt zich – ook in Nederland – vooral op jongeren. GFP heeft om die reden de bevolking die de achttienjarige leeftijd bereikt in 2025 in kaart gebracht. Het betreft in Nederland een groep van pakweg 200.000. Terwijl Nederland in de overall ranking op plaats 36 van 145 landen staat, zijn er volgens deze ranking 74 landen met een grotere groep die deze (militaire) leeftijd van 18 jaar bereikt. Nogmaals een indicatie dat de vergrijzing aanstaande is en dat Nederland het zal moeten hebben van het slim inzetten van zijn bewapening en personeel.

Ook andere landen richten zich op het rekruteren van jongeren en de signalen daaruit zijn allerm minst hoopvol. Het Engelse tijdschrift *The Economist* spreekt over een ‘langdurige rekruteringscrisis’, waardoor landen als het VK en de VS niet in staat zijn geweest om hun rekruteringsdoelen te halen.¹⁷ Zo miste de VS deze doelen in 2022 en 2023 met 25 procent, wat neerkomt op ongeveer 15.000 actieve militairen per jaar. De verklaring is enerzijds dat minder mensen bereid zijn voor hun land te vechten dan tien jaar geleden, anderzijds omdat de geschiktheid van potentiële rekruten afneemt: ‘de meesten zijn te dik, te gedrogeerd of depressief om te dienen’. Slechts 23 procent van de Amerikanen van 17-24 jaar voldeed aan de eisen om zich aan te melden op basis van hun gewicht, medische aandoeningen en eerder drugsgebruik en ook Denemarken, Zweden en Groot-Brittannië wezen ongeveer 60 procent van de sollicitanten af. Overigens zijn er ook steeds meer signalen dat de mentale gezondheid van Nederlandse jongeren onder druk staat.

Een krijgsmacht van 122.000 betekent een beslag van bijna twee procent van de fit-voor-service bevolking en gaat ten koste van andere prioriteiten

The Economist gaat daarnaast in op de wijze waarop de strijdkrachten in continentaal Europa en het VK omgaan met de concurrentieslag op de arbeidsmarkt. In 2024 kregen Britse troepen hun grootste loonsverhoging in twee decennia en aanmeldbonussen zijn royaal. Huisvesting, gezondheidszorg, collegegeld, verhuizing en hypotheekfinanciering maken deel uit van een Brits contract. Ook in Nederland worden ruime arbeidsvoorwaarden geboden. Economen Van Kesteren, Rutten en Heyma laten zien dat de uurlonen van Defensie over de hele linie hoger liggen dan van vergelijkbare werknemers in andere sectoren.¹⁸ Gemiddeld lag het uurloon zo’n 14 procent hoger.

Een probleem is ook dat mensen bijna net zo snel de strijdkrachten verlaten als dat ze zich aansluiten. Eén op de vier nieuwe rekruten verlaat de Bundeswehr binnen zes maanden na toetreding; in België zou 44 procent binnen een

17 ‘Western armed forces have struggled to fill their ranks to deter Russia’, *The Economist*, 4 december 2025. Zie: <https://www.economist.com/international/2025/12/04/western-armed-forces-have-struggled-to-fill-their-ranks-to-deter-russia>.

18 J. van Kesteren, A. Rutten en A. Heyma, ‘Lonen bij Defensie hoger dan in andere sectoren’, *Me Judice*, 24 februari 2024. Zie: <https://www.mejudice.nl/artikelen/detail/lonen-bij-defensie-hoger-dan-in-andere-sectoren>.



Een Estse militair rondt zijn basistraining af. Estland zit in een groep landen met een bovengemiddeld aantal militairen als aandeel van de fit-voor-service-bevolking, Nederland zit onder het gemiddelde

jaar zijn vertrokken. Een van de redenen voor deze uitstroom vormt de moeilijkheid waarmee een normaal gezinsleven kan worden opgebouwd, omdat veel militairen elke anderhalf tot twee jaar van functie moeten wisselen en elders moeten wonen. Het artikel in *The Economist* bevat geen informatie voor Nederland, toch is er geen enkele indicatie dat het hier anders is. Uit een CBS-onderzoek uit 2019 blijkt dat in 2015-2017 jaarlijks bijna 10 procent van het defensie-

personeel uitstroomt.¹⁹ Uit een maatwerktabel blijkt dat dit recent nog iets is toegenomen.²⁰ Om die reden wil men het burgerpersoneel van Defensie en beroepsmilitairen die reeds zijn uitgestroomd actief benaderen om reservist te worden.

Slot

De ambitieuze plannen om onze krijgsmacht in 2030 tot 'minimaal 122.000 mensen' uit te breiden lijken niet realistisch. Onvoldoende helder is wat dit aantal betekent voor de defensieorganisatie inclusief de werving en selectie en ook voor de andere prioriteiten van de overheid. Ook de koppeling met een

¹⁹ Centraal Bureau voor de Statistiek, 'Defensiepersoneel, instroom en uitstroom, 2015-2017', 17 september 2019. Zie: <https://www.cbs.nl/nl-nl/maatwerk/2019/38/defensiepersoneel-instroom-en-uitstroom-2015-2017>.

²⁰ Centraal Bureau voor de Statistiek, 'Defensiepersoneel, instroom en uitstroom, 2018-2022', 2 april 2024. Zie <https://www.cbs.nl/nl-nl/maatwerk/2024/14/defensiepersoneel-instroom-en-uitstroom-2018-2022>.

opkomstplicht voor het geval deze opschaling niet slaagt verdient heroverweging. Liggen andere oplossingen niet meer voor de hand? En moet in een vergrijzende samenleving niet eerst nagegaan worden of oplossingen zoals een Europees leger of vergaande samenwerking in een Europese kopgroep aangegrepen moeten worden?

Juist in een vergrijzende samenleving biedt een Europees leger veel voordelen zoals verhoogde efficiëntie door minder overlap, specialisatie en een sterkere geopolitieke vuist. Het verdient aanbeveling om vooral specialisatie verder uit te werken. Nederland is van oudsher gespeciali-

seerd in maritieme operaties en luchtmacht en zou zich minder moeten toelagen op de landmacht. Het beroep op de arbeidsmarkt van deze krijgsmachtdelen is evident lager (van de operationele eenheden is in 2025 nog 46 procent van het personeel werkzaam bij de landmacht). De vaak genoemde nadelen zoals omvangrijke politieke besluitvormingsprocessen en de complexiteit in bevelstructuren kunnen in belangrijke mate overwonnen worden door oprichting van een Europese kopgroep van gelijkgestemde landen. Daarbij moet gedacht worden aan de landen die bij de start van de EU betrokken zijn zoals de Benelux, Duitsland, Frankrijk en Italië. ■



FOTO MCD BAREND WESTERVELD

De Karel Doorman neemt deel aan EU-operatie Aspides. Vergaande samenwerking in Europees verband, waarbij Nederland zich verder specialiseert in maritieme taken, zou een oplossing kunnen zijn die meer slagkracht genereert

Meaningful human control onder vuur

Verantwoord gebruik AI in het targetingproces tijdens Iron Swords

Dr. ir. Job Timmermans en luitenant-kolonel Stas Kloos*

Operationele toepassing van AI is essentieel voor een toekomstbestendige krijgsmacht. Een (ethisch) verantwoorde inzet is daarbij randvoorwaardelijk. Zo ook voor de ondersteuning door AI van het operationele targetingproces waarbij *meaningful human control* (MHC) als een vereiste geldt om menselijke (eind)verantwoordelijkheid te borgen. Ondanks theoretische en beleidsmatige aandacht ervoor blijft praktische reflectie op MHC achter. In dit paper wordt daarom een verkennend onderzoek gedaan naar de mogelijkheid van MHC in een praktijkcasus – Operatie Iron Swords – aan de hand van vijf kernelementen: *awareness, weaponeering, context control, prediction en accountability*.

FOTO MCD



Minister Brekelmans van Defensie benadrukte in 2024 op een top in Zuid-Korea het belang van verantwoordelijk militair gebruik van AI

Het onderzoek laat zien dat hoewel MHC in principe gerealiseerd kan worden, er drie risicofactoren zijn die MHC ondermijnen: een te hoge werklust, te weinig beschikbare tijd voor validatie en automatiseringsbias. Tot slot worden drie aanbevelingen gedaan die bijdragen aan de mitigatie van deze risico's.

Tijdens een AI-top in Zuid-Korea in september 2024, en wederom in Spanje in 2026, waar- schuwde minister van Defensie Brekelmans voor de hoge prijs die krijgsmachten zullen betalen als ze niet actief deelnemen aan AI-ontwik- keling.¹ Tegelijkertijd benadrukte hij het belang van verantwoordelijk militair gebruik van AI in lijn met de *political declaration* van de Global Commission on Responsible AI in the Military Domain (REAM).² Dit geldt zeker ook voor de inzet van AI bij targeting. In het operationeel targetingproces worden doelen geselecteerd, geprioriteerd en de juiste response bepaald, rekening houdend met operationele vereisten en capaciteiten.³ In de targeting cyclus spelen inlichtingen een cruciale rol in de ondersteuning van het besluitvormingsproces waarbij de toepassing van AI de snelheid en nauwkeurig- heid van besluitvorming in theorie significant kan verbeteren.^{4 5 6}

De automatisering van doelidentificatie en -selectie door AI roept echter fundamentele vragen op over menselijke betrokkenheid in besluitvorming. Naarmate AI-systemen een prominenter rol krijgen, dreigen menselijke controle en kritische oordeelsvorming af te nemen.⁷ Om de verantwoorde inzet van AI in het militaire domein te waarborgen is er internationale consensus dat er daarbij altijd *meaningful human control* (MHC) moet zijn.⁸ Hoewel er uiteenlopende definities zijn, houdt MHC in de kern in dat mensen – en niet algoritmes – uiteindelijk de controle moeten behouden over het gedrag van AI-systemen en daardoor ook moreel verantwoordelijk blijven.⁹ Het gaat verder dan het idee van een *human-in-the-loop* (bijvoorbeeld alleen maar op een knop hoeven drukken) door te waarborgen dat mensen over de nodige informatie, tijd en psychologische capaciteit beschikken om werkelijke (betekenisvolle) invloed uit te oefenen op een systeem.¹⁰

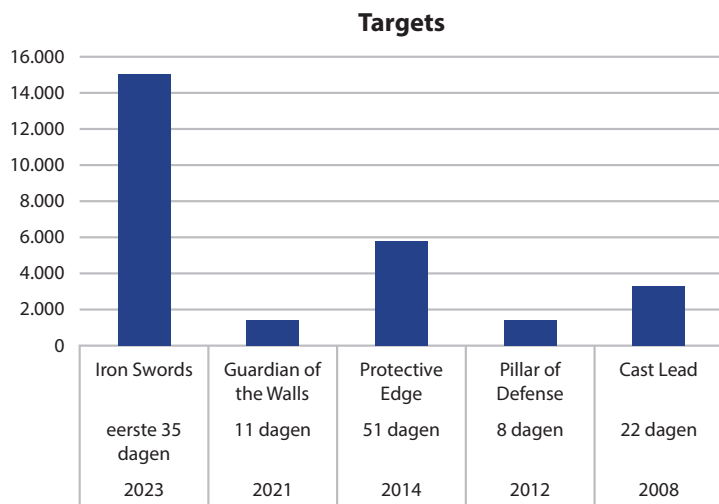
Ondanks de aandacht voor MHC in wetenschap- pelijke papers en beleidsstukken ontbreekt inzicht over het realiseren daarvan in de praktijk. Dit paper doet een eerste aanzet om deze lacune te dichten door de theoretische kenmerken van MHC te toetsen aan één van de eerste casussen waarbij AI uitgebreid is ingezet in verschillende fases van het targetingproces.¹¹

Operatie Iron Swords

Operatie Iron Swords is de vijfde oorlog binnen het Israël-Gaza conflict sinds 2008. Aanleiding is de aanval van Hamas op 7 oktober 2023, waarbij de terreurbeweging vanuit de Gazastrook nederzettingen in Israël aanviel. Als reactie daarop volgde met operatie Iron Swords een Israëlische militaire invasie in de Gazastrook.

* Job Timmermans is universitair hoofddocent Ethiek en Organisatie aan de Faculteit Militaire Bedrijfswetenschappen van de Nederlandse Defensie Academie; luitenant-kolonel Stas Kloos is senior stafofficier bij de Directie Plannen van de Defensiestaf. Hij rondde in 2025 de Hogere Defensievorming af. Dit artikel is een afgeleide van zijn HDV-thesis.

- 1 Ministerie van Defensie, 'Afspraken over kunstmatige intelligentie in militair domein zijn nodig en in ons belang', *defensie.nl*, 10 september 2024. Zie: <https://www.defensie.nl/actueel/nieuws/2024/09/10/brekelmans-afspraken-over-kunstmatige-intelligentie-in-militair-domein-zijn-nodig-en-in-ons-belang>.
- 2 O.Y. Shehabi en A. Lubin, 'Algorithms of War. Military AI and the War in Gaza', *Lieber Institute West Point*, 24 januari 2024. Zie: <https://lieber.westpoint.edu/algorithms-war-military-ai-war-gaza/>.
- 3 'NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting' (Brussel, NAVO, 2008).
- 4 M.A.C. Ekelhof, 'Lifting the fog of targeting', *Naval War College Review* 71 (2018) (3) 61-95.
- 5 H.W. Meerveld e.a., 'The irresponsibility of not using AI in the military', *Ethics and Information Technology* 25 (2023) (1) 1-14.
- 6 M.A.C. Ekelhof, 'AI is changing the battlefield, but perhaps not how you think. An analysis of the operationalization of targeting law and the increasing use of AI in military operations', in: R. Geiß en H. Lahmann (red.), *Research Handbook on Warfare and Artificial Intelligence* (Cheltenham, Edward Elgar Publishing, 2024) 161-178.
- 7 E. Chavannes en A. Arkhipov-Goyal, 'Towards Responsible Autonomy – The Ethics of RAS in a Military Context', *The Hague Centre for Strategic Studies* (2019) 1-83. Zie: <https://hcass.nl/report/towards-responsible-autonomy-the-ethics-of-ras-in-a-military-context/>.
- 8 J. Kwik, 'A Practicable Operationalisation of Meaningful Human Control', *Laws* 11 (2022) (3) 1-21.
- 9 L.C. Siebert e.a., 'Meaningful human control over AI systems. Beyond talking the talk', *arXiv* (2021).
- 10 F. Santoni de Sio en J.M. van den Hoven, 'Meaningful human control over autonomous systems. A philosophical account', *Frontiers in Robotics and AI* 5 (2018) (15) 1-14.
- 11 Shehabi en Lubin, 'Algorithms of War'.



Figuur 1 Aanvallen op targets in Gaza in verschillende IDF-operaties

Rond Iron Swords spelen (ethische) gevoeligheden. Het gebruik ervan als casuïstiek voor onderzoek is daarom ook gevoelig. Vanuit militair oogpunt biedt de casus echter een unieke inkijk in de inzet van AI bij targetting. Dit is uitermate relevant voor de Nederlandse krijgsmacht, juist ook wanneer het gaat om het garanderen van verantwoordelijk militair gebruik van AI. Zonder de bredere ethische discussie te bagatelliseren, beperken we ons tot de vraag of voldaan kan worden aan de voorwaarden van een verantwoorde inzet van AI bij targetting. Daarbij is de hoeveelheid (primaire) bronnen over Iron Swords zeer beperkt. Dit

onderzoek heeft daarom een sterk exploratief karakter waarbij wordt teruggevallen op extrapolatie en het doen van gefundeerde aannames.

In eerdere operaties waren de Israel Defense Forces (IDF) volledig afhankelijk van handmatig werk van inlichtingsofficieren om targets te genereren, wat resulteerde in een beperkte doelwittenlijst van slechts enkele tientallen hooggeplaatste individuen.¹² Tijdens Iron Swords is de taak van doelwitidentificatie grotendeels overgenomen door 'Lavender'. Op basis van informatie over bijna alle 2,3 miljoen inwoners van de Gazastrook,¹³ identificeert deze AI-applicatie mogelijke leden in de militaire vleugel van Hamas en Palestijnse Islamitische Jihad (PIJ) als potentieel doel.¹⁴ Dit leidde tot een drastische toename in het aantal gegenereerde targets en daarmee ook in het aantal aanvallen in Gaza (zie figuur 1).¹⁵

Deze ontwikkeling wordt verder ondersteund door de integratie van nog drie AI-decision support systems (AI-DSS) in het vervolg van de targetting-cyclus. Nadat doelwitten zijn geïdentificeerd lokaliseert 'The Gospel' gerelateerde infra-structuren van de militanten, zoals particuliere woningen,¹⁶ waarna 'Where's Daddy' de geïdentificeerde militanten volgt en de IDF in real-time informeert wanneer ze thuiskomen.¹⁷ 'Fire Factory', ten slotte, kan op basis van een analyse van data zoals historische gegevens over eerder goedgekeurde doelen, de benodigde hoeveelheid munitie berekenen, optimale tijdschema's voorstellen en de prioritering en toewijzing van doelen optimaliseren.¹⁹

Meaningful Human Control

Hoewel het aantal (type) targets en aanvallen significant is gestegen rijst de vraag welke impact dit heeft gehad op de menselijke controle op het proces. Om deze vraag te beantwoorden moet worden vastgesteld of er gedurende het proces is voldaan aan de eisen van MHC. Verschillende (academische) bronnen hebben suggesties gedaan voor kenmerken waaraan voldaan zou moeten worden om te kunnen

12 Y. Abraham, 'Lavender'. The AI machine directing Israel's bombing spree in Gaza', +972 Magazine, 3 april 2024. Zie: <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.

13 Idem.

14 E. Tekin, *Assessing Artificial Intelligence's Military Application in Urban War: A Study of the Israel Defense Forces Operations Since 2021* (Washington, D.C., George Washington University, 2024).

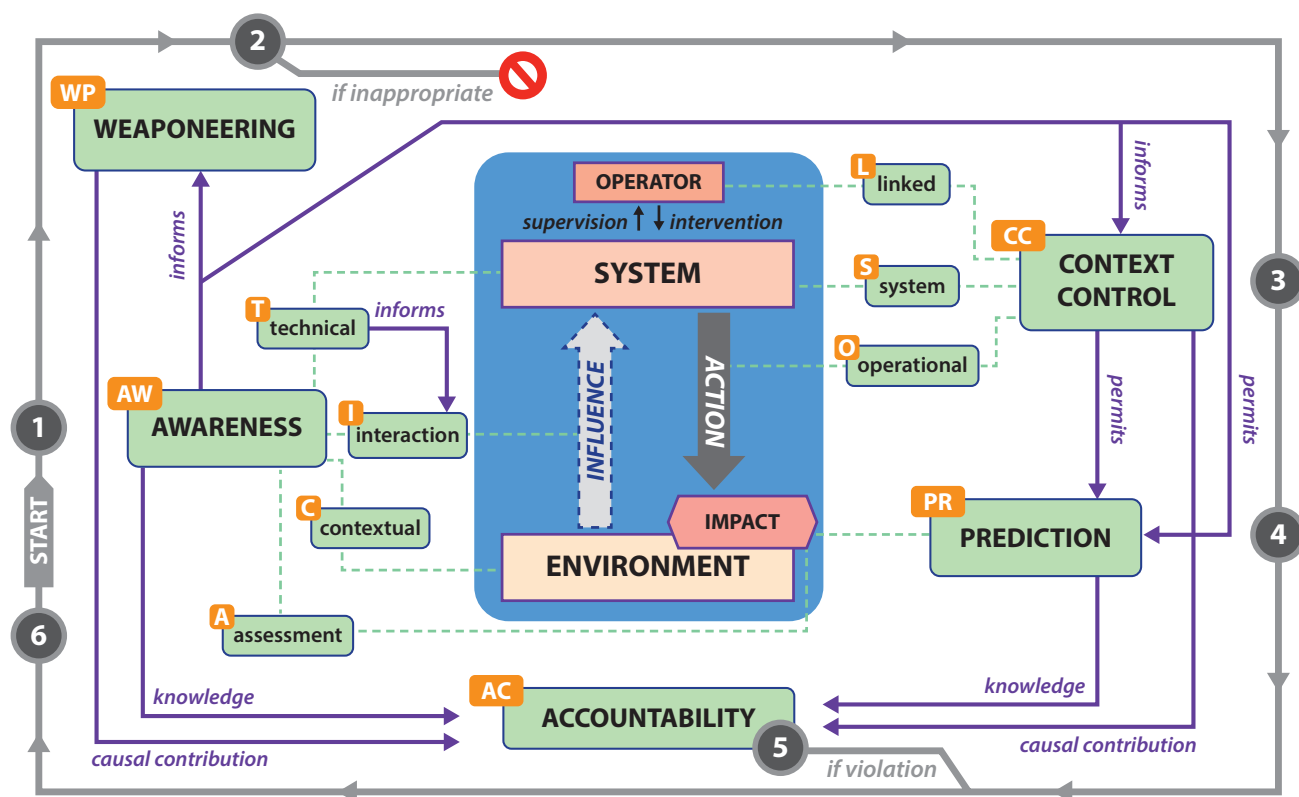
15 Idem.

16 IDF press release, 'A glimpse into the IDF's round-the-clock target enterprise', 2 november 2023.

17 R. Rommen, 'Israel's 'Where's Daddy' AI system helps target suspected Hamas militants when they're at home with their families, report says', *Business Insider*, 7 april 2024. Zie: <https://www.businessinsider.com/israel-ai-system-wheres-daddy-strikes-hamas-family-homes-2024?international=true&r=US&IR=T>.

18 Abraham, 'Lavender'.

19 M. Newman, 'Israel Quietly Embeds AI systems in Deadly Military Operations', *Bloomberg*, 16 juli 2023. Zie: <https://www.bloomberg.com/news/articles/2023-07-16/israel-using-ai-system>.



Figuur 2 Geïntegreerd MHC framework (Bron: Kwik 2022)

spreken van MHC bij de inzet van autonome wapen systemen (AWS).^{20 21 22} Het MHC-framework van Jonathan Kwik brengt deze kenmerken op een samenhangende manier bij elkaar.²³ Het identificeert vijf kernelementen – awareness, weaponneering, context control, prediction en accountability – die, aan elkaar gekoppeld, corresponderen met de causaliteit en chronologie van het militaire targetingproces (zie figuur 2).

Hieronder is voor ieder kernelement uiteengezet wat het vereist om vervolgens na te gaan of hier in operatie Iron Swords casus aan wordt voldaan of niet. Daarbij is geput uit verschillende publiek toegankelijke, openbare bronnen, bronnen afkomstig van Israëlische overheidsinstanties en interviews met anonieme Israëlische inlichtingsofficieren.²⁴

Element 1. Awareness

Awareness is essentieel om de inzetbeslissers in staat te stellen weloverwogen keuzes te maken

over wapeninzet.²⁵ Dit vereist inzicht in het functioneren van het systeem, de operationele omgeving en de mogelijke effecten.²⁶ Vier vormen van bewustzijn zijn hierbij van belang:

- 20 Article 36, 'Key Elements of Meaningful Human Control,' Background paper to comments prepared by Richard Moyes at the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, Switzerland, 11-15 april 2016.
- 21 Santoni en Van den Hoven, 'Meaningful human control over autonomous systems', 1-14.
- 22 R. Moyes, 'Autonomous weapon systems and the alleged responsibility gap,' in: *Autonomous Weapon Systems. Implications of Increasing Autonomy in the Critical Functions of Weapons* (Versoix, ICRC, 2017) 46-52.
- 23 J. Kwik, 'A Practicable Operationalisation of Meaningful Human Control', 1-21.
- 24 Rapportages van het Israëlisch onderzoekscollectief +972, *The Guardian* en *The Washington Post*, die interviews afnamen met anonieme IDF-militairen die tijdens operatie Iron Swords met AI decision support systems werkten.
- 25 M. Horowitz en P. Scharre, 'An Introduction to Autonomy in Weapon Systems', CNAS, 2025. Zie: <https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems>; ICRC, 'Views of the ICRC on autonomous weapon systems', paper presented at ICRC prepared for the Meeting of Experts on Lethal Autonomous Weapons Systems, Geneva, Switzerland, 11 april 2016.
- 26 J. van den Boogaard en M. Roorda, 'Autonomous' Weapons and Human Control', in: R. Bartels e.a. (red.), *Military Operations and the Notion of Control Under International Law* (Berlijn, Springer, 2021).

*Technical, Contextual, Interaction en Assessment awareness.*²⁷

1a Technical awareness

Technical awareness omvat begrip door de gebruikers van de functies, beperkingen en betrouwbaarheid van het systeem. In de casus wordt dit ondersteund doordat IDF-militairen uitgebreide training krijgen over de functionaliteiten van het AI-DSS.²⁸ Daarnaast zijn gebruikers in staat om inzicht te krijgen in de onderliggende data waarop het systeem zijn aanbevelingen baseert. Zo verklaart de IDF dat The Gospel de gebruiker de mogelijkheid biedt om 'beschikbare en begrijpelijke' data op te vragen waarmee het systeem zijn aanbevelingen genereert.²⁹ Een commandant van de eenheid die AI-toepassingen ontwikkelt omschrijft het in een interview als het achterlaten van technische 'broodkruimels' waardoor gebruikers in staat zijn om de aanbevelingen te reconstrueren.³⁰ Bovendien is de technologische betrouwbaarheid van AI-toepassingen zoals Lavender in de beginfase van het conflict door de IDF geverifieerd. Een steekproef toonde aan dat het systeem in 90 procent van de gevallen correct de link tussen individuen en Hamas identificeerde, wat leidde tot goedkeuring voor grootschalig gebruik.³¹

Israël heeft bovendien de ontwikkeling van AI gestimuleerd door de toepassingen voorafgaand aan operatie Iron Swords in bezette gebieden te testen, wat de operationele prestaties en betrouwbaarheid in relevante omgevingen verbeterde. Door gezichtsherkenning en biometrische dataverzameling in bezette

gebieden op de Westelijke Jordaanoever te gebruiken, kregen Israëlische technologie-bedrijven een uniek platform om hun AI-toepassingen praktisch te testen, verfijnen en valideren.

Daarentegen blijkt uit een *after-action report* dat het AI-systeem weliswaar veel trainingsgegevens had over wat als target werd beschouwd, maar tegelijkertijd informatie miste over zaken die menselijke analisten als *niet-target* hadden aangemerkt. Het Israëlische leger had de historische gegevens van afgewezen targets namelijk niet verzameld, waardoor de training van het AI-DSS in eerste instantie bevooroordeeld was geraakt.³² Algoritmes zijn zo goed als de data waarmee ze getraind zijn, en een fout in de data kan dus leiden tot het identificeren van verkeerde targets, wat de kans op burgerslachtoffers vergroot.

Ten slotte dienen gebruikers er op te kunnen vertrouwen dat het systeem *compliant* is aan het internationaal recht. In een persbericht verklaarde de IDF over The Gospel dat 'geldende voorschriften duidelijk vereisen dat voorgestelde targets in overeenstemming zijn met de relevante definities onder internationaal recht'.³³ Daarnaast geeft de krijgsmacht in hetzelfde statement aan dat de beslissing van een commandant om een aanval goed te keuren altijd onderworpen is aan de beperkingen van het internationale recht. Hiermee maakt Israël duidelijk dat het gebruik van AI-toepassingen gebonden is aan de regels voor onderscheid, proportionaliteit en voorzorgsmaatregelen onder het humanitair oorlogsrecht.

Verschillende juristen schrijven echter dat de praktijk uitwijst dat de toegenomen snelheid en schaal van targetting de morele terughoudendheid ten aanzien van het grondig valideren van targets onder Israëlische inlichtingenfunctionarissen vermindert.³⁴ Dit zou leiden tot disproportionele nevenschade, waardoor de naleving van de regels omtrent het beginsel van proportionaliteit onder het humanitaire oorlogsrecht twijfelachtig wordt. Juristen wijzen hier specifiek op het risico op burgerslachtoffers tijdens targetting. Het feit dat The Gospel huizen linkt aan Hamas-militanten en Where's Daddy

27 NB omdat awareness niet rechtstreeks is vast te stellen, is het geoperationaliseerd middels het al dan niet aanwezig zijn van de randvoorwaarden daarvoor.

28 I. Dolinko en L. Antebi, 'Embracing the Organized Mess. Defense AI in Israel', in: H. Borchert, T. Schütz en J. Verbovsky (red.), *The very Long game. 25 Case Studies on the Global State of Defense AI* (Heidelberg, Springer, 2024) 397-420.

29 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing', 18 juni 2024.

30 Newman, 'Israel Quietly Embeds AI systems in Deadly Military Operations.'

31 Abraham, 'Lavender'.

32 Tekin, *Assessing Artificial Intelligence's Military Application in Urban War*.

33 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

34 M. Bo en J. Dorsey, 'The 'Need' for Speed. The Cost of Unregulated AI Decision-Support Systems to Civilians', *OpinioJuris*, 24 april 2024, Zie: <https://opiniojuris.org/2024/04/04/symposium-on-military-ai-and-the-law-of-armed-conflict-the-need-for-speed-the-cost-of-unregulated-ai-decision-support-systems-to-civilians/>.



Een Israëlische eenheid op weg naar de grens met Gaza. Israël zegt dat beslissingen van commandanten altijd onderworpen zijn aan de beperkingen van het internationale recht

informeert wanneer deze militanten thuis zijn, vergroot de kans op onnodige burgerslachtoffers aanzienlijk wanneer deze vervolgens in hun huis aangevallen worden.

Daar staat tegenover dat er aan het begin van een militaire operatie *targeting guidance* uitgebracht wordt waarin ook het aantal geaccepteerde *non-combatant casualties* per aanval zijn opgenomen. Van operatie Iron Swords is bekend dat het aantal varieerde van vijf casualties bij *low-level*-militanten tot meer dan honderd voor Hamas-commandanten.³⁵ Los van het morele vraagstuk hoeveel burgerslachtoffers per aanval acceptabel zijn, is de IDF op dit vlak compliant aan IDF-regelgeving zolang een targeting operatie voldoet aan de gestelde eisen van het maximaal aantal burgerslachtoffers.

1b. Contextual awareness

Contextual awareness verwijst naar het begrijpen van de omgeving waarin het systeem zal functioneren. Dit vereist dat gebruikers beschikken over voldoende actuele informatie over de context.³⁶ Hoewel er geen directe informatie is over de toegang tot actuele en betrouwbare inlichtingen, kan een beredeneerde aanname gemaakt worden dat dit het geval is.

Op basis van hun beschrijvingen blijkt dat Lavender en The Gospel gebruik maken van data uit diverse bronnen. In de jaren voorafgaand aan de Hamas-aanval heeft de IDF uitgebreide systemen ontwikkeld voor het monitoren van Palestijnen in Gaza, waaronder biometrische databases, gezichtsherkenningstechnologie en cybersurveillancesystemen. Het is aannemelijk dat deze bronnen als actueel en betrouwbaar werden beschouwd voordat ze in de AI-toepassingen werden geïntegreerd.³⁷ Bovendien heeft de IDF verklaard dat voor systemen als Lavender en The Gospel regelmatige updates plaatsvinden.³⁸ Bij Where's Daddy gaat dit nog een stap verder, met continue updates gebaseerd op real-time positiebepaling van targets.³⁹ Het regelmatig updaten van het systeem met informatie en inlichtingen dient een dubbel

35 F. Wolfe, 'Pentagon Removed Non-Combatant Casualty Cut-Off Value From Doctrine in 2018', *Defense Daily*, 11 juni 2021, Zie: <https://www.defensedaily.com/pentagon-removed-non-combatant-casualty-cut-off-value-doctrine-2018/pentagon/>.

36 Moyes, 'Autonomous weapon systems and the alleged responsibility gap', 46-52.

37 S. Goodfriend, 'Israel's High-Tech Surveillance Was Never Going to Bring Peace', *Foreign Policy*, 30 oktober 2023, Zie: <https://foreignpolicy.com/2023/10/30/israel-palestine-gaza-hamas-war-idf-high-tech-surveillance/>.

38 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

39 Rommen, 'Israel's 'Where's Daddy' AI system helps target suspected Hamas militants'.

doel: het vergemakkelijkt de toegang van analisten tot relevante data en zorgt ervoor dat zij beter geïnformeerd zijn door de meest actuele inlichtingenbronnen.⁴⁰

1c. Interaction awareness

Interaction awareness is een meer geavanceerde vorm van technical awareness waarbij het niet alleen draait om begrip van het systeem zelf, maar ook van reacties daarvan op externe factoren zoals tegenmaatregelen van de tegenstander.

De voorspelbaarheid van reacties van een AI-DSS op zijn omgeving hangt af van de leercapaciteiten van dat systeem. Bij geavanceerde leercapaciteiten zijn interacties minder voorspelbaar, waardoor interaction awareness van groter belang is.⁴¹

Zoals hierboven aangehaald is er interactie tussen de applicaties en de context via de updates van de invoerdata. Met name Where's Daddy vertoont daarbij enige dynamiek doordat het real-time potentiële targets volgt.⁴² Hoewel de input van het AI-DSS dus veranderlijk is, wijzigt de manier van reageren door het systeem hierbij echter niet.

Daarnaast is bekend dat de IDF *machine learning*-technieken gebruikt om algoritmes te optimaliseren (zie hieronder).⁴³ Dit wijst op een potentieel meer adaptieve vorm van interactie met de omgeving in plaats van een puur reactieve. Het gaat hier echter nog om een optimalisatie van de algoritmen en niet om het veranderen van de onderliggende regels van het systeem voor het genereren van uitkomsten.⁴⁴ Ook in dit geval blijft de manier van reageren dus gelijk.

Ook zijn er geen directe indicatoren gevonden in de beschikbare informatie dat er sprake is van impact van tegenmaatregelen op het functioneren van de applicaties. Het uitblijven van een terugval in het aantal bombardementen suggereert dat Hamas nog geen effectieve tegenmaatregel heeft ontwikkeld, of dat de IDF

40 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

41 P.D. König e.a., 'Ch.2 Essence of AI. What Is AI?', in: L.A. DiMatteo, C. Poncibò, en M. Cannarsa (red.), *The Cambridge Handbook of Artificial Intelligence. Global Perspectives on Law and Ethics* (1st ed.) (Cambridge, Cambridge University Press, 2022) 18-34.

42 Abraham, 'Lavender'.

43 Tekin, *Assessing Artificial Intelligence's Military Application in Urban War*.

44 König e.a., 'Ch.2 Essence of AI. What Is AI?', 18-34.



Palestijnse brandweerlieden blussen de auto van politiechef Jamal Abu Kamil, die als 'target' om het leven kwam bij een Israëlische luchtaanval

in staat is geweest de eigen systemen aan te passen om de effectiviteit te behouden. De diversiteit aan inlichtingenbronnen die de IDF gebruikt voor triangulatie maakt het bovendien uitdagend voor Hamas om effectieve tegenmaatregelen te implementeren tegen het gehele spectrum van AI-toepassingen.

1d. Assessment awareness

Assessment awareness, ten slotte, richt zich op de continue evaluatie en verbetering van de ingezette AI-toepassingen, wat essentieel is voor het behouden en verhogen van de operationele effectiviteit.

De IDF hanteert hiertoe een systemische aanpak voor AI-toepassingen. Dit werd duidelijk tijdens de operatie tegen Hamas in 2021, waarbij de IDF 150 systeemupdates doorvoerde tijdens een tiendaagse operatie.⁴⁵ Deze frequentie van updates onderstreept de dynamische aard van de AI-systemen en de bereidheid van de IDF om snel aanpassingen door te voeren op basis van operationele ervaringen. In operatie Iron Swords zet de IDF deze praktijk voort. Feedback van inlichtingsofficieren wordt gebruikt om AI-algoritmes te verbeteren en te verrijken.⁴⁶ Naast menselijke feedback maakt de IDF ook gebruik van machine learning-technieken. Deze stellen de AI-toepassing in staat een eigen geautomatiseerd beoordelingsproces te doorlopen. Dit proces is dynamisch en wordt voortdurend verfijnd door de verwerking van nieuwe gegevens en de interne feedbackloop van het AI-DSS. Hierdoor kan het algoritme zijn voorspellende nauwkeurigheid in de loop van tijd verbeteren, wat leidt tot een steeds effectiever systeem.⁴⁷

Deze gelaagde aanpak van assessment, die zowel menselijke expertise als geavanceerde machine learning-technieken combineert, stelt de IDF in staat de AI-systemen continu te optimaliseren. Dit kan resulteren in een adaptief en steeds nauwkeuriger wordend systeem dat beter kan inspelen op de complexe en snel veranderende operationele omgeving.

2. Weaponeeing

Op basis van de informatie uit de awareness-fase, volgt bij weaponeeing het besluit om het

AI-gegenereerde target al dan niet op te volgen en te bepalen welke middelen nodig zijn om een gewenst effect te bereiken. In Iron Swords wordt dit proces ondersteund door Fire Factory.

Ondanks de integratie van Fire Factory wordt volgens de IDF 'de beslissing om al dan niet aan te vallen [...] genomen door de operationeel commandant'.⁴⁸ De commandant behoudt dus de *opt-out*-optie bij targetingsbeslissingen.

Daarnaast houden operators toezicht op Fire Factory en beoordelen de voorgestelde toebereiding van wapens en inzetmiddelen. Hierbij hebben ze de bevoegdheid om de aanbevelingen goed te keuren of te verwerpen.⁴⁹

De mogelijkheid voor commandanten en operators om AI-gegenereerde voorstellen niet op te volgen waarborgt dat kritische beslissingen over de inzet van militaire middelen niet volledig worden overgelaten aan geautomatiseerde systemen, maar altijd onderworpen blijven aan menselijk oordeel.

3. Context control

Zodra commandanten ervoor kiezen een AI-systeem in te zetten, kunnen zij middels drie vormen van *context control* aanvullende beperkingen op het systeem afdwingen, namelijk: *system control*, *operational control* en *linked control*.

3 a. System control

System control verwijst naar het aanpassen van de parameters van het AI-systeem. Voortvloeiend uit zijn *guidance, intent & direction* kan de commandant beperkingen opleggen in de vorm van de taken die het systeem mag uitvoeren, zoals bijvoorbeeld *targeting restrictions* op bepaalde targets of strijdende partijen.

Onderzoek heeft aangetoond dat het algoritme van Lavender kan worden verfijnd en dat parameters ook tussentijds zijn aangepast door

45 C. Yoav, AI in Defense – Digital Transformation and AI in the Intelligence Domain (Israel, Tel Aviv University, 13 februari 2023) Zie: <https://www.youtube.com/watch?v=CJvOoX7dK1M>.

46 H. Davies en B. McKernan, 'IDF colonel discusses 'data science magic powder' for locating terrorists', *The Guardian*, 11 april 2024, Zie: <https://www.theguardian.com/world/2024/apr/11/idf-colonel-discusses-data-science-magic-powder-for-locating-terrorists>.

47 Tekin, *Assessing Artificial Intelligence's Military Application in Urban War*.

48 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

49 Newman, 'Israel Quietly Embeds AI systems in Deadly Military Operations'.

de IDF.⁵⁰ Zo kon de drempelwaarde voor banden tussen een individu en Hamas worden gewijzigd. Door deze parameter aan te passen worden meer of minder individuen gelieerd aan Hamas, waardoor Lavender meer of minder targetsuggesties deed.⁵¹ Daarnaast is ook de parameter voor geaccepteerde burgerslachtoffers aangepast, wat het aantal suggesties van Where's Daddy beïnvloedde wanneer familieleden bij een target aanwezig waren.⁵²

3b. Operational control

Operational control betreft het beperken van de acties die het systeem kan uitvoeren in de operationele omgeving. Dit wordt gerealiseerd door de operationele context te reguleren. Voor Iron Swords zijn er geen directe indicatoren gevonden die duiden op het beperken van de acties die het AI-DSS kan uitvoeren in de operationele omgeving. Het is echter aannemelijk dat operational control wordt gerealiseerd door de operationele context te reguleren op basis van afgebakende datasets. Door bijvoorbeeld uitsluitend persoonsgegevens, telefoondata of satellietbeelden te gebruiken van Gaza en van een afgebakende recente periode, is er ook ruimtelijke of tijdgebonden controle die zorgt voor context control.

3c. Linked control

Linked control, ten slotte, is een speciale vorm van context control waarbij een voortdurende verbinding tussen het AI-systeem en een menselijke operator wordt vereist. Dit stelt de operator in staat om in te grijpen en aanvallen te initiëren en te beëindigen.⁵³

Voor Iron Swords komt een gemixt beeld naar voren ten aanzien van Linked control. Officieel stelt de IDF dat er duidelijke richtlijnen zijn voor gebruik van AI-toepassingen.⁵⁴ De identificatie van targets wordt altijd gedaan door mensen en niet door technologische toepassingen.⁵⁵ Er mag niet uitsluitend worden vertrouwd op een suggestie van Lavender of The Gospel.⁵⁶ Deze bindende instructies zouden een integraal onderdeel vormen van de opleiding en training van IDF-personeel en men is verplicht om volgens deze procedures te opereren.⁵⁷

De praktijk van menselijke supervisie over AI-gegenereerde targets lijkt echter significant af te wijken van het officiële beleid. Tegenover het statement van de IDF staan de praktijkervaringen van verschillende anonieme Israëlische inlichtingenofficieren die direct betrokken zijn bij het gebruik van AI voor het genereren van targets tijdens Iron Swords. Zij verklaren dat na een initiële interne controle die aangaf dat Lavenders suggesties in 90 procent van de gevallen nauwkeurig waren, de IDF brede goedkeuring gaf aan analisten om deze suggesties over te nemen zonder grondige validatie.⁵⁸ Er moest snel gewerkt worden en er was geen tijd om diep in de voorgestelde targets te duiken.⁵⁹ De druk om snel te werken en een hoog aantal targets te genereren heeft geleid tot een situatie waarin menselijke analisten minimale tijd besteedden aan het beoordelen van AI-voorstellen.⁶⁰

De discrepantie tussen het officiële IDF-standpunt en de operationele realiteit is veelbetekend. Het snelle tempo van doelwitgeneratie door AI-systemen, gecombineerd met de beperkte tijd voor menselijke beoordeling, creëert een situatie die mogelijk niet voldoet aan wettelijke en morele verplichtingen om onnodige slachtoffers te voorkomen.⁶¹ ⁶² Deze omstandigheden vergroten het risico op automatiseringsbias, waarbij analisten onder

50 Newman, 'Israel Quietly Embeds AI systems in Deadly Military Operations.'

51 Abraham, "'Lavender': The AI machine directing Israel's bombing spree in Gaza'.

52 Idem.

53 Article 36, 'Killer Robots. UK Government Policy on Fully Autonomous Weapons', *Technical Report* (Londen, Article 36, 2013).

54 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

55 E. Dwoskin, 'Israel built an 'AI factory' for war. It unleashed it in Gaza', *The Washington Post*, 29 december 2024, Zie: <https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/>.

56 Idem.

57 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

58 Abraham, 'Lavender'.

59 Y. Abraham, 'A mass assassination factory: Inside Israel's calculated bombing of Gaza', *+972 Magazine*, 3 april 2024, Zie: <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.

60 Idem.

61 T. Mimran en G. Dahan, 'Artificial Intelligence in the Battlefield. A Perspective from Israel', *OpinioJuris*, 24 april 2024, Zie: <https://opiniojuris.org/2024/04/20/artificial-intelligence-in-the-battlefield-a-perspective-from-israel/>.

62 J. Dorsey en M. Bo, 'AI-Enabled Decision-Support Systems in the Joint Targeting Cycle. Legal Challenges, Risks, and the Human(e) Dimension.', *International Law Studies* 106 (2025) 1-45.



FOTO ANP/XINHUA, RIZEK ABDELJAWAD

Omstanders inspecteren de schade na een Israëlische luchtaanval in Khan Younis. De praktijk van menselijke supervisie over AI-gegenereerde targets lijkt significant af te wijken van het officiële Israëlische beleid

druk geneigd zijn AI-aanbevelingen te snel en onkritisch te accepteren.⁶³

De neiging om besluitvorming uit te besteden aan geautomatiseerde systemen wordt versterkt in complexe situaties met hoge cognitieve belasting. Onderzoek toont aan dat mensen in omstandigheden gekenmerkt door hoge complexiteit, druk, stress en tijdsbeperkingen eerder geneigd zijn het oordeel van machines te volgen.⁶⁴ Deze dynamiek vergroot de kans op overmatig vertrouwen in AI-systemen, zelfs wanneer er mogelijk tegenstrijdige informatie beschikbaar is.

4. Prediction

Prediction heeft betrekking op de voorspelbaarheid van AI-toepassingen in de

inzetomgeving en de mate waarin deze het beoogde effect bereiken. Voorspellend inzicht wordt vaak genoemd als een essentiële vereiste voor een commandant om meaningful control uit te oefenen.⁶⁵ Commandanten moeten niet alleen weten wat de beoogde effecten zijn, maar ook inzicht hebben in mogelijke incidentele en onbedoelde gevolgen van AI-inzet.^{66 67}

63 Bo en Dorsey, 'The 'Need' for Speed'.

64 Idem.

65 J. Kwik, 'A Practicable Operationalisation of Meaningful Human Control', 1-21.

66 UNIDIR, 'The Weaponization of Increasingly Autonomous Technologies. Considering How Meaningful Human Control Might Move the Discussion Forward', *Technical Report UNIDIR*, Resources No. 2 (Geneva, UNIDIR, 2014).

67 D. Garcia, 'ICRAC Statement on Technical Issues to the 2014 UN CCW Expert Meeting', *Technical Report*, ICRAC, 4 december 2024. Zie: <https://www.icrac.net/icrac-statement-on-technical-issues-to-the-2014-un-ccw-expert-meeting>.

Uit de bronnen komen aspecten naar voren die er op wijzen dat de IDF kennis heeft van de mate van nauwkeurigheid van de AI-applicaties. Steekproeven toonden een nauwkeurigheid van 90 procent aan.⁶⁸ Een hoge nauwkeurigheid zorgt ervoor dat de applicatie het beoogde effect bereikt, draagt bij aan de voorspelbaarheid van de systemen en versterkt het vertrouwen van commandanten in de AI-gegenereerde aanbevelingen.

Desondanks zijn IDF-functionarissen zich bewust van de beperkingen en potentiële onbedoelde effecten van AI-inzet. Een treffend voorbeeld hiervan is het gebruik van Where's Daddy, het systeem dat militanten lokaliseert op basis van telefoongegevens.

Inlichtingenfunctionarissen erkennen het risico dat een target zijn telefoon aan zijn zoon, oudere broer of gewoon een willekeurige man kan overdragen, wat kan leiden tot het onbedoeld treffen van burgers.⁶⁹ Dit bewustzijn van mogelijke foutmarges is cruciaal voor het behouden van menselijke controle en het voorkomen van onbedoelde slachtoffers.

Een ander voorbeeld komt naar voren in een interne audit. Deze onthulde onnauwkeurigheden in AI-systemen voor het verwerken van de Arabische taal, met name bij het interpreteren van slangwoorden en -uitdrukkingen.⁷⁰ Deze tekortkoming kan leiden tot het aandragen van bepaalde targets op basis van verkeerde vertalingen van specifieke woorden.

Hoewel er minder uitgebreid is gerapporteerd over het aspect van prediction in vergelijking met *context control*, bieden deze voorbeelden duidelijke indicaties dat de IDF actief streeft naar inzicht in de voorspelbaarheid van hun AI-systemen. Het bewustzijn van zowel de kracht als de beperkingen van AI-toepassingen is essentieel voor het handhaven van MHC in militaire besluitvorming.

5. Accountability

Het uiteindelijke doel van MHC is betekenisvolle controle als voorwaarde voor het kunnen toekennen van accountability ofwel (eind) verantwoordelijkheid aan de menselijke operator – ultimo de commandant – voor de toepassing van AI in de targeting cyclus. Accountability volgt wanneer alle voorgaande vier kernelementen correct en in samenhang zijn geïmplementeerd.

Zo zorgen awareness en predictability ervoor dat de commandant over de nodige (technische) kennis en voorspellend inzicht over het AI-DSS beschikt, terwijl de kernelementen weaponering en context control het daadwerkelijke handelen met het AI-systeem omvatten die tot het resultaat hebben geleid. Om de samenhang tussen de kernelementen te borgen is het daarbij vereist dat er een duidelijke structuur van verantwoordelijkheid is.⁷¹

In tabel 1 zijn de bevindingen per kernelement samengevat. Hieruit blijkt dat op basis van bronmateriaal de aanwezigheid van alle vier de kernelementen is te onderbouwen. De implementatie van de elementen is echter niet eenduidig.

Bij (technical) awareness en (linked) context control is het beeld dat rijst uit de interpretatie van de bronnen ambigu (gele arcering). Automatiseringsbias, de ervaren werklust door het grote aantal AI-gegenereerde targets en de beperkte tijd (daardoor) voor controle en validatie hebben er toe geleid dat er in de praktijk niet altijd MHC was over targeting-beslissingen tijdens operatie Iron Swords. Dit duidt op het bestaan van een discrepantie tussen de beoogde toepassing en daadwerkelijke gebruik van AI-DSS binnen de operationele context.

Ook ten aanzien van de aanwezigheid van verantwoordelijkheidsstructuren zijn de bronnen niet eenduidig (zie tabel 1).

In een officieel statement tijdens operatie Iron Swords heeft de IDF de verantwoordelijkheidsstructuur voor targeting uiteengezet, waarbij de nadruk ligt op de centrale rol van de operationeel commandant.⁷² Volgens de IDF maakt target identificatie, al dan niet uitgevoerd door een AI-DSS, deel uit van een breder

68 Abraham, 'Lavender'.

69 Idem..

70 Dwoskin, 'Israel built an 'AI factory' for war'.

71 Article 36, 'Key Elements of Meaningful Human Control', Background paper to comments prepared by Richard Moyes at the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, Switzerland, 11-15 april 2016.

72 IDF press release, 'The IDF's Use of Data Technologies in Intelligence Processing'.

	Element	Factor	Onderbouwing
1	Awareness		
1a	Technical	Technologische betrouwbaarheid	Validatie van targets vooraf & tijdens operatie, hoewel met initiële bias door ontbreken niet-target data.
			Aanvankelijk uitgebreide controles, namen echter af nadat vertrouwen in systeem toenam.
		Technologische transparantie	Gebruikers krijgen uitgebreide trainingen in functionaliteiten en hebben inzicht in data.
		Compliance	Beslissing over en eisen aan targets conform internationaal recht. Door schaal, snelheid en methode AI echter onnodige burgerslachtoffers.
1b	Contextual	Toegang tot informatie	Veel (soorten) betrouwbare data door jarenlange surveillance vooraf.
		Inlichtingenupdates	Lavender en The Gospel regelmatig geüpdatet en Where's Daddy continu door real-time positie bepaling van targets.
1c	Interactional	Complexiteit interactie	Interactie van het systeem met zijn context via input en machine learning heeft echter geen impact op manier van reageren door systeem.
		Impactanalyse tegenmaatregelen	Geen afname bombardementen dus geen indicatie voor tegenmaatregelen Hamas.
1d (6)	Assessment	Evaluatie	Hoge frequentie van updates op basis van operationele ervaringen.
		Verbetering	Feedback van inlichtingenofficieren wordt gebruikt om AI-algoritmes te verbeteren en te verrijken; daarnaast machine learning voor zelfverfijning van het systeem.
2	Weaponering	Beslissingsbevoegdheid (opt-out)	Aanvalsbeslissing bij operationeel commandant, daarnaast toezicht operators op voorgestelde toedeling wapens en inzetmiddelen.
3	Context control		
3a	System	Configuratie	Algoritme van Lavender (en Where's Daddy) kan worden verfijnd en parameters zijn tussentijds aangepast.
3b	Operational	Beperkingen	Operationele context te reguleren op basis van afgebakende datasets.
3c	Linked	Human control	Officieel duidelijke richtlijnen gebruik AI, in praktijk echter, door hoge druk om snel te werken, gebrekkige validatie van targets door analisten.
			Omstandigheden die kunnen leiden tot automation bias.
4	Prediction	Voorspelbaarheid	Steekproeven wijzen op hoge nauwkeurigheid, IDF-functionarissen zijn zich echter bewust van de beperkingen (foutmarges) en potentiële onbedoelde effecten van AI-inzet.
		Impactanalyse	Voorbeelden geven indicaties dat IDF actief streeft naar inzicht in de voorspelbaarheid.
5	Accountability	4 elementen correct geïmplementeerd	Bronnen (& aannames) wijzen op de aanwezigheid van alle voorgaande elementen in het proces, hoewel niet eenduidig geïmplementeerd (zie gele arcering).
		Structuur van verantwoordelijkheid	Een verantwoordelijkheidsstructuur die de commandant expliciet centraal stelt, Israël erkent echter internationale rechtsinstanties niet, zodat commandanten niet internationaal berecht kunnen worden.

Tabel 1 Overzicht uitkomsten (NB Gele arcering betekent: geen eenduidige implementatie)



De Israëlische premier Benjamin Netanyahu overlegt met de Amerikaanse president Trump. De premier en Israëlische commandanten genieten een zekere mate van internationale strafrechtelijke immuniteit

targetingproces. De uiteindelijke beslissing om een aanval uit te voeren ligt bij de operationeel commandant. Deze beslissing wordt genomen na zorgvuldige afweging van alle beschikbare informatie over het target, inclusief operationele, beleidsmatige, humanitaire en juridische aspecten. De IDF benadrukt dat het de operationele commandanten zijn die aanvallen goedkeuren, niet de inlichtingenanalisten of technologische hulpmiddelen.

De praktische uitvoering van accountability wordt echter gecompliceerd door Israël's internationale juridische positie. Israëlische commandanten genieten een zekere mate van internationale strafrechtelijke immuniteit, aangezien Israël internationale rechtsinstanties

waaronder het Internationaal Strafhof in Den Haag niet geheel erkent.⁷³ Bovendien is Israël geen partij bij het Aanvullend Protocol I bij de Verdragen van Genève van 1949, waarin de 'law of targeting' is vastgelegd.⁷⁴ Dit betekent dat als Israëlische commandanten worden beschuldigd van oorlogsmisdaden, zij mogelijk niet door Israël zullen worden uitgeleverd aan internationale tribunalen.

Deze juridische situatie creëert een spanningsveld tussen de interne verantwoordingsstructuren van de IDF en de internationale mechanismen voor oorlogsrechtshandhaving. Hoewel militaire commandanten theoretisch kunnen worden opgepakt en uitgeleverd aan het Internationaal Strafhof als ze zich bevinden op het grondgebied van een van de meer dan honderd landen die lid zijn van het hof,⁷⁵ blijft de praktische uitvoering van internationale accountability beperkt.

Conclusie en aanbevelingen

Het hier gepresenteerde onderzoek naar MHC heeft een sterk exploratief karakter. Het beperkte aantal bronnen en het ontbreken van

73 D. Benoliel en R. Perry, 'Israel, Palestine, and the ICC', *Michigan Journal of International Law*, 11 februari 2010. Zie: <http://www.icc-cpi.int/NR/rdonlyres/4CC08515->.

74 Merriam, 'Inside IDF Targeting'.

75 'Strafhof vaardigt arrestatiebevelen uit tegen Netanyahu, Gallant en Hamas-leider', *NOS*, 21 november 2024, Zie: <https://nos.nl/artikel/2545356-strafhof-vaardigt-arrestatiebevelen-uit-tegen-netanyahu-gallant-en-hamas-leider>.

76 Zoals hierboven naar voren is gekomen bij de bespreking van het kernelement interactional awareness (1c).

77 König, Krafft, Schulz en Zweig, 'Ch.2 Essence of AI: What Is AI?', 18-34.

primaire bronnen noopt tot extrapolatie en soms tot het doen van gefundeerde aannames en daarmee tot terughoudendheid in het trekken van conclusies. MHC is bovendien nog geen vaststaand concept en het gebruikte framework is dus ook niet definitief of uitputtend. Daarnaast kan er ook gekozen worden voor een alternatieve operationalisering van de verschillende elementen daarvan.

Desalniettemin biedt de analyse een (eerste) waardevolle blik op hoe MHC kan worden geïmplementeerd in de militaire operationele praktijk. Hieruit rijst een gemengd beeld. Hoewel er voor alle elementen onderbouwing naar voren komt uit de analyse is deze niet altijd eenduidig. Dit wijst op een discrepantie tussen de papieren werkelijkheid en de toepassing van AI-DSS in de praktijk. Dit betekent echter niet dat er principiële, onoverkomelijke belemmeringen zijn voor MHC bij AI-ondersteunde targeting. Er zijn eerder risicofactoren zoals een te hoge werklast, te grote snelheid en (automatiserings)bias die MHC potentieel kunnen ondermijnen.

Een voorbehoud hierbij is de mate van 'geavanceerdheid' van de AI. Tijdens de operatie Iron Swords is de relatie van de AI-applicaties tot hun omgeving reactief van aard en heeft machine learning een beperkte impact.⁷⁶ De voorspelbaarheid van het systeem is daardoor relatief hoog. Bij toenemende complexiteit van AI in de toekomst, bijvoorbeeld wanneer het de onderliggende regels voor hoe te reageren zelf kan veranderen, is dit echter minder het geval.⁷⁷ Het implementeren van MHC wordt daarmee moeilijker te realiseren.

Desondanks zijn uit het onderzoek drie belangrijke lessen te trekken voor de Nederlandse krijgsmacht.

Ten eerste verdient het aanbeveling om bij de integratie van AI binnen de Nederlandse krijgsmacht MHC te nemen als een kerncriterium in ontwikkelings-, inkoop- en integratieprocessen. Dit betekent dat AI-systemen zo ontworpen en ingezet moeten worden dat menselijke besluitvorming centraal blijft staan. Dit onderzoek toont aan dat het technisch mogelijk is om MHC toe te passen op AI-

gestuurde targetingbeslissingen. Daarom is het essentieel dat ook de Nederlandse Defensie bij het ontwikkelen of aanschaffen van AI-toepassingen expliciete eisen stelt. Dit kan door het gebruiken van een MHC-raamwerk bij ontwikkelings- of aanschafnormen die de menselijke rol in kritieke besluitvormingsprocessen waarborgen.

Ten tweede toont het onderzoek aan hoe MHC tijdens Iron Swords afneemt door de ervaren werklast door het grote aantal AI-gegenereerde targets en de beperkte tijd voor validatie. Om dit te voorkomen is het aan te bevelen te zorgen voor een werkklimaat waarin operators voldoende tijd krijgen om AI-voorgestelde targets kritisch te beoordelen. Daarbij is het van belang om de opt-out te benadrukken, zodat de operators AI-beslissingen kunnen verwerpen of herzien.

Ten slotte blijkt uit het onderzoek dat als gevolg van een hoge initiële AI-nauwkeurigheid, de menselijke controle steeds minder intensief werd toegepast. Vormen van bias moeten daarom expliciet worden behandeld in AI-trainingen binnen Defensie. Daarbij is het van belang dat wordt geleerd om AI-uitkomsten kritisch te evalueren en om bewustzijn te creëren over hoe cognitieve processen het gebruik van AI beïnvloeden.

Eerder is gerefereerd aan de politieke gevoelheden die bestaan omtrent operatie Iron Swords. Omdat dit artikel zich beperkt tot de mogelijkheid van een verantwoorde militaire inzet van AI is het daarom belangrijk ook de invloed van politiek-strategische overwegingen in ogen-schouw te nemen. Het verdient daarom aanbeveling om dit perspectief te onderzoeken in verdere research. ■

Er zijn geen principiële, onoverkomelijke belemmeringen voor Meaningful Human Control bij AI-ondersteunde targeting



Dat de digitalisering doorzet bewijst onder meer de F-35, een vliegende 'datastofzuiger' die vol zit met technologie

FOTO MCD, JAN DIJKSTRA

Het versterken van warfighting capabilities door digitalisering

Commandeur b.d. Peter van den Berg

Dr. ir. Michiel Borgers

Brigade-generaal Aard Lettink

Ir. Rob Schepens*

Drones, cyberaanvallen, ontploffende piepers, unmanned vehicles, desinformatie: de digitalisering in het militaire conflict neemt steeds verder toe en zou zomaar in een toekomstig conflict het verschil kunnen maken. Hoe kan Defensie in een gewapend conflict doeltreffender optreden door de inzet van IT? Op basis van een analyse van recente conflicten geeft dit artikel een overzicht van *warfighting capabilities* en hoe de digitalisering die capability heeft verbeterd. Welke warfighting capabilities zijn in het gevecht essentieel en hoe kan digitalisering die versterken?

* Cdr b.d. Peter van den Berg is strategisch adviseur IT bij CZSK; dr. ir. Michiel Borgers is directeur JIVC (het IT-bedrijf van Defensie); brigade-generaal Aard Lettink is decentrale Chief Information Officer bij de Koninklijke Marchaussee; ir. Rob Schepens is decentrale Chief Information Officer bij de Bestuursstaf van Defensie.

1 Digitalisering: wanneer data uit de hele organisatie en haar omgeving worden verwerkt met behulp van geavanceerde digitale technologieën, wat leidt tot fundamentele veranderingen in bedrijfsprocessen die kunnen leiden tot nieuwe bedrijfsmodellen en sociale veranderingen.

Digitalisering van het gevecht

Digitalisering,¹ als instrument om doelen te bereiken door middel van technologische innovaties en digitale transformaties, heeft op veel plekken in de maatschappij voor een fundamentele verandering gezorgd. Voorbeelden hiervan zijn Airbnb in de recreatiesector, het

thuiswerken met *video conferencing* en de cryptovaluta en digitaal bankieren in de banksector. Op het militaire vlak is deze fundamentele verandering ook al in gang gezet. De traditionele manier van oorlogvoering wordt gecombineerd met de inzet van (digitale) technologieën om het beoogde effect te realiseren. De adequate inzet van gedigitaliseerde warfighting capabilities² is daarmee van cruciaal belang voor de militair om succesvol te zijn in het conflict. Recente conflicten worden gekenmerkt door de inzet van veel nieuwe technologie, maar kijkend naar de mogelijkheden van AI en quantum-technologie is de verwachting dat de digitalisering een nog grotere impact zal hebben.

Sinds de grootschalige inval van Rusland in Oekraïne op 24 februari 2022 is een verandering in het gevecht zichtbaar geworden. Meerdere (gewapende) conflicten in een breed geopolitiek spectrum hebben elkaar in hoog tempo opgevolgd, met een paradigmaverschuiving van pure kinetische oorlogvoering naar het hybride gevecht. Het gevecht wordt meer en meer gevoerd in het digitale domein. Het fysieke domein kent de inzet van grote hoeveelheden drones en onbemande voertuigen, dit alles ondersteund door de inzet van AI. Op het slagveld van Oekraïne worden nieuwe technologieën in snel tempo geïntroduceerd, uitgetest en verbeterd.

Digitalisering als multiplier

Uit de geschiedenis blijkt dat er bij elk gewapend conflict een versnelling in de technologische ontwikkeling plaatsvindt. De opkomst van computers tot en met het ontdekken van nieuwe ruimtetechnologieën zijn hier voorbeelden van. In de Tweede Wereldoorlog zorgde de computer, onder meer ontwikkeld door Alan Turing, er voor dat met de Enigma gecodeerde berichten van de Duitsers ontcijferd konden worden. Dit zou er zelfs voor gezorgd hebben dat de geallieerden uiteindelijk zouden overwinnen.³ Deze nieuw ontwikkelde computer zorgde voor de juiste informatiepositie en verbetering van wat tegenwoordig Informatiegestuurd Optreden wordt genoemd.⁴ De technologische ontwikkelingen hebben sinds de Tweede Wereldoorlog niet stilgestaan. De toepassing en de integratie

van IT in allerlei defensiematerieel is steeds groter geworden, dan wel onmisbaar. Duidelijke voorbeelden hiervan zijn de Reaper en de F-35, die gezien kunnen worden als vliegende 'datastofzuigers' en vol zitten met allerlei technologie.

Defensie wil uiteraard ook doeltreffender kunnen optreden in het militaire domein. De digitalisering zoals in de eerste paragraaf beschreven dient gericht te zijn op de warfighting capabilities die in het kader van hoofdtak 1 relevant zijn.

Hierna komen die warfighting capabilities aan bod, gezien vanuit het Defensie Capability-model. Daarna wordt, op basis van recente conflicten, gekeken welke warfighting capabilities Defensie met behulp van digitalisering moet versterken.

Warfighting capabilities

Een Defensie Capability-model is een handig instrument bij het beschrijven en analyseren wat een organisatie kan of zou moeten kunnen doen. Of nauwkeuriger: business capabilities zijn de vaardigheden of functies die een organisatie heeft of zou moeten hebben om haar doelen te bereiken. Een business capability omvat de mensen, processen, informatie en middelen van de organisatie.⁵ Door de capabilities inzichtelijk te maken, ten opzichte van elkaar te ordenen en te waarderen, kan een organisatie eenvoudiger weloverwogen beslissingen nemen over prioriteiten en daarbij behorende investeringen. Welke capabilities heeft Defensie nodig om klaar te zijn voor het gevecht?

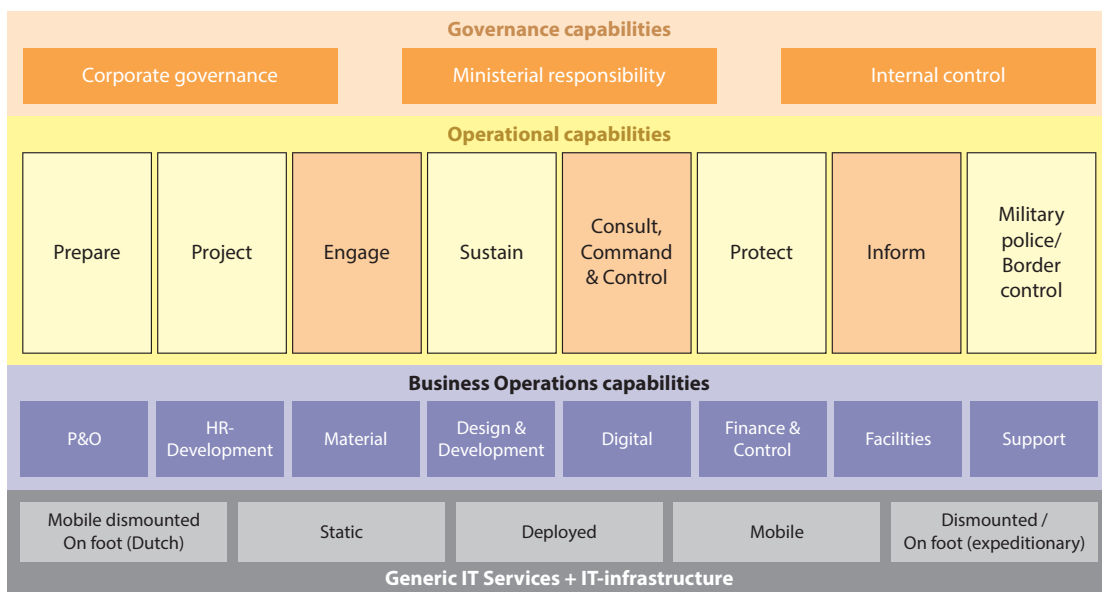
De Nederlandse defensieorganisatie heeft haar business capabilities eveneens in een zogeheten

2 Warfighting capability: een militaire functie die een defensieorganisatie nodig heeft in het gevecht.

3 Zie voor meer informatie over de Enigma-codeermachine: [https://nl.wikipedia.org/wiki/Enigma_\(codeermachine\)](https://nl.wikipedia.org/wiki/Enigma_(codeermachine)).

4 Beleidsvisie Informatiegestuurd Optreden. Sneller, slimmer, sterker (Den Haag, ministerie van Defensie, 4 juli 2023).

5 TOGAF Business Capabilities Guide V2. Zie: https://pubs.opengroup.org/togaf-standard/business-architecture/business-capabilities.html?utm_source=chatgpt.com.



Figuur 1 Het Defensie capability-model

capability model geplaatst, waarbij als basis gebruik is gemaakt van het capability model van de NAVO. In het model wordt een onderscheid gemaakt in besturende, bedrijfsvoerings- en operationele capabilities (zie figuur 1). De operationele capabilities zijn functies die specifiek zijn voor de defensieorganisatie. De operationele capabilities behelzen functies, zoals 'Prepare' en 'Consult, Command & Control'. De eerste functie omvat onder andere de personele- en materiële gereedstelling, terwijl onder de tweede de commandovoering is terug te vinden. Dus als het om warfighting capabilities gaat, dan gaat het over de operationele capabilities van Defensie.

Digitalisering van de warfighting capabilities

Door de teruglopende defensiebegrotingen vanaf 2011 is er sinds die tijd ook structureel te weinig geïnvesteerd in IT. Daardoor kon het IT-landschap niet meegroeien met haar tijd en bleef de digitalisering van de warfighting capabilities achter. Vanaf 2015 zijn er wel investeringen gedaan in een aantal grote programma's om de

achterstand in te halen,⁶ maar grote programma's worden meestal niet gekenmerkt door snelle resultaten.

In 2025 heeft de defensieorganisatie een herijking gedaan van haar IT-portfolio om meer focus aan te brengen in de veelheid van projecten. Met deze herijking richt Defensie het realisatievermogen op de meest essentiële warfighting capabilities. Deze ingreep zal ervoor zorgen dat er meer water uit de IT-kraan komt. Voor deze herijking is op basis van het capability model gekeken naar de capabilities die vanuit digitalisering prioriteit zouden moeten krijgen in het kader van het uitvoeren van hoofdtak 1. Daarnaast is gekeken welke van deze capabilities nog onvoldoende of geen IT-ondersteuning hebben gehad. Hierbij kan gedacht worden aan het op orde krijgen van de internationale interoperabiliteit via de FMN-standaarden⁷ of het versterken van de *situational awareness* en *situational understanding*. Uit die analyse komt naar voren dat er nog over een breed gebied van capabilities geïnvesteerd moet worden. Door die noodzaak aan investeringen in digitalisering blijft het risico dat Defensie te weinig snelheid maakt. Om in het gevecht echt het verschil te maken, is een aanscherping van de prioriteiten

⁶ Ministerie van Defensie 2 H Definitief v1.0.

⁷ What is the NATO Warfighting Capstone Concept? Zie: <https://www.act.nato.int/activities/federated-mission-networking/>.

wenselijk. Hierna zoomt dit artikel daarom eerst in op de digitalisering zoals deze is toegepast in recente conflicten. De praktijk geeft dan mogelijk extra richting aan welke warfighting capabilities het belangrijkst zijn om te versterken.

Digitalisering in recente conflicten

Als het gaat om warfighting capabilities dan is het interessant om te bekijken hoe digitalisering in een aantal recente gewapende conflicten is ingezet. Zowel in de Oekraïne-oorlog als ook in het Midden-Oosten heeft digitalisering op een aantal terreinen een vlucht genomen. Deze zijn te groeperen naar vier trends.

1 Offensieve cyberoorlogvoering

Bij cyberoorlogvoering gaat het om het verstoren van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Oftewel, offensieve cyberoorlogsvoering is gericht op het beïnvloeden, verstoren of vernietigen van informatie en informatiesystemen van tegenstanders. Deze operaties kunnen variëren van het verzamelen van inlichtingen tot het uitvoeren van aanvallen die fysieke effecten hebben, zoals het uitschakelen van kritieke infrastructuur.⁸ Een concreet voorbeeld hiervan is het door de Verenigde Staten uitschakelen van de stroom in Venezuela bij het ontvoeren van president Maduro.

Rusland voerde, ruim voor de inval in 2022, al digitale aanvallen uit op het elektriciteitsnetwerk en het fiscale systeem van Oekraïne in respectievelijk 2015-2016 en 2017.⁹ Ook in het conflict tussen Israël en Hamas heeft allerlei cyberoorlogvoering plaats gevonden, zoals de DDos-aanvallen (Distributed Denial-of-Service) van Hamas op Israëlische organisaties.¹⁰ Kijkend naar het capability model, komt offensieve cyberoorlogvoering terug bij veel van de operationele capabilities waar de nadruk ligt op Engage en Inform. Het kan zorgen voor een effect in het fysieke, virtuele of het cognitieve domein.¹¹

2 Intel-to-shooter

Om de vijand succesvol te kunnen aanvallen moet het tijdsverloop tussen doeldetectie en 'wapen op doel' zo kort mogelijk zijn. Inlichtingen dienen snel en efficiënt gebruikt te worden om een doelwit te lokaliseren. Dit kunnen vijandelijke posities, militaire activiteit of bepaalde grondbewegingen zijn die via middelen zoals drones, radar, satellieten of menselijke waarnemingen worden opgevangen.^{12,13} De inlichtingen dienen real-time verwerkt en gedeeld te worden met de shooter: van de gevechtsvlieger tot aan de drone-operator. De oorlog in Oekraïne laat dagelijks het belang van het concept *intel-to-shooter* zien, waarbij op allerlei manieren doelinformatie wordt vergaard en verwerkt, zowel op tactisch als op strategisch niveau.

Innovatieve ontwikkelingen op het gebied van C4ISR (Command, Control, Communication & Computers, Intelligence, Surveillance en Reconnaissance) zorgen ervoor dat informatie en aanvals- en verdedigingsopdrachten vrijwel direct worden gedeeld met de juiste eenheden. Naast deze (*near*) *real-time* samenwerking is nauwkeurigheid bepalend voor het succesvol onder vuur nemen van doelen of juist het ontwijken van vijandelijk vuur. Met deze ontwikkeling worden vooral de capabilities Engage, Consult, Command & Control en Inform versterkt.

Innovatieve ontwikkelingen op het gebied van C4ISR (Command, Control, Communication & Computers, Intelligence, Surveillance en Reconnaissance) zorgen ervoor dat informatie en aanvals- en verdedigingsopdrachten vrijwel direct worden gedeeld met de juiste eenheden. Naast deze (*near*) *real-time* samenwerking is nauwkeurigheid bepalend voor het succesvol onder vuur nemen van doelen of juist het ontwijken van vijandelijk vuur. Met deze ontwikkeling worden vooral de capabilities Engage, Consult, Command & Control en Inform versterkt.

3. Situational awareness en situational understanding

In meerdere recente conflicten wordt geprobeerd om informatie uit allerlei publieke en private bronnen te verzamelen en te combineren om zo te zorgen voor *situational awareness* en *situational*

8 P.A.L. Ducheine, 'Je hoeft geen zwaard en schild te dragen om ridder te zijn', *Militaire Spectator* 185 (2016) (3) 123-135.

9 K. Arnold, P. Pijpers en P. Schrijver, 'Assessing the Dogs of Cyberwar. Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War', in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024) 231-256.

10 Omer Yoachimik en Jorge Pacheco, 'Cyber attacks in the Israel-Hamas War' (23 oktober 2023). Zie: https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/?utm_source=chatgpt.com/.

11 H. van Beek en S. Rietjens, 'Open-Source Intelligence in the Russia-Ukraine War' in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024).

12 L. Peperkamp en P. Bolder, 'The Space Domain and the Russia-Ukraine War', in: Maarten Rothman e.a. (red.), *Reflections on the Russia-Ukraine War* (Leiden, Leiden University Press, 2024).

13 Delta (situational awareness system). Zie: [https://en.wikipedia.org/wiki/Delta_\(situational_awareness_system\)](https://en.wikipedia.org/wiki/Delta_(situational_awareness_system)).



Een Oekraïense drone-operator monteert een Starlink-communicatiesysteem. Oekraïense eenheden passen hun drones real-time aan aan veranderende electronic warfare-omstandigheden op het gevechtveld

understanding. Deze wordt vervolgens gebruikt om tot een Common Operational Picture te komen en de strategie daarop aan te passen. Oekraïne heeft met zijn Delta-systeem zijn situational awareness vergroot en heeft deze gekoppeld aan zijn Battlefield Management Systeem. Deze trend kan het best gezien worden als wat bij Defensie Informatiegestuurd Optreden wordt genoemd en raakt in de kern de capabilities Consult, Command & Control en Inform.

4 Drones en (semi-)autonome systemen

De toepassing van (semi-)autonome systemen bij gewapende conflicten is niet meer weg te denken. Voorbeelden van militaire (semi-)autonome systemen die we op het slagveld van Oekraïne tegenkomen zijn bewapende drones (UAV's), robotica voor mijndetectie en opruiming, zelfrijdende en -varende wapendragers en verdedigingssystemen die zelfstandig detecteren en onderscheppen. De technologie achter deze systemen heeft een grote vlucht genomen, waarbij de effectiviteit door de introductie van AI aanzienlijk is verbeterd. Tegenwoordig wordt het concept van *human-in-the-loop* steeds meer losgelaten en nemen de systemen autonoom

beslissingen zoals het identificeren van vijandelijke doelen of het afvuren van wapens. Vanuit de recente conflicten hebben Israël en ook Oekraïne en Rusland aanzienlijke stappen gezet in de ontwikkeling en inzet van autonome en onbemande systemen. Er is op dit moment nog geen publiek beschikbare informatie die bevestigt dat deze landen gevechten uitvoeren met bijna uitsluitend autonome systemen. De integratie van deze technologieën lijkt momenteel vooral complementair te zijn aan traditionele militaire operaties. De inzet van (semi-)autonome systemen richt zich op de Engage- capability.

Delta

De vier bovenstaande trends laten zien dat digitalisering vooral effect heeft op drie warfighting capabilities: Engage, Consult, Command & Control en Inform, zoals die in figuur 1 terug zijn te vinden. Als Defensie haar warfighting capabilities wil versterken met digitalisering dan zouden deze drie capabilities in ieder geval aandacht moeten krijgen. Daarbij is het interessant om te zien dat de Inform-capability een belangrijke rol speelt ter ondersteuning van de andere twee. Want zonder

informatie – en daarmee de ondersteuning van digitalisering – is geen enkele capability goed uit te voeren. Om dit concreet te maken kan het Delta-systeem uit Oekraïne als voorbeeld gelden. Delta is zowel een situational awareness- als een Battle Management System dat door de Oekraïense Defensie ontwikkeld is. De kracht van het systeem is dat het uit een grote diversiteit aan bronnen informatie verzamelt, zoals satellietbeelden, drones, inlichtingen en geo-informatie. Delta wordt gebruikt voor het plannen van operaties, coördinatie en informatievoorziening.¹¹ Met het Delta-systeem heeft Oekraïne daarmee niet alleen zijn Inform-capability versterkt, maar ook de Consult, Command & Control en Engage-capabilities. Deze betere informatiepositie is een van de redenen waarom Oekraïne nog steeds standhoudt tegen een kwantitatief veel grotere tegenstander.

Conclusies en vervolg

De wereld van oorlogvoering is aan het veranderen. De digitalisering zorgt er voor dat het

gevecht andere vormen aanneemt. Om Defensie daarop voor te bereiden is in dit artikel gekeken naar hoe de Nederlandse warfighting capabilities kunnen worden versterkt met digitalisering. Recente conflicten – en de oorlog in Oekraïne in het bijzonder – tonen aan dat er drie capabilities zijn die Defensie met digitalisering kan versterken: Engage, Consult, Command & Control en Inform. Op de juiste manier ingezet kan digitalisering het verschil maken in het gevecht.

Als Defensie hierop wil versnellen zal de organisatie moeten transformeren naar andere manieren van voortbrenging en levering van IT. De Digitale Transformatie Strategie, en het multi-modaal werken daarbinnen, gaat zorgen voor die versnelling. In ieder geval luidt de conclusie dat Defensie met urgentie de digitalisering zal moeten oppakken als zij in de afschrikking en in een gewapend conflict het verschil wil maken. Hierbij is het werken met capabilities het vertrekpunt. De uiteindelijke winst van de digitale transformatie is immers een grotere gevechtskracht. ■



FOTO ANP/AP: SERGEJ STOEPINSKI

Zonder informatie – en daarmee de ondersteuning van digitalisering – is geen enkele capability goed uit te voeren. Om dit concreet te maken kan Defensie het Delta-systeem uit Oekraïne als voorbeeld nemen

Waarom Rusland ontregelt, en wat dit van ons vraagt

Luitenant-generaal mr. J.W. Maas MMAS*

Rusland verandert zijn methodes sneller dan wij onze aannames herzien. Het gat dat daardoor ontstaat is onderdeel van de dreiging geworden. Niet als bijkomend risico, maar als het centrale risico. De vraag is dan niet langer of we dit gat zien. We zien het, maar de vraag is wat dit betekent voor de manier waarop wij onze militaire formaties inrichten en laten optreden. Naar mijn overtuiging verdienen negen verschuivingen prioriteit boven alle andere. En ze houden pas echt stand als ze niet los van elkaar staan, maar door één en dezelfde logica worden gedragen.

Er is een economisch feit dat we te weinig hardop uitspreken: de Russische economie is, ondanks twee decennia groei, niet groter dan die van de Benelux of Italië. Toch is het de sleutel tot bijna alles wat Rusland doet. Rusland is geen

wereldmacht in wording en ook geen supermogendheid. Het is een middelgrote macht met een groot kernwapenarsenaal en een nog grotere ambitie. Rob de Wijk noemt Rusland in *De nieuwe wereldorde* dan ook niet de strateeg. Dat predicaat

Militaire parade in Moskou op 9 mei 2026. Rusland is geen supermogendheid en grijpt naar ontregeling als een weg naar relevantie





FOTO ANPICTURE ALLIANCE, HENDRIK SCHMIDT

Antonov-vliegtuigen op de luchthaven van Leipzig voor transporten naar Oekraïne. Duitsland heeft Rusland formeel beschuldigd van een mislukte aanslag op de toestellen in augustus en enkele sancties tegen Moskou ingesteld

reserveert hij voor China, dat welbewust decennia vooruitdenkt. Rusland noemt hij de ontregelaar.¹ Dat onderscheid is scherp en het is precies waar onze eigen aannames misgaan.

Een land dat structureel niet de economische diepte heeft om via opbouw een rol van betekenis te claimen, heeft maar één andere weg naar relevantie. En dat is ervoor zorgen dat niemand om hem heen kan. Niet door overtuigingskracht en niet door welvaart, maar door onvoorspelbaarheid tot instrument te maken. De Krim. De inmenging in westerse verkiezingen. De beschadigde kabels in de Baltische Zee. De branden in Poolse magazijnen en de aanslagen op Poolse spoorwegen. En het bewerken van Russischtalige minderheden in de Baltische staten met narratieven over discriminatie en 'bescherming van landgenoten'. Dit zijn geen losse incidenten meer. Dit is een bewust opgezette strategie. Het doel is niet één beslissende slag, maar een permanent geopolitiek instrumentarium dat naar believen kan worden op- en afgeschaald. Precies genoeg om ons voortdurend te dwingen rekening te houden met Moskou, maar nooit genoeg om een ondubbelzinnig

antwoord van de NAVO uit te lokken. Dat is een precisie-instrument en geen bot wapen. Het werkt juist omdat het onder onze reactiedrempel blijft.

Dit is geen nieuwe Russische uitvinding. De Sovjet-Unie werkte al decennia met actieve maatregelen, desinformatiecampagnes en gerichte destabilisatie van bondgenootschappen. Nieuw zijn de schaal en de snelheid. Digitale netwerken, sociale media en de verwevenheid van onze infrastructuur bieden Moskou mogelijkheden die in de Koude Oorlog nog niet bestonden. Een kabel doorknippen kost weinig. De economische en psychologische schade die daarmee wordt aangericht, staat niet in verhouding tot die kosten. Precies die verhouding maakt ontregeling voor een middelgrote macht met beperkte middelen zo aantrekkelijk.

* Luitenant-generaal Jan-Willem Maas is Commandant van het Defensie Ondersteuningscommando (DOSCO). Dit artikel is op persoonlijke titel geschreven.

¹ Rob de Wijk, *De nieuwe wereldorde. Hoe China sluipenderwijs de macht overneemt* (Amsterdam, De Arbeiderspers, 2019).



Hedgehog 2025 liet pijnlijk zien dat onze formaties bewogen volgens de aannames van een wereld die niet meer bestaat FOTO MINISTERIE VAN DEFENSIE ESTLAND

Er schuilt ook een boodschap in voor onszelf. Wij zijn geneigd macht af te meten aan de omvang van onze economie, onze bevolking en de hoogte van ons defensiebudget. Rusland, maar ook Oekraïne en de Houthi's, laten echter zien dat een kleinere macht met de juiste methode grote schade kan aanrichten zonder ooit een conventioneel conflict te hoeven winnen. Dat is een ongemakkelijke les. Ze ondermijnt de geruststellende gedachte dat wij, met onze grotere gezamenlijke economie, per definitie de sterkere partij zijn. Op het niveau van ontregeling is die rekensom echter niet relevant.

Een andere logica dan de onze

Dit is een fundamenteel andere logica dan die waarop onze militaire eenheden zijn gebouwd. Onze formaties zijn opgeleid en ingericht om

een aanval te herkennen, te lokaliseren en te beantwoorden. Wij denken in duidelijke besispunten. Een grens die wordt overschreden. Een colonne die oprukt. Een moment waarop de wereld het eens wordt dat er iets gebeurt. Ontregeling biedt dat moment nooit. Het is er juist op ontworpen om nooit duidelijkheid te bieden. Moskou opereert bewust in de ruimte onder onze drempels, wetende dat wij drempels nodig hebben om te mogen en kunnen handelen. Elke actie is net klein genoeg om geen Artikel 5-discussie te forceren, en net groot genoeg om effect te hebben. Dat is geen zwakte van Rusland. Dat is de kern van de strategie.

Onze eigen structuren versterken dit probleem. Besluitvorming binnen de NAVO vraagt consensus. Consensus vraagt tijd. Tijd is precies wat een ontregelaar nodig heeft om zijn volgende stap te zetten voordat wij de vorige hebben afgerond. Zolang ons antwoord gekoppeld blijft aan een

proces van duidelijke beslispunten en eenduidige dreigingen, blijft elke kleine, ambigue actie van Moskou effectief. Niet omdat wij zwak zijn, maar omdat onze eigen procedures de tegenstander de tijd geven die hij nodig heeft.

Waarom wij naar oude antwoorden grijpen

Martijn Kitzen en Tim Sweijs beschrijven in *De oorlog van morgen* waarom wij zo moeizaam reageren op deze verandering.² Hun observatie is niet dat wij de trends niet zien. Drone-zwermen aan de randen van Europa. Kunstmatige intelligentie die militaire taken overneemt. Desinformatie en sabotage van fysieke infrastructuur als vast onderdeel van het geweldsspectrum. Wij zien dit allemaal. Hun observatie is dat westerse krijgsmachten, geconfronteerd met die verandering, keer op keer teruggrijpen naar vertrouwde oplossingen. Niet uit onwil, maar omdat vertrouwde oplossingen simpelweg makkelijker te begroten, te trainen en te verantwoorden zijn in plaats van een fundamenteel andere manier van denken over wat oorlog is geworden toe te passen. Een nieuw wapensysteem past in een bestaand verwervingstraject. Een nieuwe manier van denken past nergens in.

Precies die reflex, een nieuw probleem beantwoorden met een oud antwoord, legde de NAVO-oefening Hedgehog 2025 in Estland pijnlijk bloot. Tijdens die oefening, met ongeveer zestienduizend militairen uit twaalf NAVO-landen, schakelde een team van ongeveer tien Oekraïense drone-operators met dertig drones binnen enkele uren twee bataljons uit.³ Niet omdat onze mensen tekortschoten, maar omdat onze formaties nog bewogen volgens de aannames van een wereld die niet meer bestaat. Namelijk die van grote colonnes, zichtbare commandoposten en geconcentreerde troepenformaties.

Dat laatste is misschien wel het meest ontnuchterende element. We wisten van drones. We hadden erover geschreven, erover gesproken en erop geoefend. En toch bewogen onze eenheden zich alsof de lucht boven hen nog steeds ons

exclusieve domein was. Kennis van een dreiging én gedrag dat op die dreiging is aangepast, blijken twee heel verschillende dingen.

Een collectieve keuze om niet voorbereid te zijn

Kitzen legt in *De terugkeer van oorlog* uit hoe we in die positie terecht zijn gekomen.⁴ Zijn punt is niet primair tactisch, maar mentaal. Decennia lang liet Europa het fenomeen oorlog bewust uit zijn aandacht verdwijnen. Schuilkelders gingen dicht, de dienstplicht werd opgeschort en er werd fors bezuinigd op de krijgsmacht. Dit gebeurde in de overtuiging dat oorlog iets was wat wij als continent ontgroeid waren, en dat het hooguit een kwestie van tijd was voordat andere landen ons voorbeeld zouden volgen. Andere landen en extremistische groeperingen deden precies daar hun voordeel mee. Onze afwezigheid van een dreigingsbeeld werd hun kans.

Dit is geen technisch verhaal over drones of algoritmes. Het is een verhaal over een collectieve keuze om niet meer voorbereid te zijn. Die keuze verklaart minstens zoveel van onze huidige achterstand als welke technologische verrassing dan ook. Een technologische achterstand kun je inhalen met geld en tijd. Een mentale achterstand vraagt de bereidheid om toe te geven dat een generatie lang de verkeerde aanname centraal stond.

Drie boeken, drie lagen met dezelfde diagnose

De Wijk verklaart waarom Rusland ontregelt. Kitzen en Sweijs verklaren waarom wij, eenmaal geconfronteerd met die ontregeling, hardnekkig naar oude antwoorden grijpen. Kitzen verklaart,

2 Martijn Kitzen en Tim Sweijs, *De oorlog van morgen* (Amsterdam, Balans, 2025).

3 Jillian Kay Melchior, 'Ukrainian Troops Defeated Opponent With Drones at 2025 NATO Exercise', *The Wall Street Journal*, 13 februari 2026; zie ook de Nederlandse berichtgeving over NAVO-oefening Hedgehog 2025 in Estland.

4 Martijn Kitzen, *De terugkeer van oorlog. Pleidooi voor de verdediging van vrede* (Amsterdam, Cossee, 2026).

in zijn recentste boek, waarom we onszelf in de uitgangspositie hebben gebracht waarin we die oude antwoorden nog steeds als vanzelfsprekend beschouwen.

Samen leveren ze een ongemakkelijke, maar heldere conclusie op. De tegenstander verandert zijn methodes sneller dan wij onze aannames herzien. Het gat dat daardoor ontstaat is onderdeel van de dreiging geworden. Niet als bijkomend risico, maar als het centrale risico.

De vraag is dan niet langer of we dit gat zien. We zien het, maar de vraag is wat dit betekent voor de manier waarop wij onze militaire formaties inrichten en laten optreden. Naar mijn overtuiging verdienen negen verschuivingen prioriteit boven alle andere. En ze houden pas echt stand als ze niet los van elkaar staan, maar door één en dezelfde logica worden gedragen.

Negen benodigde verschuivingen

1. De bevolking als slagveld

Waar Rusland Russischtalige gemeenschappen in bondgenootschappelijk gebied bewerkt met narratieven van verwaarlozing en dreiging, kunnen we daar in louter militaire termen niets tegen uitrichten. Deze dreiging tegen de bevolking vraagt om vroege herkenning van desinformatiepatronen, om samenwerking met lokale bestuurders en gemeenschapsleiders, en om zichtbare, geloofwaardige aanwezigheid juist in die regio's. Niet pas nadat de narratieven al wortel hebben geschoten. Een militaire formatie die deze dimensie alleen aan inlichtingen-diensten of aan hoofdsteden overlaat, mist de helft van het slagveld waarop de tegenstander

daadwerkelijk actief is. Dit is geen taak erbij. Dit is een kerntaak die we nog onvoldoende als zodanig herkennen.

In de Baltische staten is dit geen theorie. Russischtalige gemeenschappen krijgen dagelijks een narratief voorgeschoteld waarin de eigen staat hen verwaarloost of bedreigt, en waarin Rusland zich opwerpt als beschermer. Militaire aanwezigheid alleen weerlegt dat narratief niet. Zichtbare, geloofwaardige aanwezigheid die samengaat met investering in de lokale gemeenschap, wel. De strijd om het narratief is net zo bepalend als de strijd om het terrein, maar het militaire gedrag dat daarbij hoort is structureel anders. Dat vereist meer aanwezigheid buiten de kazernes, meer samenwerking met lokale instanties en een inlichtingenfunctie die vroegtijdig patronen herkent in plaats van pas reageert nadat het narratief al is ingesleten.

2. Structurele samenwerking met én in de samenleving

Dit is de verschuiving die de andere verschuivingen pas echt laat werken. Niet als los liaison-element naast het militaire optreden, maar als één geïntegreerd geheel.

Verspreide eenheden hebben civiele infrastructuur en lokale informatie nodig om effectief te zijn. Snelle reactiecapaciteit tegen sabotage is zonder civiele meldketens en samenwerking kansloos. Het herkennen van narratieven in kwetsbare gemeenschappen lukt alleen met lokaal bestuur, onderwijs en media. Innovatie en nieuwe technologie heeft evengoed civiele kennis en industrie nodig als militaire expertise. En structureel voortzettingsvermogen, denk aan reserves, industrie en civiele weerbaarheid, is per definitie een civiel-militair vraagstuk en geen zuiver militair vraagstuk.

3. Onze eigen drempels serieus nemen

Wat is nu wél en wat is geen aanval, voordat Artikel 5 in beeld komt? Deze drempel wordt door de tegenstander even zorgvuldig bestudeerd als door onszelf. Zolang die drempel vaag blijft, blijft ontregeling voor Rusland de goedkoopste vorm van invloed die het land zich kan veroorloven.

Door onze eigen onduidelijkheid dragen we bij

De strijd om het narratief is net zo bepalend als de strijd om het terrein



Oefening in Litouwen. In de Baltische staten weerlegt alleen militaire aanwezigheid het Russische narratief niet

FOTO MCD

aan onze eigen dreiging. Een scherper gedefinieerde drempel, ook als die bewust hoog ligt voor bepaalde categorieën incidenten, ontnemt de tegenstander een deel van de ruimte waarin ontregeling nu zo goed gedijt.

4. Hyperadaptiviteit toepassen

Hiermee doel ik op het vermogen om nieuwe technologie, zoals drones, AI-ondersteunde besluitvorming en softwaregedreven elektronische oorlogvoering niet eenmalig in te voeren maar continu te herzien. Met als enige doel het initiatief zo snel mogelijk te grijpen en, belangrijker nog, vast te houden.

Tegen een tegenstander die zijn methodes sneller verandert dan onze verwervingstrajecten toestaan is de organisatie die het snelst leert en aanpast in het voordeel, ongeacht wie op enig moment het beste materieel heeft. Dat vraagt om experimenteerruimte, korte innovatiecycli en een cultuur waarin falen tijdens het testen goedkoper is dan vasthouden aan wat gisteren werkte. Dit is een organisatieprincipe, geen technologieprogramma. Het raakt aan hoe we besluiten nemen, niet alleen aan wat we kopen.

De oorlog in Oekraïne laat zien hoe snel dit kan gaan als de organisatie het toelaat. Drone-ontwerpen veranderen daar in dagen, niet in jaren. Software wordt in het veld aangepast op basis van wat die week wel en niet werkt. Onze eigen standaard verwervingstrajecten, met lange programma's van eisen en langlopende contracten, zijn onvoldoende ontworpen voor dat tempo. Dat betekent niet dat we elk verwervingsproces moeten afschaffen. Het betekent wel dat er, naast de grote, langlopende programma's, ruimte moet zijn voor een kleinere en snellere aanpak. Een aanpak met beperkte budgetten, korte doorlooptijden en de bevoegdheid om op eenheidsniveau te experimenteren zonder voor elke aanpassing terug te hoeven naar Den Haag.

We moeten er bovendien voor waken om alleen te leren van wat nu al werkt in Oekraïne. Wat als counter-drone maatregelen op afzienbare termijn zo effectief worden dat drones veel minder bruikbaar zijn? We moeten innovatie zo inrichten dat we ook dan snel het initiatief kunnen hernemen en behouden, zodat we Rusland blijvend met dilemma's kunnen

confronteren, ook op tactisch en operationeel niveau. Onze militaire capaciteiten moeten dus niet streven naar een ontwikkeling van versie 1.0 naar 1.3, maar van 1.0 naar 3.0.

5. Van geconcentreerde naar verspreide slagkracht

Als ontregeling wint bij onvoorspelbaarheid, dan winnen wijzelf bij het onvoorspelbaar maken van ons eigen optreden. Grote, zichtbare formaties vormen voor een drone en voor een sabotagenetwerk hetzelfde soort doelwit. Ze zijn makkelijk te vinden, makkelijk te volgen en makkelijk te raken.

Kleinere, verspreide eenheden zijn moeilijker op te sporen en moeilijker in één klap uit te

schakelen. Dit vraagt om een andere balans tussen massa en spreiding dan waarop onze huidige formaties zijn gebouwd. Niet minder slagkracht, maar slagkracht die zich anders presenteert aan een tegenstander die juist op herkenbare patronen jaagt.

Naast de Israëliërs en de Amerikanen in recente conflicten, hebben ook wij in de oefening Hedgehog 2025 deze les op de hardst mogelijke manier geleerd. Dezelfde twee bataljons die eerder al genoemd werden, vormden juist door hun concentratie en herkenbaarheid het doelwit dat dertig drones konden uitschakelen. Diezelfde slagkracht, verspreid over kleinere, mobiele eenheden met eigen sensoren, electronic-warfarecapaciteiten en eigen luchtverdediging,



was voor diezelfde drones een fundamenteel ander probleem geweest. Spreiding kost coördinatie en coördinatie kost oefening. Maar het alternatief, vasthouden aan concentratie omdat dat historisch effectiever was tegen een conventionele tegenstander, is precies de reflex die Kitzen en Sweijs beschrijven.

6. Reactiecapaciteit loskoppelen van zware gevechtscapaciteiten

Een militaire formatie die alleen kan reageren via zijn zwaarste middelen, reageert per definitie te laat en mogelijk disproportioneel op een tegenstander die welbewust klein en *deniable* opereert. Je stuurt geen brigade af op een gesaboteerde spoorlijn.

Er is een aparte, snel inzetbare capaciteit nodig,

die samen met civiele capaciteiten kan handelen binnen uren, niet dagen. Specifiek gericht op sabotage en hybride activiteiten, met een eigen afgestemd mandaat en een eigen besluitvormingslijn. Zonder dat mandaat loopt elke reactie vast in dezelfde procedures die voor een klassieke aanval zijn ontworpen, en die voor dit soort incidenten simpelweg te traag zijn.

Denk aan de eerder genoemde incidenten in Polen en de Baltische Zee. In beide gevallen duurde het dagen voordat duidelijk was wie verantwoordelijk was, en nog langer voordat een reactie volgde. Tegen die tijd had de tegenstander zijn punt, namelijk onvoorspelbaarheid en straffeloosheid, in één actie allang gemaakt. Een snelle reactiecapaciteit hoeft niet elk incident

Kleinere, verspreide eenheden zijn moeilijker op te sporen en moeilijker in één klap uit te schakelen. Dit vraagt om een andere balans tussen massa en spreiding dan waarop onze huidige formaties zijn gebouwd



militair te beantwoorden. Ze moet wel razendsnel kunnen vaststellen wat er is gebeurd, wie erbij betrokken was, en welke opties er zijn, zodat politieke besluitvorming niet vertraagd wordt door een gebrek aan feiten.

7. Logistiek als een noodzaak, niet als vanzelfsprekendheid

Een tegenstander die uit is op ontregeling, slaat toe waar de schade het grootst is voor de laagste kosten. Dat is zelden tegen een gevechtscapaciteit. Vaker is dat tegen een depot, een spoorlijn of een internetkabel. De voorbeelden zijn al in het nieuws geweest.

Onze planning gaat nog te vaak uit van logistiek als een gegeven, iets dat er gewoon is. Die aanname was al niet juist, maar klopt nu helemaal niet meer. Logistieke knooppunten verdienen dezelfde beveiligingslogica als operationele hoofdkwartieren, omdat de tegenstander ze inmiddels ook zo behandelt. Dat vraagt niet alleen om logistiek serieuzer te nemen. Het vraagt ook om de durf om bestaande

standaarden los te laten. Niet elke norm die in vredetijd of tijdens stabilisatiemissies werkte, is haalbaar in een langdurig, gewapend conflict met Rusland. Vasthouden aan een norm die niet meer haalbaar is, kost meer dan hij oplevert. Hij wekt een schijnzekerheid die op het moment zelf instort.

Neem de medische zorgketen. Onze normen voor zorg binnen een vastgestelde tijd gaan uit van een beheersbare context en een functionerende afvoerketen. Onder de dreiging van drones, raketten, verstoorde verbindingen en verspreide formaties is die keten niet meer gegarandeerd te sluiten. Dit gaat niet over het verlagen van onze ambitie voor gewonden. Het gaat over eerlijk erkennen dat een enkele, centrale keten dat niet meer waarborgt. We moeten dus investeren in een systeem dat die gebreken kan opvangen om de overlevingskansen van onze militairen zo goed mogelijk te waarborgen. Vasthouden aan de oude norm zonder die investering legt een onrealistische druk op eenheden en op de zorgverleners zelf en

Onze planning gaat nog te vaak uit van logistiek als een gegeven, iets dat er gewoon is. Die aanname was al niet juist, maar klopt nu helemaal niet meer

FOTO MCD



ondermijnt het vertrouwen van onze militairen in het systeem zodra de norm structureel niet wordt gehaald.

Hetzelfde geldt voor onze onderhoudsdoctrine, die nog grotendeels uitgaat van centrale werkplaatsen waar materieel voor reparatie naartoe kan. In een omgeving waarin juist die knooppunten doelwit zijn, is dat een aanname die het conflict zelf al heeft ingehaald. En het geldt voor onze voorraadnormen. De genormeerde *Days of Supply* zijn berekend op een werkende bevoorradingsketen. Dat volstaat niet tegen een tegenstander die bewust op onze bevoorrading aast.

Deze normen loslaten en herbezien is geen bezuiniging en geen kwaliteitsverlies. Het is erkennen dat een norm die niet meer haalbaar is, geen norm meer is, maar een blinde vlek. Ook op dat gebied moeten we logistiek serieuzer nemen.

8. Voortzettingsvermogen herstellen

Een militaire formatie kan nog zo slim worden ingericht, als de gereedheid en de vereiste aanvullingen, de defensie-industriële basis en de maatschappelijke weerbaarheid onvoldoende zijn, mist zij precies het uithoudingsvermogen dat ontregeling het meest test.

Dit voortzettingsvermogen hebben we in de vredesdividend-jaren welbewust afgebouwd. Het is geen tekort dat je in een jaar met geld alleen herstelt. Het vraagt reservecapaciteit, industriële diepte en een samenleving die begrijpt waarom dit nodig is. Ontregeling is per definitie een strategie van de lange adem. Wie daar geen lange adem tegenover zet, verliest uiteindelijk, ook zonder ooit een directe confrontatie te verliezen.

Voorraden, personeelslogistieke ketens, onderhouds capaciteit en de industriële basis om verliezen aan te vullen klinken minder aansprekend dan een nieuw wapensysteem. Ze zijn echter wel bepalend voor de vraag of een militaire formatie een langdurige campagne van kleine, aanhoudende druk kan doorstaan. Rusland rekent er niet op dat wij één klap niet

Voortzettingsvermogen is niet alleen een logistiek vraagstuk, maar ook een vraagstuk van militair, politiek en maatschappelijk volhouden

kunnen incasseren. Het rekent erop dat wij, na een reeks kleine klappen verspreid over jaren, murw raken en zelf de prijs van voortdurende paraatheid te hoog gaan vinden. Voortzettingsvermogen is daarmee niet alleen een logistiek vraagstuk, maar ook een vraagstuk van militair, politiek en maatschappelijk volhouden.

9. Operationeel raamwerk in balans, en altijd multi-domein

Dit is de negende en misschien meest onderbelichte verschuiving. De eerste acht gaan vooral over de nabije operatie en de achtergebiedsoperatie, over kleinere eenheden, snelle reactiecapaciteit, voortzettingsvermogen en bescherming van logistiek. Dat betekent niet dat de klassieke, zware middelen overbodig zijn. Zonder tanks, artillerie en luchtverdediging houdt geen enkele formatie, hoe adaptief ook, stand tegen een grootschalige aanval. En zonder geloofwaardige tegenmacht wordt een ontregelaar een sloper.

Rusland kiest niet toevallig voor ontregeling boven een grootschalig treffen met de NAVO. Dat het land al meer dan vier jaar een grootschalige, conventionele oorlog voert tegen Oekraïne spreekt dat niet tegen. Oekraïne beschikt over een fractie van de gezamenlijke slagkracht van het bondgenootschap, en zelfs die oorlog drukt de Russische economie inmiddels tot aan de grens van wat ze kan dragen. Een



Russische raketten treffen Kyiv op 8 september. Rusland kiest niet toevallig voor ontregeling boven een grootschalig treffen met de NAVO. Dat het land al meer dan vier jaar een grootschalige, conventionele oorlog voert tegen Oekraïne spreekt dat niet tegen

langdurige, conventionele oorlog tegen de NAVO kan Rusland economisch niet dragen. Ontregeling levert tegen de NAVO hetzelfde strategische effect op, maar tegen een fractie van de kosten. Maar dominant betekent niet exclusief. Onze formaties moeten daarom op twee borden tegelijk kunnen schaken. Dat is het bord van aanhoudende, ambigue druk, en het bord van een daadwerkelijk gewapend treffen, mocht ontregeling escaleren.

Voor dat tweede bord is een betere balans nodig binnen het operationeel raamwerk, tussen de achtergebiedsoperatie, de nabij operatie en de diepe operatie. De eerste acht verschuivingen versterken vooral de eerste twee. Dat is onmisbaar, maar niet voldoende. Zodra het tot een treffen komt, is het net zo bepalend dat wij de tegenstander diep in zijn territorium kunnen vinden, volgen en treffen, voordat hij ons eigen gebied bereikt. Dat vraagt om betere inlichtingen, meer sensoren en meer *deep-strike* capaciteiten.

Al deze activiteiten moeten bovendien altijd onderdeel zijn van multi-domeinoperaties, niet als extra laag, maar als voorwaarde. Ontregeling is zelf al multi-domein. Een tegenstander die vrij tussen domeinen beweegt, wordt niet gestopt door een verdediging die slechts in enkele domeinen sterk is. Zonder die integratie blijft elke investering, hoe goed bedoeld ook, een geïsoleerde capaciteit die de tegenstander eenvoudig omzeilt.

Dat is de voorwaarde waaronder de eerste acht verschuivingen standhouden, mocht ontregeling ooit omslaan in iets groters. Maar wie alleen daarop rekt, ziet iets fundamenteels over het hoofd. Een formatie die uitsluitend is ingericht op de oorlog die Rusland zich economisch niet kan permitteren, mist de oorlog die het zich wél kan permitteren. En die het al voert tegen de Baltische staten, tegen Polen, en in mindere mate ook tegen ons.

Wat dit vraagt van ons denken

De negen verschuivingen hierboven zijn geen wensenlijst. Het zijn keuzes die met elkaar samenhangen en die vragen om een andere manier van plannen dan waarop onze huidige militaire organisatie is gebouwd. De klassieke dreigingsanalyse gaat uit van een tegenstander die zich op enig moment onmiskenbaar toont. Ontregeling is ontworpen om dat moment te vermijden.

Wie deze negen verschuivingen apart van elkaar organiseert, verliest precies de snelheid en focus die nodig zijn om het initiatief te pakken en te houden. Wie ze bewust tot één systeem smeedt, over alle domeinen heen en geïntegreerd in een operationeel raamwerk, heeft een reële kans om in deze competitie sneller te zijn dan de ontregelaar zelf. We zullen dus ook middenin en mét de samenleving moeten optrekken.

Dat vraagt niet om meer van hetzelfde, sneller uitgevoerd. Het vraagt om een andere vraag vooraf. Wat doen wij, als de tegenstander er juist voor kiest om nooit dat ene heldere aanvalsmoment te bieden waarop onze hele organisatie is voorbereid? Wie die vraag structureel stelt, bij elke oefening, elke aanschaf en elke reorganisatie, bouwt vanzelf toe naar de negen verschuivingen die hierboven staan.

Dat economische plafond, niet groter dan de Benelux of Italië, verdwijnt ook de komende jaren niet. Het verandert niets aan de dreiging die ervan uitgaat. Het verklaart alleen waarom die dreiging een andere vorm aanneemt dan wij gewend zijn te herkennen. Wie dat onderscheid eenmaal ziet, kan niet meer terug naar het oude denken. En dat is precies waar de opgave voor ons begint. ■

Onze formaties moeten tegelijk kunnen schaken op het bord van aanhoudende, ambigue druk, en het bord van een daadwerkelijk gewapend treffen, mocht ontregeling escaleren



Space weather impacts in the Arctic: where the Sun touches ice

M. Brchnelová PhD and LtCdr A.M. Verheij MA*

Few of us think of space when we hear the term 'weather'. To most of us, weather is a concept tied to our atmosphere that ceases to exist as soon as we rise a few tens of kilometers above the ground. However, while here on the ground, rain of water droplets and wind of air are experienced; in space, our planet faces a rain of highly-energetic particles and a wind of hot plasma escaping the Sun. Even though many of these phenomena remain confined to space, some of them penetrate Earth's magnetic shield and upper atmosphere, triggering disturbances that can be felt all the way down on the ground, and that can impact the functioning of our systems.

* M. Brchnelová PhD is an assistant professor at the Netherlands Defence Academy (NLDA) in Den Helder and represents the Netherlands in the NATO military space weather panel. LtCdr A.M. Verheij is a lecturer-researcher and PhD-candidate at the Netherlands Defence Academy; he was deployed to the Baltic and High North multiple times as a Staff Officer METOC (Meteorologist and Oceanographer) for NATO and the Royal Netherlands Navy.

Northern lights in the Arctic region.
Space weather phenomena like
Aurora Borealis can have impact
on military operations



In this article, the characteristics of these kinds of phenomena are explored and the variety of impacts they can have on our technology will be discussed and illustrated by both historical and recent examples. These range from signal jamming and radio blackouts to sea mine explosions and failure of electrical power grids. Many of these possible impacts are also far more prevalent in the Arctic, creating a potential challenge for us if operations in this region are to be further expanded. This paper will also outline how such risks might be mitigated and how, in time, a deeper understanding of space weather could allow us not only to protect against its effects, but perhaps even to harness them to our advantage.

The Sun, the Earth and the Arctic

When the weather is concerned, rain, wind, clouds, humidity and snow are the first characteristics that come to mind. The term ‘weather’ generally describes the atmospheric conditions that we experience here on Earth and is an important factor to consider in planning many kinds of activities, military operations included. The landing operation in Normandy in June 1944 is a good example in which weather forecasting was a crucial element of the mission’s success.¹ A more recent example is the intervention of the US in Venezuela, which was reportedly delayed by four days due to adverse weather conditions.²

Knowing ‘regular’ weather is, however, not always enough. Over the last decades, our operations have become significantly dependent on a variety of sensors and signals, which are sensitive to environmental circumstances other than just what normal weather typically describes. These include, among others, the

intensity and frequency of the incoming light from the Sun, the signal propagation conditions in the various portions of the atmosphere, the changing magnetic field of the Earth and the presence of highly energetic particles, which may affect the behaviour and health of electrical components onboard spacecraft. The origin of many of these influences is in space, which is also why the term *space weather* is used to describe them collectively.

Space weather can have a wide spectrum of impacts on our systems. For instance, at times, the Sun can generate such intense radio emission that it jams our radio and radar systems, which may include satellite communications and navigation services. Especially now, in an era when signal jamming (and service denial in general) has been a tactic frequently employed by our adversaries, knowing the difference between the natural and man-made causes of these disturbances may be instrumental for decision-making. Further, if the cause of jamming is natural, it is also advantageous to know what to expect in terms of duration and extent of the event.

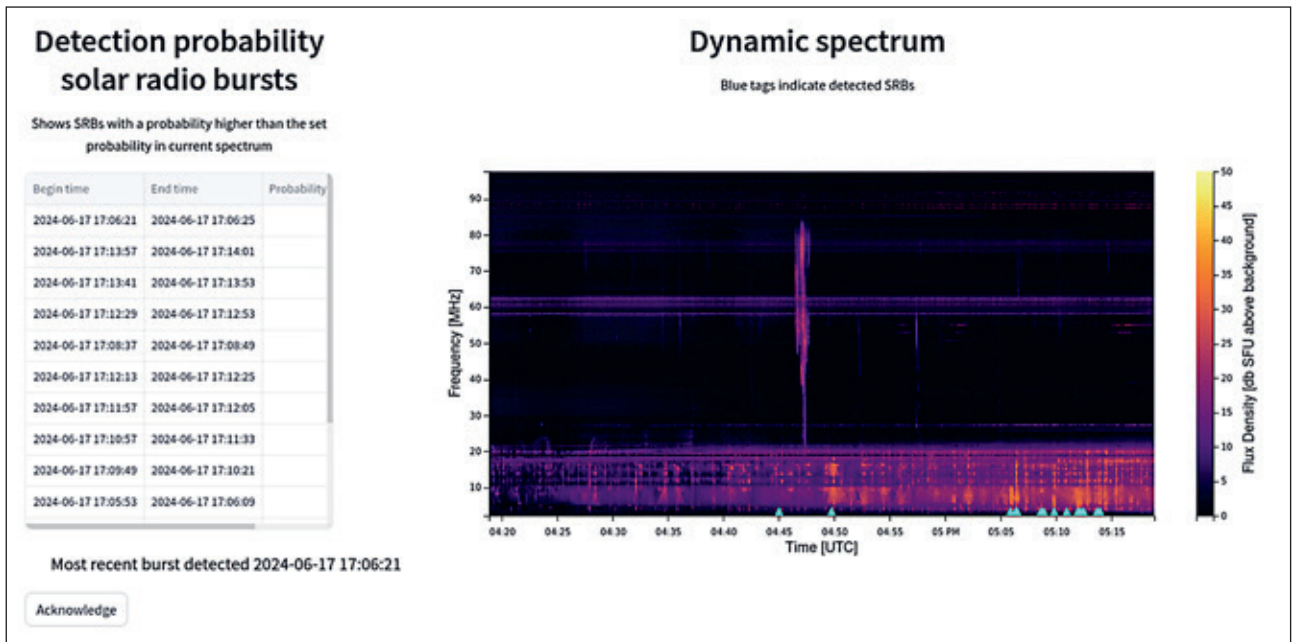
There is also another reason why the interest in space weather has been growing recently. Due to the structure of our magnetic field, it is especially the Arctic that feels many of these effects far more intensely than, for instance, the Netherlands. Now that our focus is partly shifting in the direction of the Arctic, understanding space weather phenomena may thus be especially useful if we want to be able to operate our systems in these regions reliably and accurately.

Cycles of activity

Many of us imagine space as an empty, dark volume in which our Earth orbits and the nature of which barely changes in time. This is, however, hardly the case in reality. Interplanetary space is filled with radiation, highly-energetic particles and magnetic fields that constantly interact with the Earth and, by extension, also with us and our technology. In the vicinity of the Earth, the most important external source of

1 Royal Meteorological Society, ‘How weather forecast made history — the D-Day landings’. See: <https://www.rmets.org/metmatters/how-weather-forecast-made-history-d-day-landings>.

2 Gareth Evans, ‘Spies, drones and blowtorches: How the US captured Maduro’, *BBC*, 4 January 2026. See: <https://www.bbc.com/news/articles/cdred61epg4o>.



Screenshot from the DISTURB system as used by HNLMS Johan de Witt during Exercise Baltops24. Solar radio bursts can cause technical problems for equipment like radar

these particles, radiation and fields is our closest star, the Sun.

Even though humans have been studying the Sun for thousands of years, how certain solar processes operate is still, to this day, a mystery. For instance, the atmosphere of the Sun, which we also call the *corona*, is millions of degrees hot while the solar surface underneath (or, what we at least refer to as ‘surface’) is only a few thousands. The fact that we cannot explain this heating demonstrates that we are still not aware of some of the most fundamental processes that dictate solar activity.

One of the few things that we can predict about solar activity, however, is its regular 11-year-long cycle, during which the periods of high and low activity regularly exchange. The maximum of the current solar cycle took place in 2024,³ and the activity is now steadily decreasing until we reach a minimum in five to six years. While during solar maxima the frequency of strong space weather events is higher, that does not mean that during minima strong events cannot occur. Actually, historically, some of the

strongest space weather events have been seen during the declining phase of solar activity.⁴

Solar radio jamming

In May 1967, the US Ballistic Missile Early Warning System showed signs of jamming.⁵ Given the heightened tensions of the Cold War, it was only natural that the Americans immediately assumed that the Russians were trying to jam the system to start a large-scale attack and were ready to react. The Sun almost triggered World War III.

- 3 SIDC, ‘SC56 maximum in October 2024’. See: <https://www.sidc.be/article/sc25-maximum-october-2024>.
- 4 N.A. Frissell et al, ‘High-frequency communications response to solar activity in September 2017 as observed by amateur radio networks’, *Space Weather* 17 (2019) (1) 118–132. See: <https://doi.org/10.1029/2018SW002008>.
- 5 D.J. Knipp et al, ‘The May 1967 great storm and radio disruption event: Extreme space weather and extraordinary responses’, *Space Weather* 14 (2016) (9) 614–633. See: <http://dx.doi.org/10.1002/2016SW001423>.

One of the symptoms of solar activity are the so-called *solar flares*, eruptions on the solar surface, often resulting in a large release of energy in the form of light. This emission includes a wide spectrum of frequencies, including radio that may interfere with our own signals. Sometimes, associated with these flares, are expulsions of mass and high-energy particles into the interplanetary space. Especially the former, which are also called *coronal mass ejections*, may also be a strong source of radio signals. Collectively, these irregular outbursts of radio from the Sun are termed *solar radio bursts* (SRB's).

During these bursts, the radio intensity of the Sun at certain frequency ranges increases well above normal levels, to the point that our own systems operating at these frequencies become jammed by it if the Sun happens to be in their field of view at the time. Especially systems that have a wide field of view (for instance, radars with a wide coverage) are thus at increased risk. Generally, lower frequencies are affected more often since these are easier to generate during the various physics processes as they require less energy.

While most of the well-known historical radio disruptions came from strong space weather events just like the one in 1967, a strong event is not always needed to create a technical problem. In November 2015, for instance, a medium-intensity solar flare created a radio burst that affected exactly the frequencies of secondary air traffic radars.⁶ As a result, radars in Belgium observed dozens of fake echoes in the direction

of the Sun, obstructing the tracing of real aircraft. In Sweden, the effects were so severe that it prompted the country to close its airspace for more than an hour.⁷

Solar radio bursts sometimes also affect our own maritime operations. That is why the Defence organisation is currently developing the so-called DISTURB system to constantly monitor radio signatures of the Sun.⁸ A demonstration was carried out by the officers of the Royal Netherlands Navy, the Joint Meteorological Group, the German Bundeswehr and MARCOM as a contribution to Baltops24, during which solar radio bursts were also actually recorded.

Naturally, the frequencies affected can also be those corresponding to the GNSS (Global Navigation Satellite System) signals, leading to what may appear as GNSS jamming. The same holds for other satellite services, such as for communication. However, since GNSS frequencies are relatively high (1 to 1.5 GHz), strong GNSS disruptions due to radio bursts are expected to occur only roughly 9 times per solar cycle of 11 years.⁹

Compared to man-made jamming, solar radio bursts usually only last a limited time, typically minutes to tens of minutes. In addition, they are broadband disruptions, meaning that they influence an entire range of frequencies. This is typically not the case for man-made jammers, since jamming requires quite a lot of energy. Most artificial jammers are, thus, limited to a specific frequency channel (or multiple) of the service in use by their adversary.

As mentioned above, for a signal to be jammed by the Sun, the system must 'see' the Sun. For that reason, the Arctic is at a higher likelihood of experiencing such jamming during the day because there, the Sun stays at low elevations, meaning that the radios and radars looking at the horizon and just above it may notice this phenomenon more often. This is the case for Line-of-Sight communications at Earth, SATCOM, surveillance radars and most of the GNSS-signals. Of course, during the polar night, there is no risk of direct solar radio jamming.

6 Christophe Marqué et al, 'Solar radio emission as a disturbance of aeronautical radionavigation', *Journal of Space Weather and Space Climate* 8 (2018) Article A42. See: <https://doi.org/10.1051/swsc/2018029>.

7 AP News, 'Solar storm knocks out flight control systems in Sweden', 4 November 2015. See: <https://apnews.com/article/efd138980b9e473e805221439c71a031>.

8 Netherlands Ministry of Defence, 'Instrument Disturb bepaalt: zon of vijand', 30 May 2024. See: <https://www.defensie.nl/actueel/nieuws/2024/05/30/instrument-disturb-bepaalt-zon-of-vijand>.

9 Xinan Yue et al, 'The effect of solar radio bursts on GNSS signals', in: Natalia Buzulukova (ed.), *Extreme Events in Geospace: Origins, Predictability, and Consequences* (Elsevier, 2018) 541–554.



HF radio generally suffers from space weather events much more than other radio types

PHOTO MCD, BAREND WESTERVELD

Blackouts of long-distance radio

One of the complications of the precarious situation in 1967 was the fact that along with radio disruption at VHF and UHF frequencies, long-distance HF (high-frequency) radio stopped working as well. At the time, since satellite communication services were not yet developed, the HF radio was the only method to communicate with the pilots over long distances efficiently. This means that had aircraft been sent to retaliate the presumed Russian attack, the pilots would have had no means of receiving further orders once underway. There would thus be no way to recall the mission.

Long-distance HF radio operates by refraction of the signal from the ionosphere (a charged layer within our upper atmosphere), meaning that its propagation is directly dependent on the condition of the ionosphere. Since the ionosphere responds strongly to space weather, HF radio generally suffers from space weather events much more than other radio types. The

same holds for over-the-horizon radars that use the same principle and frequencies.

In mid-latitudes, HF radio blackouts generally follow strong solar flares, the high-energy light from which enhances the absorptive layer of the ionosphere where the HF signal becomes lost instead of being allowed to propagate further. Strong solar flares may lead to a complete blackout of all HF frequencies for up to hours in the regions with daylight. These blackouts can be especially problematic since often HF radio is used as a back-up in emergencies as an infrastructure-independent communication method when cell, internet and/or satellite systems fail. In September 2017, for instance, solar activity caused a blackout of HF radio precisely at the time when hurricanes Irma and Jose were causing significant damage to the Caribbean, meaning that unexpectedly, this service could not be used for emergency communication.¹⁰

10 Frissell et al, 'High-Frequency Communications Response to Solar Activity'.

Northern lights can be intense enough to light up the night and take away the (dis)advantage of darkness

In the Arctic, HF radio faces more frequent and long-lasting problems. The region lies in the vicinity of the magnetic pole, which is characterised by open magnetic field lines. The open field lines provide a path for highly energetic particles from space to enter the atmosphere. Just like high-energy light, these particles can enhance the absorptive layer of the ionosphere and lead to the loss of signals. However, compared to the emission of the light, particles generally keep storming in for much longer. As a result, HF radio blackouts in polar regions often last days. In other cases, the precipitation of particles in the region may enhance other layers of the ionosphere (the so-called auroral-E) and improve signal propagation over shorter distances.

Next to these abnormalities due to enhanced absorption in the ionosphere, there is also another mechanism that frequently obstructs the use of HF. As mentioned above, solar flares are sometimes associated with mass ejections from the Sun that may also collide with the Earth and disturb the Earth's magnetic field (though changes in the 'plasma wind' that the Earth faces from the Sun can also happen due to

other phenomena and have the same effect). We feel this disturbance as a change to our Earth's magnetic field – the geomagnetic field – and thus call it a *geomagnetic storm*.

After periods of geomagnetic storms, often the opposite is witnessed than during solar flares, and the ionosphere becomes depleted instead. If the ionosphere is too thin, it does not contain enough electrons to refract the HF signals, and these signals escape to space. This phenomenon also happens more frequently in polar regions and limits the use of higher HF frequencies.

Especially during solar maxima, HF propagation abnormalities due to these various mechanisms are a fairly regular occurrence, especially in the Arctic. It is, therefore, important to take this into account in mission planning, especially if these are to take place in the Arctic and rely on long-distance HF radio. In the Arctic, HF radio may be of special importance as many SATCOM services do not provide sufficient coverage in the region.

Polar lights obstructing versus enabling the view

The fact that the particles from space have an easier way to penetrate into the Earth's atmosphere in the Arctic is also the reason why this region is known for one of the world's most beautiful natural phenomena – the northern lights, or Aurora Borealis. These lights are caused by interaction of the incoming particles with gasses in our atmosphere, and depending on the reacting gas, they display a variety of vibrant colours; from purple, through bright green to red.

However beautiful they are, in especially active conditions, northern lights can be intense enough to light up the night and take away the (dis)advantage of darkness. This was, for instance, the case during the Second World War, when the auroral light in September 1941 allowed the British to carry out a raid on a German supply base in the Baltic Sea and the Germans to bombard Leningrad.¹¹

11 J. Janssens et al, 'Space weather: The impact on security and defense', in: K.-U. Schrogl et al. (eds.), *Handbook of space security* (Cham: Springer, 2019). See: https://doi.org/10.1007/978-3-030-22786-9_94-1.

In addition, and more importantly nowadays, the phenomenon of aurora also interacts with our radio signals and may cause their scattering. In radar operations, this is referred to as *auroral clutter*.¹² Just like other sources of radio or radar clutter, it may significantly limit ranges and thus radar detection capability. This backscatter may also further appear in some radio communications through the atmosphere as increased noise.

Twinkling of satellite links

Trans-atmospheric radio links may also be impacted in regions outside of those experiencing aurora. In March 2002, during Operation Anaconda in Afghanistan, a Quick Reaction Force was directed to rescue units from the summit of Takur Ghar. While underway, a message was sent via SATCOM (satellite communications) letting the crew know to avoid the mountain top due to the presence of Al Qaeda and Taliban fighters. The message was never received, however, and the helicopter landed under intense fire, with the mission eventually leading to loss of life.¹³

During times of increased geomagnetic activity, the structure of the ionosphere can often become disturbed. Disturbances cause a so-called *scintillation* of the signal, which is a rapid variation in the signal's amplitude and phase as it is travelling through its layers. Beyond a certain level of scintillation, the signal may become completely useless. Strong scintillation is more likely to happen in Arctic and equatorial regions compared to mid-latitudes.

Strong ionospheric scintillation affects many of our signals propagating through the atmosphere, including SATCOM at lower frequencies (less than a few GHz) and less robust GNSS services. Especially in the Arctic, the coverage of satellites is generally worse than in mid-latitudes, and some of them only rise to lower elevations above the horizon. This means that the signal has to travel through the disturbed ionosphere longer and thus becomes more distorted. Plus, while in mid-latitudes and

equatorial regions, it is usually straightforward to connect to a different satellite of the service with a link that does not suffer from these effects, due to the worse coverage in the Arctic, this is not always possible.

A user may perceive this phenomenon as a simple disruption of service. Strong scintillation in the Arctic occurs largely around midnight and noon,¹⁴ but during very strong geomagnetic storms the ionosphere may be strongly disturbed for hours to days.¹⁵

Such ionospheric changes also result in the fact that the refractive index, important for signal propagation, varies strongly in time and space. In that case, radar users may notice that their signals no longer propagate along the shortest paths across the atmosphere and ranging accuracy thus becomes impacted.

Magnetic variations confusing sensors

In August 1972, near the North Vietnamese port of Hai Phong, dozens of sea mines spontaneously exploded, without any object passing by.¹⁶ These sea mines were designed to sense changes in the magnetic field, assuming that any variations would be caused by passing ships. At the time, however, there were none – the variations were caused by the Sun.

The geomagnetic field is continuously influenced by the plasma wind that comes from the Sun. Because of the open magnetic field lines in

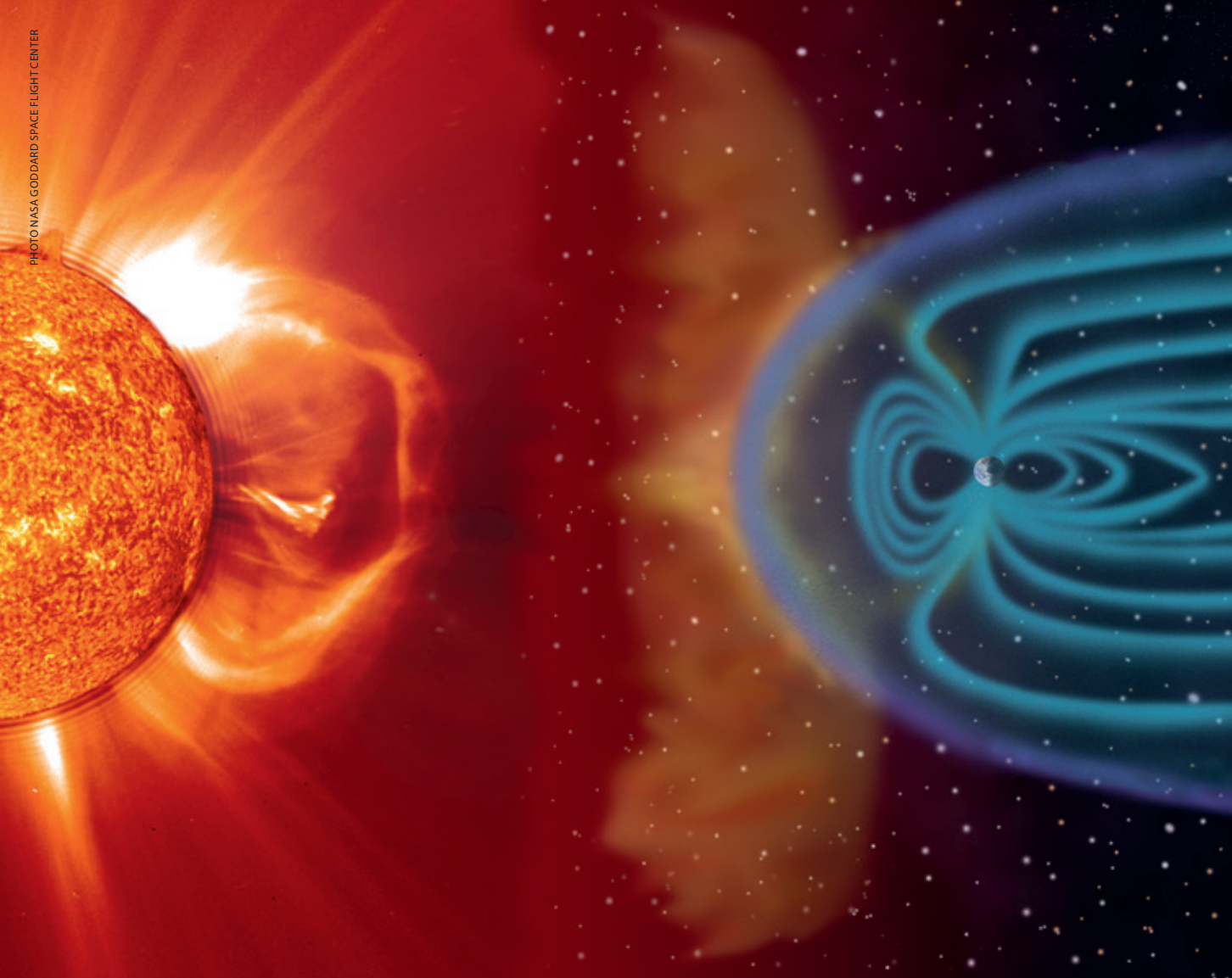
12 S. Simpson, 'U.S. Air Force Predicts Space Weather Impacts on Technological Systems', *Space Weather* 2 (2004) (12). See: <https://doi.org/10.1029/2004SW000108>.

13 Michael A. Kelly et al, 'Progress toward forecasting of space weather effects on UHF SATCOM after OPERATION Anaconda', *Space Weather* 12 (2014) (10) 601–611. See: <https://doi.org/10.1002/2014SW001081>.

14 Knut Stanley Jacobsen and Michael Dähnn, 'Statistics of ionospheric disturbances and their correlation with GNSS positioning errors at high latitudes', *Journal of Space Weather and Space Climate* 4 (2014) Article A27. See: <https://doi.org/10.1051/swsc/2014024>.

15 Knut Stanley Jacobsen et al, *Scintillation in the Arctic during the May 2024 Mother's Day storm*, *Journal of Space Weather and Space Climate* 15 (2025) 57. <https://doi.org/10.1051/swsc/2025045>.

16 Scientific American, 'A solar storm detonated U.S. Navy mines during the Vietnam War', 14 November 2018. See: <https://www.scientificamerican.com/article/a-solar-storm-detonated-u-s-navy-mines-during-the-vietnam-war/>.



A coronal mass ejection (CME) blasts from the Sun's surface in the direction of Earth, where the blue lines represent magnetic field lines that (mostly) deflect the blast. CME's take some time to reach Earth which gives a window to issue warnings

the Arctic, it is this region that feels this activity the strongest. In extreme solar events, such as in August 1972, the changes in the geomagnetic field are so large that they are felt all over the globe, such as was the case of Vietnam. Geomagnetic activity may influence the accuracy and reliability of any system making use of magnetic sensing, including magnetic detection (for instance of submarines), sea mines and magnetic navigation.

The influences of a changing magnetic field may also have wider-scale effects. Following the laws of electromagnetism, magnetic field variations create electric currents. These direct currents may enter power systems and transformers, and since transformers are designed to work with alternating currents instead, they can become saturated and damaged. Due to this phenomenon, for example in March 1989,¹⁷ a solar storm caused several millions of people to lose power for nine hours in Quebec, Canada. Actually, one of the first mentions of space weather goes back to the Carrington event in 1859, the strongest space weather event measured to date, during which the induced currents were so strong that they disrupted telegraph lines globally and even caused their operators to receive electric shocks.¹⁸

17 BBC, 'What the 1989 storm did to Quebec'. See: <https://www.bbc.co.uk/programmes/w3ct4x8h>.

18 Jasna Hodžić, 'The Carrington Event of 1859 Disrupted Telegraph Lines. A "Miyake Event" Would Be Far Worse', *Jstor Daily*, 7 September 2023. See: <https://daily.jstor.org/the-carrington-event-of-1859-disrupted-telegraph-lines/>.

To this date, these currents affect the performance of power grids in Nordic countries, especially in regions where the ground allows the currents to accumulate. During strong solar activity, one must thus not only beware of the integrity and accuracy of their signals and sensors but also of the robustness of their power infrastructure to unexpected currents.

Mysterious technical problems that resolve themselves?

Even though the Sun has been affecting the reliability of our systems and infrastructure ever since their beginnings, proper awareness of space weather effects among the users of these systems is often still lacking, especially at latitudes where these events are not felt so strongly. Part of the reason why this is the case may be the fact that the actual system effects, such as temporary losses of signal and increased radio noise, can be easily attributed to a variety of technical problems that occur in these systems frequently. Such incorrect attribution may then lead to waste of resources with the systems being flagged as inoperable until they receive a technical check later and until it is confirmed that they mysteriously started working according to the specifications again.

For this reason, if odd technical issues occur, especially with systems using radio signals and especially if these affect multiple systems simultaneously, consulting the local space weather centre may be advantageous before classifying the issue as purely technical. Frequently, all that is required is determining whether an event has indeed taken place at the given time and if it could have impacted the given location and frequencies.

Of course, in actual operational scenarios, understanding space weather effects is not only needed to properly interpret technical malfunctions, but also to determine what the correct course of action should be to have them resolved. Depending on the space weather event and the affected systems, there are various mitigation strategies from which the system

operator may choose, depending on the type of situation they are in and the resources they have available.

Mitigation strategies

Just like with terrestrial ‘regular weather’, one of the most important strategies for mitigation is actively monitoring current conditions and their forecasts. Many countries issue their own space weather products with forecasts for the following days, just as it is done for terrestrial weather. In the Netherlands, a space weather product is issued by the earlier mentioned Joint Meteorological Group. For instance, it takes one to three days for a coronal mass ejection to arrive from the Sun, which gives us a window to issue warnings. It should be noted, however, that the accuracy of space weather forecasts is still limited due to the fact that to a great degree, our detailed understanding of the underlying processes is lacking. As a consequence, some phenomena (such as the timing of solar flares) are still impossible to forecast.

Unfortunately, we also cannot always accurately predict how severely a system will be impacted by a specific event. System response to space weather depends on many factors with the often unknown internal design of it being one. For instance, less advanced and therefore cheaper, civilian GPS will be inaccurate at much lower levels of ionospheric disturbance than military GPS. The military should always, when possible, make use of dual-frequency military-code GPS, in short MilGPS.

Incorrect attribution may lead to waste of resources

The effects of space weather are much more difficult to understand intuitively when compared to terrestrial weather

If an event is expected that may disturb a system (or a service) essential for a mission, this mission can be postponed or fast-tracked. If fast tracking or delaying is not possible, one may choose to deploy additional systems to ensure redundancy. For instance, if the beginning of a mild particle storm is observed that causes an HF blackout, but does not significantly impact the operations of satellites, commanders planning Arctic operations dependent on long-distance communication may prefer to rely more heavily on super high-frequency SATCOM over HF radio. Likewise, if a strong geomagnetic storm is predicted that may disturb the ionosphere significantly in the region and impact SATCOM, carrying HF radio as a backup for long-distance communication may be a good option.

System redundancy can also be implemented on a permanent basis. For instance, in June 2024, during Baltops24, HNLMS Johan de Witt experienced significant solar radio burst effects that also affected the availability of GPS for a specific duration of time. However, the inertial navigation system of the ship was more than accurate enough to be able to bridge that timeframe.

If temporary or permanent redundancy is not possible, system operators who experience a blackout may decide to try other system settings, such as different frequencies, if they have these available. For instance, radio bursts typically only affect a certain portion of the radio spectrum, so trying out another channel may resolve the issue. For HF blackouts due to solar flares, lower frequencies of the HF spec-

trum are affected much more, so switching to the higher ones may work to restore communication. Overall, system users should be aware of the potential vulnerabilities of their system to these effects and what may be attempted to overcome them.

To achieve this level of understanding, in the longer term, raising awareness among the system users, commanders and other decision-makers is crucial by appropriate training. This training must be developed in such a way that it directly links the observed space weather conditions to system effects, ideally in the language of the system user.

On the practical side, it is important to keep participating in exercises that take place in Arctic regions where these effects happen on a more regular basis and share know-how with allies who have more experience in this area. This includes Nordic countries, which are used to experiencing these effects and correcting for them during their operations. This can be complemented by exercises that simulate operations in denied, degraded, and disrupted operational environments.

However, space weather does not only have to be a pitfall, especially if combined with a good preparedness level and the knowledge of potential impacts on the adversary. For instance, knowing that specific systems of the adversary are not currently operational, or simply being better prepared for these impacts, can lead to a tactical advantage. This is called a 'Tactical Exploitation of the Environment', and it also forms a focus of planned future research within the Ministry of Defence.

Conclusions and recommendations

Space weather, just like regular weather, is here to stay. It can cut our communications, degrade navigation accuracy, obstruct our radar vision and even damage our power systems. Especially in the Arctic, these effects are difficult to ignore when safe and undisturbed operations are a priority.



HNLMS Johan de Witt participated in Exercise Baltops24. During the exercise, the ship experienced loss of GPS for a specific duration as a result of solar radio bursts. System redundancy mitigated the effects: the ship's inertial navigation system was more than accurate enough to bridge that timeframe

Understanding and interpreting space weather, however, remains a challenge. The effects of space weather are much more difficult to understand intuitively when compared to terrestrial weather as they are often not visible to humans other than through the responses of their systems.

Our understanding of solar activity is still limited. So is our ability to accurately predict system responses due to the fact that system behaviour frequently depends on the often unknown details of its internal design. These two aspects combined mean that it is still very difficult for us to issue accurate forecasts and corresponding detailed advice for system users.

Still, monitoring current conditions and attempting to forecast them for the hours and days to come remains the best practice to mitigate the effects. With a sufficient warning in advance, missions potentially sensitive to

these effects can be delayed or fast-tracked, or decisions can be made to deploy less vulnerable equipment instead. Interpretation of atypical technical malfunctions, especially those involving radio signals, can happen with the advice of space weather experts to avoid attributing these effects to the adversary or simply labelling the system as dysfunctional. To achieve this insight, it is pivotal to keep increasing the awareness of these effects across all levels of the organization. Responsiveness and adapting to disturbances, in the planning and execution of military operations, starts with training and educating officers and system operators.

In the way ahead, there is still a long way to go before space weather is handled the same way as 'regular' weather. However, if safe and undisturbed operations all the way to the Arctic is what is required, then nothing ought to discourage us from trying. ■

Waarom de krijgsmacht baat heeft bij chemische technologie

Prof. dr. Edwin Zondervan, University of Twente

Wie aan de krijgsmacht denkt, denkt al snel aan wapensystemen, militair materieel en geopolitiek. Achter vrijwel iedere militaire operatie bevindt zich echter een minder zichtbaar systeem van processen. Brandstof moet beschikbaar zijn waar nodig, water moet worden gezuiverd, energie moet betrouwbaar worden opgewekt en gevaarlijke stoffen moeten veilig kunnen worden verwerkt. Ook beschadigde of bedreigde industriële infrastructuur moet kunnen worden beoordeeld, veiliggesteld of aangepast.

Veel van deze vraagstukken zijn in de kern procestechnologische vraagstukken. Juist bij de eerste hoofdtaak van Defensie, de bescherming van het eigen en bondgenootschappelijke grondgebied, kunnen kennis van chemische technologie en procestechniek daarom recht-

streeks bijdragen aan operationele inzetbaarheid en voortzettingsvermogen.

Diezelfde kennis is bovendien van belang bij andere vormen van militaire inzet. Europese krijgsmachten worden ook ingezet bij humanitaire operaties: de bouw van noodhospitals, ondersteuning bij vaccinatiecampagnes, hulp bij overstromingen en hulp bij bosbranden. In al deze situaties doemt dezelfde kernvraag op: hoe garanderen we onder extreme omstandigheden betrouwbare energie, schoon water en veilige leefomstandigheden? Voor een belangrijk deel ligt het antwoord in chemische technologie.

Neem bijvoorbeeld de energietransitie bij de marine. Het gebruik van synthetische brandstoffen, waterstof of hernieuwbare methanol kan CO₂-uitstoot verminderen zonder operationele slagkracht te verliezen. NAVO-landen onderzoeken de opschaling van duurzame brandstoffen voor schepen en vliegtuigen.¹ Daarnaast speelt drinkwatervoorziening in

¹ *Climate Adaptation Plan 2024* (Washington, D.C., U.S. Department of State) zie: www.sustainability.gov.

uitzendgebieden, of aan boord van onderzeeboten, een cruciale rol. Dankzij chemisch-technologische kennis zoals membranen, omgekeerde osmose en compacte zuiveringsinstallaties kan een veilige watervoorziening alleen met proceskennis worden gerealiseerd.

Ook bescherming tegen chemische, biologische en nucleaire dreigingen valt onder chemische technologie. Gasmaskers, filters en beschermen-de coatings zijn gebouwd op scheidingstechnologie en materiaalwetenschap. In crisissituaties kan civiele infrastructuur, zoals kunstmest-fabrieken, worden omgeschakeld naar de productie van defensiemiddelen, maar alleen wanneer ingenieurs de procesaanpassingen begrijpen.

Dit brengt ons bij een cruciaal punt: de krijgsmacht staat voortdurend voor procestechnologische vraagstukken. Massabalans, thermodynamica, transportverschijnselen, scheidingstechnieken, reactorontwerp, het zijn allemaal bouwstenen van chemische technologie die direct bijdragen aan de beschikbaarheid van schoon water, veilige energie en beschermingssystemen.

Relevantie voor de toekomst

De relevantie van deze verbinding wordt urgenter. Geopolitieke verschuivingen, kwetsbare internationale toeleveringsketens en technologische disrupties maken duidelijk dat de weerbaarheid van krijgsmacht en samenleving mede afhankelijk is van betrouwbare energie-, water- en industriële systemen. Dit vraagt om militaire officieren en ingenieurs met inzicht in energie-, water- en materiaalsystemen onder extreme voorwaarden.

Het strategische belang van energie- en waterzekerheid wordt ook internationaal onderkend. Zo stelt de Amerikaanse krijgsmacht eisen aan energie- en wateroptimalisatie.² Ook binnen de bredere Amerikaanse overheid hebben klimaatadaptatie en de weerbaarheid van vitale systemen aandacht gekregen.

Ook op opleidingsvlak zijn er voorbeelden. De U.S. Military Academy (West Point) biedt een

volledige opleiding chemische technologie, inclusief procesontwerp en laboratorium-practica.³ De U.S. Naval Academy kent een rigoureuze curriculum met reactorontwerp, procesregeling en massa-energiebalansen.⁴ In Servië is er zelfs een militaire academie met een officieel programma military-chemical engineering.⁵

Geen militarisering, maar versterking van veerkracht

Pleitbezorging voor een sterkere positie van chemische technologie in militaire opleidingen is géén pleidooi voor militarisering van de wetenschap. Het gaat juist om het versterken van veerkracht: veerkracht in energie- en drinkwatervoorziening; veerkracht in het ontwerpen van razendsnel inzetbare, flexibele systemen; en veerkracht bij de uitvoering van militaire én humanitaire missies.

Door deze disciplines te combineren, kunnen we een nieuwe generatie ingenieurs opleiden die niet alleen waarde aanbiedt aan de industrie, maar ook bijdraagt aan de veiligheid en weerbaarheid van de samenleving.

Van molecuul tot militaire inzetbaarheid

Chemische technologie wordt vaak omschreven als het ontwerpen van processen 'van molecuul tot onderneming'. Het is tijd om daar een nieuwe dimensie aan toe te voegen: van molecuul tot militaire inzetbaarheid en maatschappelijke weerbaarheid. In een wereld die steeds onvoorspelbaarder wordt, is het vermogen om processen te ontwerpen én aan te passen misschien wel onze meest strategische hulpbron. ■

2 U.S. Army Corps of Engineers, *Design Requirements for Energy and Water Optimization*, ER 1110-1-8173 (22 april 2025).

3 U.S. Military Academy West Point, Chemical Engineering Major. Zie: <https://www.westpoint.edu/academics/majors-and-minors/chemical-engineering-major>.

4 U.S. Naval Academy, programma chemical engineering (zie onder andere CollegeVine overzicht: <https://www.collegevine.com/faq/133101/how-competitive-is-the-chemical-engineering-program-at-the-us-naval-academy>).

5 Zie: Military Academy Serbia, Military-Chemical Engineering program, https://en.wikipedia.org/wiki/Military_Academy_%28Serbia%29.

De wapenwedloop achter het beeldscherm

Jaus Müller

Ergens in het bergland van Noord-Jemen, tussen kale rotsellingen, zanderige vlaktes, diepe ravijnen en straatarme dorpen, klappt een groep mannen een laptop open. Zo zou het tafereel eruit kunnen hebben gezien. Via een internetverbinding krijgen ze de AI-assistent Claude aan de praat. De mannen, vermoedelijk verbonden aan de Houthi-beweging, hebben een probleem: hun ballistische raketten doen niet precies wat zij willen. Mogelijke doelwitten zijn schepen in de Rode Zee of doelen in Saudi-Arabië. Om de raketsoftware te verbeteren, schakelen ze Claude in. Na een aanpassing proberen ze het opnieuw. Kennelijk met onvoldoende resultaat, want enkele uren later vragen ze de AI-assistent waarom de raket niet naar behoren functioneerde en wat eraan moet worden verbeterd.

Zo probeerden vermoedelijke leden van de Houthi-beweging, een bondgenoot van Iran, de afgelopen maanden met westerse AI-software hun raketarsenaal te verbeteren. Op het hoofdkantoor van Anthropic, de maker van Claude in San Francisco, zo'n 14.000 kilometer verderop, kwamen alarmerende berichten binnen vanuit het eigen systeem. Wat gebeurde daar allemaal in Jemen met Claude? Anthropic greep in en blokkeerde de accounts. Maar een deel van de hulp middels het Large Language Model was toen al geleverd.

Deze casus van Jemenitische doe-het-zelf-raketgeleerden laat zien hoe kunstmatige intelligentie haar weg vindt naar het militaire domein – en hoe belangrijk regulering is binnen het militaire domein. Het valt enigszins te prijzen dat Anthropic ingreep en vervolgens een uitvoerig rapport over het incident publiceerde. Tegelijkertijd weten we niet in hoeveel gevallen ingrijpen achterwege bleef en welke incidenten niet zijn gepubliceerd.¹ Het wringt dat we voor het bewaken van zulke grenzen zo sterk vertrouwen op de zelf-regulering van Amerikaanse technologie-bedrijven met grote commerciële belangen. Wie bepaalt welke militaire toepassingen toelaatbaar zijn, en wie ziet erop toe dat die grenzen worden gehandhaafd?

Telkens weer laten we ons verrassen door het enorme tempo van de wapenwedloop achter het scherm. Onlangs pakte ik het uitstekende boek *De oorlog van morgen. Wat de conflicten van nu ons leren over toekomstige dreigingen* van NLDA-collega Martijn Kitzen en Tim Sweijs er weer eens bij. Het boek, waarvan de eerste druk in april 2025 verscheen, verkent met een vooruitziende blik de toekomst van oorlogvoering en staat daarbij stil bij de stormachtige ontwikkelingen rond AI. Op pagina 124 staat bijvoorbeeld: 'Later deze eeuw, zo voorspellen sommige technologen, kan het zelfs gevolgd worden door ASI, of artificial super intelligence, die slimmer is dan mensen en onze prestaties simpelweg overtreft'.² Met de snelheid waarop AI-systemen zich sindsdien al hebben ontwikkeld, lijkt het waarschijnlijk dat deze mijlpaal eind van dit decennium wordt bereikt; wat

1 Anthropic, *Detecting and countering misuse of AI: September 2026* (10 september 2026). Zie: <https://www-cdn.anthropic.com/e50be2e51e7695dc4b1366a37a245a597377d3b5/Anthropic-Detecting-and-countering-091026.pdf>.

2 Martijn Kitzen en Tim Sweijs, *De oorlog van morgen. Wat de conflicten van nu ons leren over toekomstige dreigingen* (Amsterdam, Uitgeverij Balans, 2025) 124.



gisteren nog verre toekomst leek, wordt vandaag als voldongen feit gepresenteerd.

Met de razendsnelle opmars van AI groeien ook de zorgen binnen militaire organisaties. Statelijke actoren, zoals China, kunnen kunstmatige intelligentie gebruiken om digitale aanvallen uit te voeren. Maar minstens zo zorgelijk is dat ook niet-statelijke actoren toegang krijgen tot uiterst krachtige kennis-systemen, zoals het voorbeeld van Claude in Jemen laat zien.

Het is zeker niet de eerste keer dat de wereld wordt geconfronteerd met een nieuwe technologie waarvan de mogelijk schadelijke gevolgen nauwelijks zijn te overzien. Daarbinnen zijn er ook voorbeelden van geslaagde zelfregulering. In de jaren zeventig beloofde nieuwe DNA-technologie nieuwe medicijnen en een snellere en tevens goedkopere productie van bestaande middelen, zoals antibiotica. Tegelijkertijd konden wetenschappers daarmee genen veranderen op manieren waarvan zij de gevolgen amper konden overzien. Bij vroege experimenten werd DNA gebruikt van een virus dat kanker kon veroorzaken; andere experimenten introduceerden resistentie tegen antibiotica. Wat als zulke organismen uit het laboratorium zouden ontsnappen? Een geschrokken wetenschapper waarschuwde dat het besmettingsgevaar de mensheid aan de rand van een soort biologisch Hiroshima bracht. Wetenschappers kwamen samen in conferentiecentrum Asilomar, in het Californische Monterey, om afspraken te maken over de veilige toepassing van deze nieuwe technologie.³

Een andere historische parallel is de ontwikkeling van het kernwapen in de jaren 40 en de regulering die daarop volgde. Tegenwoordig roepen leiders van AI-bedrijven op tot regulering en waarschuwen sommigen zelfs voor de mogelijke vernietiging van de mensheid als die uitblijft. Ook binnen het Manhattanproject klonken dergelijke waarschuwingen over de gevolgen van de technologie die wetenschappers zelf hielpen te ontwikkelen. In juni 1945, nog vóór de atoombom op Hiroshima viel, richtten

Als de wereld opnieuw een kwart eeuw nodig heeft om grenzen te stellen, hoeveel valt er dan nog te beteugelen?

zij zich in het grootste geheim met het *Franck Report* tot de Amerikaanse minister van Oorlog. Daarin waarschuwden ze voor een nucleaire wapenwedloop en de verwoestende gevolgen daarvan. Internationale controle was volgens hen noodzakelijk om dat gevaar te bezweren. Het was een oproep aan de politieke leiding om in actie te komen.⁴

Het grote probleem is de factor tijd. De nucleaire geschiedenis laat zien hoe traag internationale beheersing tot stand kan komen. In juni 1945 waarschuwden wetenschappers de Amerikaanse regering voor de gevaren van een nucleaire wapenwedloop. In 1957 werd het Internationaal Atoomenergieagentschap (IAEA) opgericht. Het Non-proliferatieverdrag volgde in 1968 en trad in 1970 in werking: een kwart eeuw na Hiroshima. Er zat vijftientig jaar tussen de eerste inzet van een kernwapen en het verdrag dat de hoeksteen van de internationale nucleaire beteugeling zou worden. Zelfs tijdens de Koude Oorlog bleken zulke afspraken mogelijk. Inmiddels staat het internationale stelsel dat ze zou moeten dragen zwaar onder druk. Bovendien werd de ontwikkeling van kernwapens geleid door staten, terwijl bij AI grote technologiebedrijven het tempo dicteren. Hun activiteiten overschrijden landsgrenzen en laten zich moeilijk onder één internationaal regime brengen. Als de wereld opnieuw een kwart eeuw nodig heeft om grenzen te stellen, hoeveel valt er dan nog te beteugelen? ■

3 Kate Zernike, 'How Scientists Contained a Threat That Could Have Destroyed Humanity', *The New York Times*, 23 september 2026.

4 James Franck e.a., 'The Franck Report. A Report to the Secretary of War', juni 1945, beschikbaar via de Federation of American Scientists. Zie: <https://sgp.fas.org/eprint/franck.html>.

Zwerfvuil en pacifisme

Pien van der Hoeven

Doet u het ook wel eens? Vuil rapen? Het wint aan populariteit naarmate er overal meer zwerfvuil ligt. Ik neem me al wandelend door mijn buurt steeds weer voor de volgende keer een vuilniszak mee te nemen. Vrienden van mij zijn verder en voor hen is het rapen van vuil al vaste prik.

Natuurlijk is het jammer dat het nodig is. Het is jammer dat mensen vuil achterlaten in parken, op pleinen, op straat – maar het is de realiteit. Dus we moeten er iets aan doen. ‘Ik ben tegen zwerfvuil’, is een gratuite constatering. Het heeft ook geen zin om een demonstratie tegen zwerfvuil te organiseren. Net als het zinloos is een demonstratie tegen armoede of tegen oorlog te organiseren. Het is pas zinvol om te demonstreren als je de vraag hebt beantwoord wat de aanpak van het probleem zou moeten zijn.

De drieduizend mensen die eind vorige maand op de Dam tegen oorlog demonstreerden, waren het allerminst eens over de aanpak. Het was een bonte stoet: studenten die bang waren dat er door alle defensie-uitgaven nog meer geld aan onderwijs wordt onttrokken, principiële pacifisten en verdedigers van Poetin. Allen konden zich scharen achter de leuze ‘Peace Now’. Maar ja, wie niet?

Ieder zinnig mens is voor vrede, maar de vraag hoe we vrede behouden of bereiken wordt heel verschillend beantwoord. Grofweg zijn er voor dit

vraagstuk twee benaderingen. De eerste kan worden samengevat met het aloude Latijnse gezegde *si vis pacem, para bellum*, wat wil zeggen dat als je vrede wilt, je je verdediging op orde moet hebben. De andere benadering is precies omgekeerd. In de woorden van de Oekraïense vredesactivist en dienstweigeraar Yurii Sheliazhenko: ‘If you prepare for war you get war, if you prepare for peace you get peace’.¹ Het probleem bij de laatste benadering is: wat doe je als een ander begint met vechten? Keer je hem dan de andere wang toe? In de meeste gevallen zal de vechtersbaas dan helaas niet jouw moreel hoogstaande voorbeeld volgen, maar je verpletteren. Dus de consequentie van deze benadering is dat je niet kunt beschermen wat je lief is. Een maatschappij die zich niet verdedigt tegen potentiële vijanden zal uiteindelijk worden vernietigd, inclusief haar ideële erfgoed – zoals deze pacifistische benadering.

Maar ook de andere benadering, die de nadruk legt op afschrikking, kent serieuze problemen. Toen de Amerikaanse wapenindustrie in de Koude Oorlog een permanente status kreeg, signaleerde president Eisenhower al dat bewapening een doel in zichzelf werd, een verdienmodel voor krijgsmacht, politiek en industrie. De vijfsterrengeneraal waarschuwde dat de ondemocratische macht van dit militair-industriële complex de waarden teniet zou doen waar het bij de verdediging nu juist om draaide, de democratische manier van leven. Voor Israël, dat zwaar vertegenwoordigd is in het Amerikaanse militair-



¹ European Network Against Arms Trade & Transnational Institute, *Fanning the flames. How the European Union is fuelling a new arms race* (Amsterdam, maart 2022).

industriële complex, is deze vrees al bewaarheid. Daar functioneert de democratie nauwelijks nog vanwege de verregaande militarisering. Ook de kwaliteit van de Amerikaanse samenleving heeft – zowel in financieel als moreel opzicht – ernstig te lijden van de perverse prikkel tot oorlogvoering die uitgaat van het militair-industriële complex. In de rapporten van de denktanks waar dit complex van wemelt, worden de opties voor militaire operaties uitgewerkt. Zo liggen ze altijd klaar voor de politiek om mee aan de haal te gaan. De onsamenhangende oorlog in Iran is daar het meest recente voorbeeld van.

In de nieuwe voorstelling van het Haagse theatercollectief Firma Mes worden de twee hierboven genoemde, tegengestelde benaderingen om oorlog tegen te gaan gepersonifieerd door de hoofdrolspelers. Deze voorstelling, 'Wapens', gaat pas 21 november in première, maar laatst was er al een doorloop voor publiek. 'Wapens' gaat over twee vrouwen die elkaar bij het gezamenlijke zwerfuij rapen hebben leren kennen. Hun liefde voor elkaar heeft te lijden onder hun verschillende benadering van geweld. De ene vrouw is pacifiste en de ander werkt bij het ministerie van Defensie. Samen zijn ze afhankelijk van de baan bij Defensie, die het paar in staat stelt hun dure kindervens te vervullen. Dus de corruptie van het pacifistische ideaal zit al in de plot ingebakken.

Ik was er weer van onder de indruk hoe dit toneelgezelschap, Firma Mes, via uitvoerig onderzoek tot een voorstelling komt en zo een maatschappelijk probleem in al zijn complexiteit op de planken brengt – blikverruimend documentair theater, zoals hun slogan luidt. Na afloop van de doorloop mocht het publiek advies geven aan de theatermakers over wat nog beter kon. Ik vertelde dat ik me makkelijker identificeerde met de vrouw die zich niet schuldig wil maken aan geweld. Degene die bij Defensie werkt, werd mij iets te agressief neergezet. En dat doet af aan de bedoeling van de makers: de dilemma's rond bewapening voor het voetlicht brengen zonder (meteen) een positie in te nemen. De voorstelling wil juist duidelijk maken dat we allemaal in zekere zin gecorrumpeerd raken door ons verlangen naar

veiligheid en bestaanszekerheid, ook al hebben we nobele uitgangspunten.

Net als de twee vrouwen in 'Wapens' dat op het toneel doen, moeten we als maatschappij de twee uitersten in balans houden. We hebben beide tegengestelde benaderingen nodig om oorlog te voorkomen.

In Europa hebben we onze verzorgingsstaat kunnen opbouwen in de uitzonderlijke periode dat we profiteerden van andermans militaire afschrikking – en dat is nu voorbij. De Pax Americana bestaat niet meer. Zondagskinderen waren we, zoals Caroline de Gruyter dat noemt in haar nieuwste, gelijknamige boek. De geopolitieke realiteit is dat we nu zelf voor een afdoende afschrikking moeten zorgen. De VS en Israël zijn daarbij verkeerde voorbeelden; daar is de uitbouw van de strijdkrachten ten koste van de rest van de maatschappij – en de wereld – gegaan. Gelukkig zijn er betere voorbeelden. Polen, Finland, Zweden en de Baltische staten zijn een stuk beter voorbereid op oorlog in Europa dan Nederland, zonder dat je in hun geval kunt spreken van gemilitariseerde samenlevingen.

Maar met een afdoende militaire afschrikking alleen dienen we de vrede niet. Even goed hebben we de politieke wil nodig om er zonder gebruik van geweld uit te komen. En die wil moet stevig tegen de belangen van de aan oorlog verdienende industrie en diensten in kunnen gaan.

Dat brengt ons terug bij de aanpak. Waar gaan we de straat voor op? We moeten demonstreren voor transparantie in de defensie-uitgaven. Juist bij militaire zaken wordt al te makkelijk een beroep gedaan op geheimhouding die het democratische proces verstoort. De vraag wie waaraan verdient en of dat doelmatig is, moet in de openbaarheid worden beantwoord. Op onze spandoeken moet niet het vrijblijvende 'Peace Now' staan, maar 'Verantwoording Nu!'.

En wanneer we niet de straat op gaan met een spandoek, dan gaan we de paden op en de lanen in met een vuilniszak. Wat een genot is dat vuil rapen vergeleken met het doden tellen en puinruimen dat niet zo heel ver van ons vandaan de dagelijkse oorlogsrealiteit is. ■



The Weapons of Word War III

Ukrainian Experience
Door Roman Romanioek
Kyiv (Laboratoria) 2026
232 blz.
ISBN 9786178401931
€ 33,-

Er zijn boeken die je leest als tijdsdocument en boeken die je leest als geschiedenis. *The Weapons of World War III* van de Oekraïense auteur en journalist Roman Romanioek behoort op merkwaardige wijze tot beide categorieën tegelijk. Hoewel de Engelstalige versie pas begin dit jaar verscheen, voelt het bij het openslaan aan alsof je een archief raadpleegt. Recente wapensystemen, zoals de maritieme drones Sea Baby en Magura, waarvan de auteur de ontwikkeling gedetailleerd analyseert, zijn alweer opgevolgd door nieuwere uitvoeringen.

Het boek opent met een gewichtig voorwoord van Valerii Zaloezjnyi, de voormalige Oekraïense opperbevelhebber, tegenwoordig ambassadeur in het Verenigd Koninkrijk. Hij zet direct de toon door te stellen dat we niet langer aan de vooravond staan van een wereldwijd conflict, maar dat we er middenin zitten. Voor Zaloezjnyi is de oorlog in Oekraïne het laboratorium waar de regels voor de Derde Wereldoorlog worden geschreven. Hij betoogt dat de transitie naar autonome, door kunstmatige intelligentie gestuurde wapensystemen onomkeerbaar is en dat Oekraïne vóór 2027 een beslissend voordeel moet opbouwen.

Daarna, zo waarschuwt hij, komt er een nieuwe generatie autonome wapens aan, die de oorlog opnieuw fundamenteel zal veranderen en niet noodzakelijk in het voordeel van Oekraïne.

Prototypes

Zaloezjnyi's visie over autonome wapens en keerpunten klinkt bij vlagen bijna futuristisch. Maar Romanioek laat zien hoe snel ontwikkelingen in de Russisch-Oekraïense oorlog sinds 2022 zijn gegaan en daarmee hoe nuchter de visie van de voormalige opperbevelhebber eigenlijk is. Het boek is een opeenvolging van de ontwikkeling van verschillende wapensystemen, die ten tijde van de start van de Russische grootschalige invasie nog niet bestonden of slechts in de vorm van prototypes.

Een van deze systemen is de zelfrijdende houwitsers Bohdana. Nog niet eens volledig uitontwikkeld, wordt een prototype van dit artilleriestuk in juni 2022 ingezet om het door Rusland bezette eiland Zmiyni in de Zwarte Zee onder vuur te nemen. Dit klinkt simpeler dan het is, aangezien dit moet gebeuren vanuit de relatief nabijgelegen Donaudelta op veertig kilometer afstand van het eiland. Dit is een

moerassig gebied waar de Bohdana moeilijk kan manoeuvreren. Als oplossing wordt het artilleriestuk op een ponton geplaatst, zo dicht mogelijk bij vaste grond gebracht om daar een paar schoten te lossen, waarna het artilleriestuk weer de ponton op rijdt zodat de bemanning zich kan verplaatsen om Russisch *counter battery*-vuur te ontlopen. Het is de vuurdoop van de Bohdana, die daarna in een verbeterde versie in serieproductie wordt genomen.

Drones

De hoofdstukken over drone-ontwikkeling vormen de kern van het werk. Romanioek beschrijft hoe de eerste generaties drones kwetsbaar bleken voor Russische elektronische oorlogvoering, wat Oekraïense teams dwong om binnen enkele weken nieuwe frequenties, navigatiesystemen en vluchtpatronen te implementeren. Dit proces van *trial and error*, zoals het monteren van een Starlink-terminal op een Nemesis-quadcopter, verving traditionele, jarenlange testtrajecten.

Voortdurend doorlopen de ontwikkelaars van de defensie-industrie samen met militaire eenheden het proces van kruipen en lopen naar rennen, zo beschrijft Romanioek. Dit wordt treffend geïllustreerd in de ontwikkeling van de Lioetyi-langeafstandsdrone. Tijdens de eerste testlanceringen in het najaar van 2023 moest een auto dicht achter een opstijgende Lioetyi rijden, die op dat moment nog voorzien was van een wankel onderstel: 'This means that you have to chase this 50-kilogramme bomb from behind in a car at speeds of up to 150 km/h so that the operator can see it and align it with the runway'. Inmiddels zetten de Oekraïense strijdkrachten de Lioetyi en FP-1-drones met

honderden tegelijk in, nacht na nacht, tegen Russische olieraffinaderijen en havens. Het feit dat de vroege prototypes van deze drones nu al in musea in Kyiv staan, benadrukt de versnelling van de technologische ontwikkelingscyclus in Oekraïne.

Naast deze langeafstandsdrone gaat Romanoek ook uitgebreid in op de ontwikkeling van surveillancedrones aan het front. Hij beschrijft de werking van dit type drone, zoals de PD-2 en later ook de elektrisch aangedreven Shark, en maakt duidelijk hoe de inzet ervan de targetingcyclus enorm versnelt: 'No

artillery piece will fire, unless you will tell it where to fire', citeert hij de Oekraïense kolonel Oleksandr Popov, commandant van de 15e Artillery Reconnaissance Brigade. Dit proces koppelt de detectie van elektronische emissies aan directe visuele lokalisatie door drones, wat een snelle en precieze doelbepaling mogelijk maakt.

Tijdsdocument

The Weapons of World War III is niet het definitieve boek over de Russisch-Oekraïense oorlog, dat boek moet uiteraard nog geschreven worden. Ook heeft de auteur maar een beperkt deel van de ontwikke-

ling van nieuwe Oekraïense wapensystemen beschreven. Onderwerpen zoals de roemruchte Oekraïense FP-5 Flamingo-kruisraket en de snelle opkomst van grond drones (*unmanned ground vehicles*) zijn niet opgenomen in het boek. Maar als tijdsdocument, voorzien van een voorwoord van de militaire strateeg die de contouren van deze oorlog al vroeg scherp zag, is het interessant voor iedereen die zich in dit tijdsgewricht bezighoudt met technische innovatie en veranderingen van de krijgsmacht in brede zin. ■

Lkol Peter Schrijver MA, NLDA

AANKONDIGING

Internationale conferentie NISA

De internationale conferentie van de Netherlands Intelligence Studies Association vindt dit jaar plaats op 2 en 3 december in The Hague Conference Centre New Babylon in Den Haag.

Het centrale thema is 'Resilient Intelligence in an Era of Democratic Backsliding'. Naast diverse keynote speakers uit zowel de wetenschap als de inlichtingenpraktijk zijn er panels over onder meer autocratisering, hybride dreigingen en opkomende technologieën.

De conferentiedagen starten om 9.30 uur, met een inloop vanaf 9.00 uur.

Meer informatie is te vinden op de website van de NISA. Aanmelden kan door te mailen naar conference@nisa-intelligence.nl.



‘Goed georganiseerde weerdienst is een dringende eisch’

Fenomenen rond ‘ruimteweer’ kunnen impact hebben op militaire operaties, bijvoorbeeld wanneer radarsignalen worden verstoord. Het is natuurlijk bekend dat het ‘gewone’ weer ook van invloed is op de militaire praktijk. Al voor de Eerste Wereldoorlog hadden Frankrijk en Duitsland een militaire weerdienst. In de loop van die oorlog ‘is men het groote nut van dezen dienst gaan inzien met het gevolg, dat een enorme uitbreiding tot stand kwam’, schrijft eerste luitenant der artillerie A.L.J. de Pauw.¹ ‘Begon Duitschland in 1914 met 14 vaste en 2 verplaatsbare weerstations, in October 1918 telde de Legerweerdienst totaal 316 stations!’

Deze ontwikkeling kwam onder andere door de uitbreiding van de luchtvloot, het gebruik van het gaswapen, en het ‘in rekening brengen der daginvloeden bij de artillerie’, aldus artillerist De Pauw. De luitenant vervolgt met een vergelijking van de Franse en Duitse militaire weerdienst, die vooral veel overeenkomsten blijken te vertonen, al is het Franse materieel ‘meer geperfectionneerd dan bij de Duitschers’.

Met de lessen van 1914-1918 in het achterhoofd concludeert De Pauw: ‘Ongetwijfeld zullen in de toekomstige oorlogen de luchtvloot en de gasoorlog een groote rol spelen; de artillerie zal de daginvloeden in rekening blijven brengen en zeer zeker bij het zware geschut. Al deze strijdmiddelen hebben behoefte aan de gegevens omtrent de atmosferische toestanden; zij kunnen vrijwel niet daarbuiten. Een goed georganiseerde weerdienst is derhalve een dringende eisch.’ Is de Nederlandse krijgsmacht daartoe in staat? Bij De Pauw is nog niets bekend over een weerdienst in een oorlogsorganisatie, dus enigszins pessimistisch stelt hij: ‘Ik vrees, dat het antwoord ontkennend zal luiden; dit zou te bejammeren zijn.’

Uiteindelijk, nu ruim 100 jaar later, kan luitenant De Pauw toch tevreden zijn: niet alleen is er een afdeling voor meteorologie en oceanografie (METOC), die houdt zich ook nog eens meer en meer bezig met invloedrijke fenomenen die ontstaan buiten onze atmosfeer. ■

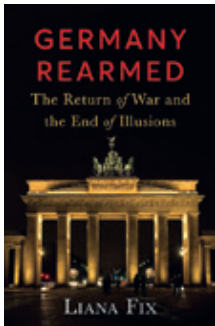


FOTO: BEELDBANK NIMH - FOTOTECHNISCHE DIENST LUCHTVAARTAFDELING

Meteorologische waarneming met behulp van de luchtballon ‘Hollandia’, 1925

¹ A.L.J. de Pauw, ‘Militaire weerdienst’, *Militaire Spectator* 93 (1924) (6) 385-392.

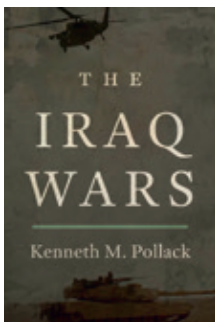
SIGNALERINGEN



Germany Rearmed

The Return of War and the End of Illusions
Door Liana Fix
Londen (Hurst) 2026
216 blz.
ISBN 9781805266808
€ 29,-

Duitsland wil een grotere militaire rol spelen in Europa en de NAVO, maar kan het land gezien de opkomst van de extreem-rechtse AfD verankerd blijven in de liberaal-democratische waarden? Die vraag stelt Liana Fix zich in *Germany Rearmed*. Fix zegt dat de Duitsers na de Tweede Wereldoorlog decennialang met de mythe van het pacifisme hebben geleefd, waarbij zij hun veiligheid uitbesteedden aan de VS. Onder president Donald Trump zijn de Amerikaanse garanties echter onzeker geworden. Volgens Fix heeft Duitsland met het *Sondervermogen* van 100 miljard euro voor de krijgsmacht een goede stap gezet voor de bewapening van het eigen land en de NAVO-taakvervulling.



The Iraq Wars

Door Kenneth M. Pollack
New Haven (Yale University Press) 2026
880 blz.
ISBN 9780300251722
€ 39,-

Sinds 1979 heeft de VS vijf oorlogen met of tegen Irak gevoerd. In *The Iraq Wars* geeft Kenneth Pollack een analyse van de politieke, diplomatieke en militaire keuzes die Washington in die conflicten in het Midden-Oosten maakte. De auteur buigt zich ook over alternatieven die mogelijk beter waren geweest, waaronder het verlengen van operatie Desert Storm met 48 uur om Saddam Hussein ten val te brengen. En was er met de kennis van toen een noodzaak om Irak in 2003 binnen te vallen? Volgens Pollack had de Amerikaanse regering geen duidelijk plan voor de tijd na de invasie en was dat een grove nalatigheid.



Iron Dome

A History of Israel's Military Strategy
Door Jean-Loup Samaan
Londen (Bloomsbury) 2026
240 blz.
ISBN 9781350499607
€ 18,-

In *Iron Dome* beschrijft Jean-Loup Samaan hoe het gelijknamige raketafweersysteem de militaire strategie van Israël heeft veranderd. Iron Dome is in korte tijd ontwikkeld en snel uitgegroeid tot een iconisch symbool van moderne oorlogvoering, aldus Samaan. Hij kijkt naar de rol van Iron Dome in de strijd tegen Hezbollah en Hamas en concludeert dat het systeem meer is dan alleen technologisch vernuft: de ontwikkeling bracht in de Israëlsche krijgsmacht een moeizaam proces op gang om de strategie aan te passen. Samaan, die eerder schreef over militaire strategie in de Golfregio, kijkt ook hoe Iron Dome de militaire samenwerking tussen Israël en de VS beïnvloedt.



The Russian General Staff

Door Oscar Jonsson
Washington, D.C., (Georgetown University Press) 2026
176 blz.
ISBN 9781647127510
€ 23,-

Oscar Jonsson behandelt in *The Russian General Staff* wat hij noemt het belangrijkste militaire orgaan in het Rusland van leider Vladimir Poetin. Volgens de auteur heeft de Russische invasie van Oekraïne in 2022 aan het licht gebracht dat er in het Westen veel onduidelijkheid heerst over de Russische militaire top, oftewel 'het brein' van Poetins krijgsmacht. Gezien de Russische dreiging is dat een gevaarlijke leemte. Jonsson ziet in de relatie tussen de generale staf en Poetins beleidsmakers veel aanwijzingen waarom Rusland in de oorlog ondermaats presteert. Hij onderbouwt zijn conclusies met interviews en empirisch onderzoek beginnend bij de Sovjet-invasie van Afghanistan in 1979.

