

Een nieuwe Militaire Revolutie?

Technologische trends, Oekraïne en de toekomst van oorlog

Adelbert Bronkhorst en Frans Osinga

Deel 2: 2014-2022: Een nieuwe koude oorlog, een nieuwe RMA (?)

Een nieuwe Koude Oorlog

De Russische annexatie van de Krim was een veiligheidspolitiek waterscheidingsmoment.¹ Een nieuwe Koude Oorlog was volgens het Kremlin een feit, en dat terwijl de NAVO in 2010 nog officieel stelde dat een grootschalig conflict op Europees gebied zeer onwaarschijnlijk was.² Op de NAVO-top in Wales besluiten de lidstaten zich weer te richten op bondgenootschappelijke verdediging en afschrikking, ofwel Artikel 5.³ De hernieuwde rivaliteit tussen de grootmachten en het risico op de terugkeer van interstatelijke oorlogvoering worden daardoor vanaf 2014 de bril waardoor Westerse analisten technologische ontwikkelingen beoordelen en niet langer crisismanagement, humanitaire interventies en optreden tegen niet-statelijke actoren. Een periode waarin, zo stelt een recent rapport van RAND, een *inflection point* is opgetreden, een ommekeer in militaire machtsverhoudingen: Westerse ‘superiority is gone, surely with respect to China but in significant ways with respect to the forces of other, less powerful adversaries as well, and it is not coming back. At its root, the problem is that the United States and its allies no longer have a virtual monopoly on the technologies and capabilities that made them so dominant against the forces of nations like Iraq, Serbia, and Afghanistan – near-real-time sensing, high-capacity communications links, precision guidance via miniaturized electronics, and advanced software being primary among these’.⁴ Dat vat goed de zorg samen van een gestage stroom aan studies over de impact van technologische trends op internationale veiligheid en oorlogvoering die sinds 2014 het licht zagen.

Hybride oorlogvoering en soft cyber attacks

Een eerste strategisch thema betreft de wijze waarop de annexatie van de Krim plaatsvond. Geen grootschalige inval met gemechaniseerde eenheden, maar een diffuse operatie waarbij

desinformatie, misleiding en cyberaanvallen gepaard gingen met acties van militairen waarvan de nationaliteit wel werd vermoed maar bewust initieel ongewis werd gelaten. Rusland ontkende in eerste instantie betrokkenheid. Het was oorlog – het militaire instrument werd agressief ingezet om een politiek doel te bereiken waarbij de soevereiniteit van Oekraïne werd geschonden – maar door het ontbreken van kinetisch geweld werd dit eerst niet als zodanig herkend. De toenmalige SACEUR, generaal Philip Breedlove, betitelde dit als *hybrid warfare*, een thema dat vervolgens zowel in de NAVO als de EU (en westerse denktanks) op de politieke en wetenschappelijke agenda’s komt.

Hybride oorlogvoering betreft de georkestreerde inzet van conventionele militaire middelen, paramilitaire eenheden, irreguliere strijdmethoden, subversieve activiteiten, opruiing, psychologische oorlogvoering, propaganda, mediamanipulatie, misleidingactiviteiten, speciale eenheden zonder herkenningstekens op het uniform en cyberaanvallen, gepaard met een verregaande controle over de eigen media. Deze brede aanpak resulteert in het vermogen om invloed uit te oefenen in een samenleving zonder direct gewapend geweld toe te passen.

- 1 AIV, *Instabiliteit Rond Europa, Confrontatie met een Nieuwe Werkelijkheid*, Rapport no. 94, (Den Haag, Adviesraad Internationale Vraagstukken, april 2015); Ida van Veldhuizen e.a., *Geopolitiek en defensie. Pal staan voor vrijheid en veiligheid*, Geschrift 136 (Den Haag, Teldersstichting, 2017).
- 2 Sam Jones, ‘Dmitry Medvedev warns of ‘new cold war’’, *Financial Times*, 13 februari 2016. Zie: <http://www.ft.com/cms/s/0/a14e8900-d259-11e5-829b-8564e7528e54.html#axzz4liVoaRgz>.
- 3 Matthew Kroenig, ‘Facing Reality: Getting NATO Ready for a New Cold War’, *Survival*, 57:1 (2015) 49-70; François Heisbourg, ‘Preserving Post-Cold War Europe’, *Survival*, 57:1 (2015) 31-48; Alexander Lanoszka, ‘Russian hybrid warfare and extended deterrence in eastern Europe’, *International Affairs* 92: 1 (2016) 175-195; Roger McDermott e.a., ‘Cold War Déjà Vu? Nato, Russia and the Crisis in the Ukraine’, in: Guillaume Lasconjerias en Jeffrey Larsen (red.), *Nato’s Response to Hybrid Threats*, Forum Paper 24 (Rome, NATO Defence College, 2015).
- 4 David Ochmanek e.a., *Inflection Point. How to Reverse the Erosion of U.S. and Allied Military Power and Influence* (Santa Monica, RAND, 2023).

Het omvat intimidatie van politieke leiders en opinieleiders, omkoping, mediamanipulatie, desinformatie, sancties, militaire dreiging langs de grens in de vorm van oefeningen, cyberaanvallen et cetera.⁵ Het is de zone tussen vrede en oorlog waarvan Rusland (en ook China) behendig gebruikt maakt om extremisme, separatisme en nationalisme op te stoken, en daarmee anti-EU en anti-NAVO sentimenten.⁶

Cyberaanvallen maken hiervan een integraal onderdeel uit. Waar vanaf 2007, na de cyberaanvallen op Estland, de nadruk lag op *hard cyber* – cyberaanvallen op kritieke infrastructuur – wordt het Westen vanaf 2014 zich in toenemende mate bewust van de zorgwekkende impact van *soft cyber*.⁷ Social media blijken een front waarop Rusland de publieke opinie in westerse landen bespeelt. Zo poogt Moskou de legitimiteit van een zittende regering te ondermijnen, evenals de uitkomst van democratische verkiezingen. In diverse talen wordt via tv-zenders zoals RT en Sputnik en *troll armies* het Russische perspectief verspreid. De visie van westerse autoriteiten en de betrouwbaarheid van westerse media wordt in twijfel getrokken via frames die suggereren dat Europa geen antwoord heeft op het migratieprobleem, het

islamitisch terrorisme, dat het veel misdaad kent, Christelijke waarden schendt, et cetera.⁸ Voor het Westen was het, zoals Thomas Rid aantoonde, een onaangename herontdekking van de Russische strategie van Active Measures uit de Koude Oorlog.⁹

4IR, emerging technologies in de nieuwe geopolitieke context

In 2014 formuleert Klaus Schwab, kijkend naar wetenschappelijke, technologische en economische trends, de 4th Industrial Revolution-these.¹⁰

De 4IR wordt gedreven door de convergentie van civiele innovaties op het gebied van materialen, AI, quantum computing, big data, en robotica en zal grote maatschappelijke en geopolitieke omwentelingen veroorzaken. De schaduwzijden worden ook direct onderkend. Een van de eerste rapporten daarover is de lijvige Britse studie *Future Operating Environment 2035*. Naast klimaatverandering, urbanisatie en demografische verschuivingen wordt technologie gezien als een voorname drijver van strategische en operationele ontwikkelingen, waarbij de proliferatie van *dual-use*-technologieën, ook naar niet-statelijke actoren, met zorg wordt gadeslagen: 'Globalisation will allow a wider range of actors access to comparatively sophisticated weapons. Actors may employ existing dual use or commercial technologies in highly innovative ways, which may be disruptive. The previous technological advantage enjoyed by Western militaries will continue to be reduced out to 2035, for a number of reasons. Proliferation of technology means that a range of actors will have access to systems which used to be the sole preserve of developed countries. Technology will lead to greater proliferation of lower-end equipment and a reduction in its cost, through economies of scale'.¹¹ Het tempo van technologieontwikkeling zal accelereren, wat westerse krijgsmachten, en vooral Europese, voor grote uitdagingen zal plaatsen, want rond 2035 Europa 'may need to become accustomed to being overmatched by derived military capabilities'.¹²

In een vooruitziende blik waarschuwt het rapport voor de A2/AD problematiek. De dreiging kan bestaan uit 'ballistic missiles

- 5 Heidi Reisinger en Alexander Golts, 'Russia's Hybrid Warfare. Waging War Below the Radar of Traditional Collective Defence', in: Guillaume Lasconjerias en Jeffrey Larsen (red.), *NATO's Response to Hybrid Threats*, Forum Paper 24 (Rome, Nato Defence College, 2015) 113-136.
- 6 Todd Helmus, e.s., *Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe* (Santa Monica, RAND, 2018).
- 7 Zie ook Frans Osinga, Net (geen) oorlog(?). Hybrid Warfare en de uitdaging van de nieuwe geopolitieke rivaliteit, *Magazine Nationale Veiligheid en Crisisbeheersing* Vol. 14, No. 5/6 (2016) 16-21.
- 8 Luke Harding, 'We should beware Russia's Links with Europe's right', *The Guardian*, 8 december 2014; Peter Foster en Matthew Holehouse, 'Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy', *The Telegraph*, 16 January 2016; Stefan Meister en Jana Puglierin, *Perception and Exploitation. Russia's Non-Military Influence in Europe*, DGAPkompakt Vol. 10, oktober 2015. Zie: <https://dgap.org/en/article/getFullPDF/27185>; NATO Parliamentary Assembly Report, *The battle for the hearts and minds: countering propaganda attacks against the Euro-Atlantic Community*. Zie: <http://www.nato-pa.int/default.asp?SHORTCUT=4012>.
- 9 Thomas Rid, *Active Measures. The Secret History of Disinformation and Political Warfare* (New York, Farrar, Straus and Giroux, 2020).
- 10 Klaus Schwab, 'The Fourth Industrial Revolution. What It Means and How to Respond', *Foreign Affairs* (december 2015).
- 11 *Future Operating Environment 2035* (Londen, UK MoD, 2015) 4-5.
- 12 Ibid, 14.

(conventional warhead), loiter-capable automated systems; anti-ship ballistic missiles; super-cavitating torpedoes; advanced (perhaps even unmanned) submarines; and weapons of mass effect. For more advanced actors, offensive space- or ground-based anti-satellite systems will be able to disrupt [...] own space assets. Offensive and defensive cyber capability will offer specific advantages – disrupting our networks and systems, while countering our offensive cyber operations. Less technical methods will include conventionally-armed terrorist attacks and proxy warfare methods that open alternative fronts'.¹³ Voorts wordt verwacht dat tegenstanders in toenemende mate in staat zullen zijn geavanceerde kruis- en ballistische raketten in te zetten, directed energy weapons (DEW), effectieve lange-dracht anti-tankwapens, bewapende drones en swarming-tactieken met grote aantallen goedkope drones waarmee de westerse verdediging kan worden overweldigd. Nieuwe typen wapens zoals hypersonische raketten zullen in 2035 hun intrede hebben gedaan.¹⁴ Ook op gebied van AI, elektronische oorlogvoering (EOV), quantum computers, cyber, sensornetwerken en big-data analytics worden zorgwekkende ontwikkelingen gezien. Rond 2035 zullen ook meerdere actoren beschikken over 'ubiquitous persistent real-time, multi-sensor surveillance capabilities', en datzelfde geldt voor systemen voor elektronische oorlogvoering en space-based technologieën. Het gevolg is dat 'the proliferation of weapons technology will mean that many future adversaries will have capabilities designed to prevent our access to the maritime, land, air, space, cyberspace and electromagnetic environments'.

Dit weerspiegelt de ingrijpende modernisering van Russische conventionele capaciteiten. Langs de Europese grenzen worden in grootschalige Russische oefeningen nieuwe generatie gevechtsvliegtuigen geconstateerd, uitbreiding van maritiem materieel, geavanceerde luchtafweersystemen, grote aantallen grond-grond raketten, offensieve en defensieve cyber-capaciteiten en middelen voor EOV.¹⁵ Rusland blijkt in staat *snap exercises* te lanceren met grote hoeveelheden materieel en personeel (soms met meer dan

Met name de gegarandeerde dominantie in de lucht brokkelt af

100.000 man) die zich snel over strategische afstanden weten te verplaatsen, waarmee een militaire intimiderende dreiging kan worden neergezet.¹⁶ Integraal onderdeel daarvan – en van de westerse zorgen – zijn de Russische Anti Access-Area Denial (A2/AD) capaciteiten, met name in de enclave Kaliningrad. Door de stationering daar van moderne luchtafweersystemen, grond-grond raketten en middelen voor elektronische oorlogvoering kan Rusland in Oost-Europa het Westen ongestoorde toegang en gebruik ontzeggen van het luchtruim, weg- en zeetransport, en het elektronisch spectrum. Met name de gegarandeerde dominantie in de lucht die een asymmetrisch voordeel en escalatie-dominante met zich mee bracht, brokkelt hiermee af, en daarmee de geloofwaardigheid van de conventionele afschrikking van het Westen.¹⁷

13 Ibid, 15.

14 Ibid, 17.

15 Andrew Monaghan, 'The war in Russia's Hybrid Warfare', *Parameters*, vol. 45(4) winter 2015-16, pp. 66-74; Patrick J. Savage, 'The Conventionality of Russia's Unconventional Warfare', *Parameters* 48(2) Summer 2018, 77-85.

16 Dmitri Trenin, 'The Revival of the Russian Military; How Moscow Reloaded', *Foreign Affairs*, May/June 2016, Vol.95, no.3, pp. 23-29; Polina Sinoviets and Bettina Renz, 'Russia's 2014 Military Doctrine and Beyond: Threat Perceptions, Capabilities and Ambitions', in Guillaume Lasconjarias and Jeffrey Larsen (eds), *Nato's response to Hybrid Threats*, Forum Paper 24, Nato Defence College, Rome, 2015, pp.73-91.

17 Jay Ballard, 'What is Past is Prologue. Why the Golden Age of Rapid Air Superiority is at an End', *Joint Air and Space Power Journal*, edition 22 (Spring/Summer 2016) 56-64; Elbridge Colby en Jonathan Solomon, 'Facing Russia. Conventional Defence and Deterrence in Europe', *Survival*, 57:6 (2015) 21-50; Martin Zapfe en Michael Carl Haas, 'Access for Allies?', *The RUSI Journal*, 161:3 (2016) 34-41; Franz-Stefan Gady, 'US Air Force: Russia Has Closed Air Power Gap With NATO', *The Diplomat* (16 september 2015), zie: <http://thediplomat.com/2015/09/us-air-force-russia-has-closed-air-power-gap-with-nato/>; Stephan Frühling en Guillaume Lasconjarias, 'NATO, A2/AD and the Kaliningrad Challenge', *Survival*, 58:2 (2016) 95-116; Dave Majumdar, 'Can America Crush Russia's A2/AD Bubbles?', *The National Interest* (29 juni 2016), zie: <http://nationalinterest.org>; Alexander Lanoszka en Michael Hunzeker, 'Confronting the Anti-Access/Area Denial and Precision Strike Challenge in the Baltic Region', *The RUSI Journal*, 161:5 (2016) 12-18.

Hypersone technologie

De Russische assertiviteit en de gestage opkomst van China als *peer competitor* leidde in de VS, maar minder in Europa, tot een opleving van aandacht voor, en zorg over, nucleaire afschriking.¹⁸ Die zorg wordt ook gevoed door de opkomst van technologieën die de relatieve nucleaire stabiliteit kunnen ondermijnen, met name hypersone rakettechnologie. Er wordt onderscheid gemaakt tussen twee typen hypersone missiles met afnemende maturiteit. Ten eerste hypersone *glide vehicles*, die middels een raket worden gelanceerd en tijdens de opvolgende glijvlucht en in het eindtraject tijdelijk manoeuvreerbaar zijn. Ten tweede hypersone kruisraketten, die over het hele vluchtpad manoeuvreerbaar zijn en hun snelheid kunnen variëren. Enkel glide vehicles zijn in de periode tot 2022 ver genoeg ontwikkeld om ingezet te kunnen worden, waarbij opgemerkt dient te worden dat de door Rusland ontwikkelde Tsirkan en Avangard-wapens een minder geavanceerde variant vormen omdat ze in feite hypersone raketten zijn – ballistische missiles die in de eindfase beperkte manoeuvres kunnen uitvoeren. De grootste impact wordt verwacht van hypersone kruisraketten en goed manoeuvreerbare glide vehicles met een lange glijvlucht.

Een RAND-rapport uit 2017 waarschuwt wat de impact kan zijn: ‘Hypersonic missiles are a new class of threat because they are capable both of maneuvering and of flying faster than 5,000

kilometers per hour, which would enable such missiles to penetrate most missile defenses and to further compress the timelines for response by a nation under attack. The proliferation of such missiles beyond the United States, Russia, and China could result in other powers compressing their response timelines in ways that set their strategic forces on hair-trigger states of readiness — such as a strategy of ‘launch on warning.’ And such proliferation could enable such states to more credibly threaten attacks on major powers’.¹⁹ Minder dan een decennium resteert volgens RAND om verdere proliferatie tegen te gaan. De zorg is dat deze wapens, wanneer voorzien van informatie over de positie van Amerikaanse atoomwapens, kunnen leiden tot uitschakeling van zowel de *first* als *second strike*-capaciteit. Al en een netwerk van ISR systemen in de ruimte, onderzee en in de lucht zouden die informatie kunnen genereren. Dit vereist vervolgens dat de VS deze technologie eveneens omarmt om zodoende pariteit en dus *deterrence stability* te herstellen.²⁰ Een studie van de Congressional Research Service relativeert deze zorgen enigszins door te stellen dat de strategische impact van hypersone wapens beperkt is omdat de huidige ballistische intercontinentale raketten al in staat zijn de verdediging van op land gestationeerde nucleaire lanceersystemen te verzadigen.²¹ Desalniettemin kunnen deze wapens disruptief zijn omdat ze ook op tactisch niveau kunnen worden ingezet, bijvoorbeeld voor het aangrijpen van commando-posten of maritieme platformen.

Militarisering van de ruimte

Een andere potentieel destabiliserende factor is de toenemende militarisering van de ruimte. Dit is een cruciaal domein niet alleen omdat het een enabler vormt van diverse technologieën die een belangrijke rol spelen in westerse maatschappijen, maar ook omdat moderne oorlogvoering steeds afhankelijker is van ongestoord gebruik van capaciteiten in de ruimte. Inzet van GPS-gebaseerde precisiewapens en *long-endurance* drones, draadloze communicatie over grote afstanden, en persistente verkenning van vijandelijke gebieden berusten alle op capaciteiten die door satellieten worden geleverd. Met name de Chinese ontwikkelingen springen in

18 Keith Payne, ‘Nuclear deterrence in a new age’, *Comparative Strategy*, 37:1 (2018) 1-8; Elbridge Colby, ‘If You Want Peace, Prepare for Nuclear War’, *Foreign Affairs* Vol. 97, No. 6, (november/december 2018) 25-32; Andrew Krepinevich, ‘The Eroding Balance of Terror. The Decline of Deterrence’, *Foreign Affairs* Vol. 98, No. 1, (januari/februari 2019) 62; Baruch Malewich, ‘Futile superiority. Decision making and the development of new-generation nuclear weapons’, *Comparative Strategy*, 36:2 (2017) 99-114; Zenel Garcia, ‘Strategic stability in the twenty-first century. The challenge of the second nuclear age and the logic of stability interdependence’, *Comparative Strategy*, 36:4 (2017) 354-365.

19 Richard Speier e.a., *Hypersonic Missile Nonproliferation. Hindering the Spread of a New Class of Weapons* (Santa Monica, RAND, 2017).

20 Todd Sechser, Neil Narang en Caitlin Talmadge ‘Emerging technologies and strategic stability in peacetime, crisis, and war’, *Journal of Strategic Studies*, 42:6 (2019) 727-735; Jesse Wasson en Christopher Bluestein, ‘Taking the archers for granted. Emerging threats to nuclear weapon delivery systems’, *Defence Studies*, 18:4 (2018) 433-453;

21 Kelley Saylor, *Emerging Military Technologies. Background and Issues for Congress* (Washington, D.C., Congressional Research Service, april 2022).

het oog. China ontwikkelde een eigen GPS equivalent – het BeiDou-systeem – waarvan in 2016 23 satellieten in een baan waren gebracht. China ontwikkelde ook antisatelliet (ASAT) capaciteiten en voerde in 2007 een succesvolle test van een ASAT-missile uit. Zoals de commandant van US Space Command in 2016 zei: ‘China will soon be able to threaten US satellites in every orbital regime, from low Earth orbit a few hundred miles above the Earth, to geosynchronous orbit more than 20,000 miles up – where some of the military’s most important satellites circle the Earth’. Dit omvat niet alleen middelen tegen grondstations maar ook ‘co-orbital’ antisatellietsystemen die middels bijvoorbeeld een explosieve lading, laser of *jammer* westerse satellieten uit kunnen schakelen.²²

Ook de commercialisering van de ruimte in de laatste decennia wordt met zorg bekeken. In 2019 werd er naar schatting 323 miljard dollar in commerciële ruimtevaart geïnvesteerd. De brede beschikbaarheid van goedkope permanente surveillance vanuit de ruimte wordt gestimuleerd door grote technologiebedrijven zoals Google en SpaceX die lanceercapaciteit – platforms en raketten – en/of satellietsystemen aanbieden, al dan niet gekoppeld aan diensten voor beeldanalyse. Dominantie in de ruimte is door deze dynamiek niet langer het voorbehoud van staten. Tot aan 2010 waren het vooral nationale geclassificeerde militair geleide programma’s waarbinnen grote geostationaire en Medium Earth Orbit (MEO) satellieten werden gebouwd en gelanceerd. Daarna is een netwerk van internationale, snel innoverende private partijen ontstaan dat vooral kleinere, relatief goedkope Low Earth Orbit (LEO) satellieten ontwikkelt en deze systemen na lancering commercieel exploiteert.²³ Brad Townsend stelt dat ‘A paradigm shift occurred with the drop in launch costs that coincided with a rapid shift toward satellite miniaturization. Miniaturization altered the economics of satellite construction, leading to a revolution in satellite imagery. Smaller satellites are cheaper’.²⁴

Deze revolutie in permanente *remote sensing* door waarnemingssatellieten die op meerdere orbit-hoogtes en over diverse soorten sensoren beschikken, behelst niet alleen dreiging voor

ationale veiligheid door de strategische inlichtingen die hiermee kunnen worden gegeneerd, maar vertaalt zich ook in een operationele dreiging voor militaire eenheden, zeker wanneer dit wordt aangevuld met informatie uit drones en andere sensoren. Dit zal voor een toenemend aantal actoren *near real-time*-observatie van militaire capaciteiten en bewegingen mogelijk maken. Staten zullen diensten gaan inkopen en vele partijen zullen laagdrempelig toegang krijgen tot accurate inlichtingen, met als consequentie dat de dominantie van grote staten op dat gebied verdwijnt. Een gevolg kan zijn dat er eerder overgegaan wordt tot ontwikkeling en inzet van ASAT-wapens en het uitvoeren van offensieve acties (kinetisch en cyber) tegen de commando- en communicatiemiddelen van het satelliet-netwerk.

Van bewapende drones naar killer robots?

De inzet van bewapende drones werd door de VS ook na 2014 voortgezet. Na de snelle opkomst van IS in Irak tuigt de VS op verzoek van de Iraakse regering Operatie *Inherent Resolve* op in wat de By-With-and-Through approach ging heten (in feite een herhaling van het Afghaanse model zoals in het vorige artikel besproken). Een geavanceerde C2-infrastructuur en een paraplu van westerse airpower traden symbiotisch op met Amerikaanse speciale eenheden en Iraakse en Koerdische eenheden. Drones werden ook ingezet voor *targeted killings* van IS-leiders en het uitschakelen van zware wapens. De steeds intensievere luchtoperaties leidden uiteindelijk in 2019 tot het verdrijven van IS uit Irak.²⁵ Dit decennium ziet ook de introductie van zogeheten *loitering munitions* die rondvliegen in de

22 Brian Chow, ‘Stalkers in Space. Defeating the Threat’, *Strategic Studies Quarterly* (Summer 2017) 83-94.

23 James Clay Moltz, The Changing Dynamics of Twenty-First-Century Space Power, *Strategic Studies Quarterly*, Spring 2019, p.72

24 Brad Townsend, The Remote Sensing Revolution Threat, *Strategic Studies Quarterly*, Fall 2021, p. 70-72

25 Joseph Votel and Eero Keravuori, ‘The By-With-Through Operational Approach’, *Joint Force Quarterly*, Vol. 89 (2nd Quarter 2018) 40-47; Becca Wasser e.a., *The Air War Against the Islamic State. The Role of Airpower in Operation Inherent Resolve* (Santa Monica, RAND, 2021); Michael Gordon, *Degrade and Destroy. The Inside Story of the War Against the Islamic State From Barack Obama to Donald Trump* (Farrar, Straus and Giroux, New York, 2022).

buurt van een doel totdat lokalisatie plaatsvindt waarna het doel wordt aangevallen. Ze zijn oorspronkelijk bedoeld voor het aanvallen van SAM-sites. Vanaf 2010 werden ze echter ook ontwikkeld en ingezet voor het aangrijpen van andere gronddoelen zoals in het conflict in 2016 in Nagorno-Karabach te zien was.

Een zorgelijke ontwikkeling hierbij was dat de targeting niet altijd door een operator werd gedaan maar ook autonoom kon plaatsvinden. De vraag was of hiermee in feite een *killer robot* was gecreëerd. De discussie die vanaf 2013 over dergelijke Autonome Wapensystemen (AWS) woedt, leidde – in het Westen – tot de conclusie

dat targeting waarbij de mens *out of the loop* is onwenselijk is, onder meer omdat het onmogelijk wordt geacht middels AI onderscheid te maken tussen *combattants* en *non-combattants* en proportionaliteit voldoende in acht kan worden gehouden. Daarnaast is *meaningful human control* nodig om duidelijk te maken wie verantwoordelijk is voor de acties van een AWS. Zoals Human Rights Watch stelde: ‘killer robots’ raise serious moral and legal concerns because they would possess the ability to select and engage their targets without meaningful human control... There are also grave doubts that fully autonomous weapons would ever be able to replicate human judgment and comply with the legal requirement to distinguish civilian from military targets. Fully autonomous weapons themselves cannot substitute for responsible humans as defendants in any legal proceeding[...] Human commanders or operators could not be assigned direct responsibility for the wrongful actions of a fully autonomous weapon’.²⁶

In de discussie herhalen de kritische argumenten zich die in het debat rond bewapende drones naar voren werden gebracht. AWS zouden tot verregaande dehumanisering en depolitisering van oorlogvoering leiden. Ze herbergen het risico dat het enigszins gemakzuchtig wordt ingezet aangezien er geen levens van eigen troepen mee in de waagschaal worden gelegd.²⁷ Schending van de soevereiniteit van een tegenstander kan dan risicoloos plaatsvinden. Als oorlogvoering geen inzet van mensenlevens vereist, wordt militair geweld dan niet te lichtzinnig en snel ingezet?²⁸ Gevreesd wordt ook de wapenwedloop op dit vlak. Verwijzend naar Paul Scharre's boek *Army of None. Autonomous Weapons and the Future of War*, waarschuwt Pax for Peace dat ‘The main rationale for building fully autonomous weapons seems to be the assumption that others might do so’, which risks becoming a ‘self-fulfilling prophecy’.²⁹

Anderzijds bepleiten diverse studies de militaire merites van deze systemen.³⁰ Zwermen van AWS kunnen bijvoorbeeld vijandelijke luchtafweer overweldigen (en dus nuttig zijn als counter-

Autonome wapensystemen zouden tot verregaande dehumanisering en depolitisering van oorlogvoering leiden

- 26 Human Rights Watch, *Mind the Gap. The Lack of Accountability for Killer Robots*, report (9 april 2015).
- 27 Markus Wagner, ‘The Dehumanization of International Humanitarian Law. Legal, Ethical, and Political Implications of Autonomous Weapon Systems’, *Vanderbilt journal of transnational law*, Vol. 47:1371-1423.
- 28 Jürgen Altmann en Frank Sauer, ‘Autonomous Weapon Systems and Strategic Stability’, *Survival*, 59:5 (2017) 117-142.
- 29 Frank Slijper, Alice Beck en Daan Kayser, *State of AI. Artificial intelligence, the military and increasingly autonomous weapons* (Utrecht, Pax for Peace, 2019) 34. Zie: <https://paxvoorvrede.nl/wp-content/uploads/import/import/state-of-artificial-intelligence-pax-report.pdf>; Paul Scharre, *Army of None. Autonomous Weapons and the Future of War* (New York, W. W. Norton & Company, 2018).
- 30 Kenneth Payne, *Strategy, Evolution and War. From Apes to Artificial Intelligence*, (Washington, D.C., Georgetown University Press, 2018); Paul Scharre, *Army of None. Autonomous Weapons and the Future of War*; Paul Scharre, ‘The Real Danger of an AI Arms Race’, *Foreign Affairs* (mei/juni 2019) 135-144; Christian Brose, ‘The New Revolution in Military Affairs. War’s New Sci-Fi Future’, *Foreign Affairs* (mei/juni 2019) 122-134; Robert Latiffe, *Future war. Preparing for the new global battlefield* (New York, Vintage Books, 2017).

A2/AD middel) of toegang tot gebieden ontzeggen (en zodoende als eigen A2/AD middel functioneren). En anders dan *human-in-the-loop* drones zijn AWS niet kwetsbaar voor storing van datalinks. Het risico voor eigen militairen in stedelijke gebieden kan worden verminderd door robots in straten te laten patrouilleren en naar sluipschutters en IED's te speuren. Een zwerm van AWS kan ook langdurig boven een gebied blijven patrouilleren op zoek naar specifiek vooraf gedefinieerde doelen, zoals tanks, artilleriesystemen of mobiele raketlanceerplatforms. AWS kunnen tevens nuttig zijn bij het zoeken naar High Value Targets, zoals leiders van terreurbewegingen. In het maritieme domein kunnen bewapende *Unmanned Surface Vehicles* worden ingezet voor het blokkeren van nauwe passages, of als *surface torpedo*.³¹ Op strategisch niveau kunnen AWS die geprogrammeerd zijn om bij specifieke indicatoren automatisch te reageren de geloofwaardigheid van een afschrikkingsstrategie versterken.³² Ten slotte is het de vraag of AWS die slechts een beperkt deel van de targeting autonoom uitvoeren veel verschillen van al in gebruik zijnde automatische wapensystemen zoals systemen die worden ingezet tegen *anti-ship missiles*, of Patriot-systemen die verdedigen tegen ballistische raketten.³³ Al met al leidt het maatschappelijk debat over AWS tot aan 2022 in de meeste westerse landen tot terughoudendheid in het investeren in de ontwikkeling van AWS, ook omdat getwijfeld wordt of AI voldoende ontwikkeld is om doelen te identificeren in de complexiteit en dynamiek van een oorlogsgebied.

Artificial Intelligence

Naast AWS vormt AI volgens veel analisten een grote destabiliserende ontwikkeling. Het zal grote voordelen bieden bij het monitoren van datastromen, videobeelden en het analyseren van grote hoeveelheden data, waardoor inlichtinganalyse versneld en versterkt kan worden.³⁴ Ook zal het een force multiplier-effect kunnen hebben bij toepassing in cyberspace of in raketsystemen die zelfstandig doelen kunnen onderkennen en in robotica. Anderzijds is de exacte vorm waarin AI strategie gaat beïnvloeden en welke strategische theorie ontwikkeld zal

worden om AI optimaal in te kunnen zetten nog onduidelijk. Desondanks stelde de Russische leider Vladimir Poetin in 2017 dat 'Artificial intelligence is the future, not only for Russia, but for all humankind (...) 'It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world'.³⁵ Analisten zoals Keith Payne voorspelde dat 'AI will change power balances. AI will likely overmatch legacy military capabilities, dramatically redrawing the balance of power'.³⁶

De kracht van AI zal zich naar verwachting initieel het meest op tactisch niveau laten gelden. Zoals Payne in 2018 en later in 2021 in zijn boek *I Warbot* stelt, zal het leiden tot versnelde commandovoeringsprocessen en mogelijkheden om tactische plannen te gamen en te simuleren: 'autonomous and intelligent platforms will be able to manoeuvre faster and employ force with more precision than those operated by humans. Autonomy and networking, along with other technologies, including nano, stealth and bio, will offer sophisticated tactical war-fighting capabilities on land and sea, and in the air'. Hier tellen snelheid en het vermogen om enorme hoeveelheden data te analyseren en patronen te herkennen. Daarmee kunnen posities en manoeuvres van vijandelijke eenheden snel worden onderkend. De optimale inzet van artillerie of luchtsteun kan in hoog tempo worden gecoördineerd en doellocaties automatisch verspreid die zelfs zo nodig met loitering AWS kunnen worden aangevallen.

31 Scott Savitz e.a., *U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs)* (Santa Monica, RAND, 2013).

32 Amitai Etzioni en Dren Etzioni, 'Pros and Cons of Autonomous Weapons Systems', *Military Review* (mei-juni 2017) 71-81; Irving Lachow, 'The upside and downside of swarming drones', *Bulletin of the Atomic Scientists*, 73:2 (2017) 96-101.

33 *Autonome wapensystemen: het belang van reguleren en Investeren*, Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (Den Haag, december 2021).

34 Greg Allen en Taniel Chan, *Artificial Intelligence and National Security* (Cambridge, Harvard Belfer Center, 2017).

35 Citaat in Michael Horowitz, 'Artificial Intelligence, International Competition, and the Balance of Power', *Texas National Security Review*, Vol. 1, No. 3 (mei 2018) 38.

36 K. Payne, 'Artificial intelligence: A revolution in strategic affairs?', *Survival*, 60 (5) (2018) 7-32. Zie: <https://doi.org/10.1080/00396338.2018.1518374>.

Ten tweede wordt op het vermogen tot leren gewezen, en om connecties aan te brengen waarmee ook complexe systemen en patronen inzichtelijk worden. AI zal zelfs in staat zijn om menselijke gedragingen en intenties te interpreteren en mogelijke toekomstige handelingsopties in kaart te brengen. Versnelde inlichtingenprocessen zullen op strategisch niveau daarmee mogelijkheden creëren sneller strategie te ontwikkelen en tot besluiten te komen. Zoals Payne stelt in 2018, 'AI will also shape strategy by offering insights to elite decision-makers based on the processing of vast datasets. Strategic-level AI operating as an 'oracle' for decision-makers will be able to test accepted wisdom, discarding spurious associations, rejecting pet theories and identifying key vulnerabilities in enemies. [...] Strategic AI will not be subject to the myriad individual and collective psychological processes at work in human decision-making, including groupthink, confirmation bias, bureaucratic politics, excessive optimism and poor risk judgement.' Maar aangezien AI niet in staat is tot strategische creativiteit wordt effectiviteit bepaald door de koppeling van besluitvorming door mens en machine, ofwel human-machine teaming.³⁷

De snelheid van AI herbergt echter ook het risico dat rivalen besluitvorming zo veel mogelijk zullen automatiseren uit angst dat de ander voor een verrassing zorgt.³⁸ Onbedoelde escalatie kan het gevolg zijn. Escalatie kan ook het gevolg zijn

van de toenemende rol van AI bij desinformatie-operaties. Zogeheten *deep fake*-technologie maakt het mogelijk audio en video te creëren waarin polariserende en escalerende woorden in de mond worden gelegd van politieke leiders. Gebruik makend van Natural Language Processing kunnen op sociale media grote aantallen *trolls* (valse accounts) worden aangemaakt die nauwelijks te onderscheiden zijn van echte gebruikers. Zo kunnen bijvoorbeeld verkiezingen worden beïnvloed en communicatie tijdens een internationale crisis worden verstoord. Tot slot, zo waarschuwen meerdere auteurs, kunnen met AI versterkte inlichtingenorganisaties in de toekomst wellicht de locatie van kernwapens vaststellen bij rivalen. Uitholling van deterrence stability wordt gevreesd, des te meer wanneer een actor ook beschikt over een nieuwe generatie hypersone raketten.³⁹

Reacties in de VS: de Third Offset Strategy

Het is niet alleen de context maar ook de onzekerheid wat de gevolgen kunnen zijn van de nieuwe technologieën die zorgen voor een *security dilemma*. Veel staten investeren in AI-onderzoek juist om daarmee vast te stellen wat de militaire mogelijkheden zijn, en – met name China – doen dit in samenwerking met universiteiten en IT-bedrijven. Dat vindt onder grote geheimhouding plaats. Alle partijen vrezen achterstand op te lopen. Het antwoord van de VS is de zogeheten Third Offset (3OS); een investeringsstrategie naar analogie van de Second Offset Strategy uit de Koude Oorlog die de kwantitatieve voordelen die het Warschaupact genoot kon compenseren. Zoals een rapport het samenvatte 'the term Third Offset conveyed confidence that technology could once again enable the United States to achieve a technological advantage over its adversaries, although this time the objective was not to offset the Soviets' conventional advantages but rather to respond to specific challenges that are particular to fighting China and Russia and their advanced A2/AD capabilities.'⁴⁰

Deze strategie betrof investeringen in nieuwe typen atoomwapens en forse modernisering van conventionele militaire ISR-, commando- en wapensystemen. De 3OS beoogde nieuwe

37 Kenneth Payne, *I, Warbot. The Dawn of Artificially Intelligent Conflict* (Oxford, Oxford University Press, 2021).

38 Kenneth Payne, *Artificial Intelligence: A Revolution in Strategic Affairs?* *Survival*, 60 (5) (2018) 7-32. Zie: <https://doi.org/10.1080/00396338.2018.1518374>

39 James Johnson, 'Artificial Intelligence & Future warfare: implications for international security', *Defence & Security Analysis*, Vol. 35, No. 2, (2019) 147-169; Keir Lieber and Daryl Press, 'The New Era of Counterforce Technological Change and the Future of Nuclear Deterrence', *International Security*, Vol. 41, No. 4 (Spring 2017) 9-49; Mark Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control', *Survival*, 61:3 (2019) 81-92; Jürgen Altmann en Frank Sauer, 'Autonomous Weapon Systems and Strategic Stability', *Survival*, 59:5 (2017) 117-142; Caitlin Talmadge, 'Emerging technology and intra-war escalation risks. Evidence from the Cold War, implications for today', *Journal of Strategic Studies*, 42:6 (2019) 864-887; Michael Horowitz, 'When speed kills. Lethal autonomous weapon systems, deterrence and stability', *Journal of Strategic Studies*, 42:6 (2019) 764-788.

40 Gian Gentile e.a., *A History of the Third Offset, 2014-2018* (Santa Monica, RAND, 2021).

technologieën snel te ontwikkelen, te testen en te voorzien van operationele concepten teneinde in ieder geval technologische pariteit te kunnen handhaven en bij voorkeur een voorsprong te kunnen herstellen. Daarmee wilde de VS het vermogen tot *power projection* handhaven. Niet minder dan een revolutie in technologie wordt essentieel geacht om de toekomstige militaire machtspositie te kunnen handhaven. De strategie stelde als doel dat de VS in staat zal zijn om volledig autonome systemen in te zetten in zogeheten hotspots. Daarnaast moet de VS op grote afstand zonder veel risico met een combinatie van stealth-vliegtuigen en onbemande systemen luchtoperaties kunnen uitvoeren ondanks vijandelijke moderne luchtverdedigingssystemen. Ten derde diende onderzeese capaciteit te worden ontwikkeld waarmee A2/AD-gebieden binnen kunnen worden gedrongen. Dat met deze ambitieuze strategie en versnelde (en kostbare) investeringen in technologische ontwikkelingen een toenemende kloof zou ontstaan ten opzichte van de NAVO-partners werd op de koop toe genomen. Europese landen werden geacht soortgelijke maatregelen te treffen.⁴¹

De Amerikaanse National Defense Strategy van 2018 beaamt de visie en de zorgen van de 3OS. Het stuk stelt dat ‘Today, every domain is contested – air, land, sea, space, and cyberspace. [...] the security environment is also affected by rapid technological advancements and the changing character of war. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology – the very technologies that ensure we will be able to fight and win the wars of the future. New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed’.⁴²

Ook *technology trend*-studies van de NAVO reflecteerden de nieuwe geopolitieke situatie en pleitten voor investeringen in nieuwe technologieën

Technology trends in de NAVO

Ook *technology trend*-studies van de NAVO reflecteerden de nieuwe geopolitieke situatie en pleitten voor investeringen in nieuwe technologieën. Net als andere Amerikaanse studies refereert het NAVO tech-trendrapport van 2022 aan de invloed van civiele technologieën en de democratisering van geweld vanwege de eenvoudige proliferatie van eenvoudig te militariseren technologieën. Het voorziet, verwijzend naar de 4IR, de ‘seventh generation military revolution’:⁴³ ‘The same wide span of Fourth Industrial Revolution technology (data, processing, connectivity, AI, robotics, biosciences, autonomy and so forth) that is changing how we live, work and play will now transform the way war is waged – in a process spanning at least a generation ... Military transformation will largely be about the rapid adoption and adaptation of civil-sector-derived technology and methods in disruptive military applications ... The future of military success will now be owned by those who conceive, design, build and operate combinations of

41 Tim Sweijs en Frans Osinga, ‘Maintaining NATO’s Technological Edge’, in: John Olsen (red.), Whitehall Paper 95 (1) (2019) *Future NATO. Adapting to New Realities*, 104-118. Zie: <https://doi.org/10.1080/02681307.2019.1731216>; Gian Gentile e.a., *A History of the Third Offset*, 71.

42 U.S. National Defense Strategy (Washington., D.C., U.S. Department of Defense, 2018).

43 *Science & Technology Trends 2020-2040. Exploring the S&T Edge* (Brussel, NATO Science & Technology Organization, Office of the Chief Scientist (maart 2022) 6.

information-based technologies to deliver new combat power'.⁴⁴

De NAVO onderkent een set prioritaire technologiegebieden, de zogeheten *emerging and disruptive technologies* (EDT's). De EDT's bestaan uit vijf disruptieve technologieën – big data, AI, autonomie, hypersone technologie en ruimte-technologie – en drie emergente technologieën – biotechnologie & *human enhancement*, quantum-technologie, en materialen & productietechnologie. Als disruptief worden die technologieën en ontdekkingen beschouwd die binnen 5-10 jaar significante en mogelijk revolutionaire impact kunnen hebben op militaire capaciteiten. 'Emergent' zijn die technologieën die pas na 10-20 jaar dergelijke effecten kunnen genereren. De NAVO-studies uit 2019 en 2022 signaleren ook drie overkoepelende kenmerken van nieuwe technologieën:

- Intelligent: de exploitatie van AI in analytische processen en systemen, en de symbiotische koppeling van AI en 'human intelligence';
- Verbonden: de exploitatie van netwerken van knooppunten in virtuele en fysieke domeinen - sensors, organisatie-elementen, individuen en autonome 'agents', die met elkaar verbonden zijn via nieuwe data-encryptie methoden;
- Gedistribueerd: uitgebreide gedecentraliseerde inzet van sensor-, opslag en analysecapaciteiten.

Hiermee zullen *battle networks* worden gevormd waarin de snelheid en effectiviteit van data-verwerving, analyse en besluitvorming drastisch verbeterd zijn. Dit zal ook nieuwe vormen van human-machine teaming vereisen. De competitie tussen battle networks zal resulteren in de noodzaak voortdurend in een hoog tempo de algoritmes van de intelligente systemen aan te passen. Ook zullen de geavanceerde C4ISR-netwerken primaire doelen worden van fysieke en cyberaanvallen. Door de toenemende rol van sensors en communicatiecapaciteiten in de ruimte vertaalt de groeiende afhankelijkheid van battle networks zich in 'the need to think,

plan and operate in a widely dispersed, interconnected and multi-domain manner'. Het zal leiden tot een continu adaptatieproces om domeindominantie te verkrijgen waarin offensieve *counter-domain capabilities* bescherming en tegenmaatregelen vereisen, die weer zullen resulteren in *counter-counter-measures*. De verregaande digitalisering van C4ISR-systemen en processen en de miniaturisering van ICT zullen de *precision strike*-capaciteiten verder vergroten. *Swarming* en het gebruik van goedkope precisiewapens zullen steeds grotere dreigingen vormen voor cruciale capaciteiten; een echo van eerdere Amerikaanse network-centric warfare toekomstvisies.

De NAVO-studie verwacht echter ook dat veel EDT's fundamentele vragen op ethisch en juridisch gebied zullen oproepen. Dat moet NAVO-landen er niet van weerhouden om onderzoek en ontwikkeling al op te starten, met name van mogelijke tegenmaatregelen. Omdat de technologieën grotendeels door commerciële belangen worden gedreven, wordt verwacht dat ze al op relatief korte termijn beschikbaar komen voor vijandelijke actoren, waardoor de strategische competitie zal verscherpen. Het toekomstige slagveld zal ook, ondanks deze verwachte innovaties, een mix vertonen van oude en nieuwe wapensystemen. Niet alle lidstaten zullen in hetzelfde tempo innoveren, wat problemen zal opleveren ten aanzien van connectiviteit, communicatie, doctrine en interoperabiliteit.

Een nieuwe RMA?

In 2019 stelde Brose, kijkend naar deze technologieën, dat zich voor onze ogen een RMA voltrekt.⁴⁵ Hij refereerde daarbij aan de gecombineerde effecten van cyberaanvallen, EO, hypersone missies, DEW, zwermen van autonome systemen, alomtegenwoordige sensoren en intelligente systemen. Daardoor wordt de *sensor-to-shooter*-tijd drastisch gereduceerd, kunnen wapens sneller en nauwkeuriger vuren, en kunnen doelen overal worden gevonden en op grote afstand worden uitgeschakeld. Een gevolg is dat het essentieel wordt om eigen middelen te kunnen verbergen en die van de tegenstander te kunnen opsporen. Brose concludeerde dat: 'The militaries that embrace

⁴⁴ Ibid, 7.

⁴⁵ Christian Brose, 'A New Revolution in Military Affairs. War's Sci-Fi Future', *Foreign Affairs*, (mei/juni 2019).

and adapt to these technologies will dominate those that do not. In that regard, the U.S. military is in big trouble'.⁴⁶

Ook O'Hanlon, kijkend naar dezelfde technologische trends, is van mening dat een RMA op handen lijkt.⁴⁷

Door het hoge, zo niet revolutionaire innovatietempo zullen de komende twee decennia zelfs meer verandering in oorlogvoering kennen dan de vorige twee. Op de horizon ziet O'Hanlon 'swarms of robotic systems, usable as both sensors and weapons', laserwapens, hypersonische missielen en onbemande onderzeeboten. De competitie tussen de grootmachten verhoogt de belangen die op het spel staan in deze race want 'The return of great-power competition during an era of rapid progress in science and technology could reward innovators, and expose vulnerabilities, much more than has been the case this century to date'. Michael Raska wijst erop dat de ontwikkelingen duiden op een AI-gedreven RMA, verschillend van de IT-RMA van de jaren 90. Voor het eerst wordt de VS geconfronteerd met een geopolitieke rivaal, China – en in mindere mate Rusland – die in staat is zijn eigen AI-RMA te realiseren die de militaire superioriteit van de VS kan ondermijnen. De innovaties binnen deze RMA worden voornamelijk door de commerciële sector ontwikkeld en kennen daardoor een grote proliferatie. Toekomstige oorlogvoering zal worden bepaald door de snelle verspreiding van robotica, autonome wapensystemen en AI-capaciteiten in militaire systemen, verwerkt in nieuwe operationele concepten en organisatiestructuren.⁴⁸

Voor het landoptreden zal de invloed ondergaan van deze ontwikkelingen. *Close combat* zal drastisch veranderen door de toegenomen transparantie en het vermogen om met drones tactische aanvallen te plegen. Dit zal ook de tactische inzet van traditionele wapensystemen van landstrijdkrachten veranderen. Het kleine formaat van drones bemoeilijkt detectie door radarsystemen. Luchtverdedigingssystemen kunnen daardoor worden gepenetreerd. Drones zullen hierdoor het offensief vermogen van niet-westelijke actoren versterken. Wellicht dat drones met groot bereik en accuratesse *close combat* op het slagveld zelfs overbodig – want

veel te riskant – maken. Aan en langs het front ontstaat een dodelijke competitie van *hider-finder* tussen drones en vliegtuigen enerzijds en lucht- en droneverdediging anderzijds. Het voorkomen van detectie wordt cruciaal in een frontlinie met zwermen van verkennings- en aanvalsdrones.

Een ander probleem is dat kleine statelijke en niet-statale actoren de beschikking zullen krijgen over capaciteiten – *small, smart and cheap* – die voorheen het privilege waren van grote staten.⁴⁹ Goedkope en accurate drones en kruisraketten met een groot bereik (respectievelijk 800 en 1500 kilometer) vormen een strategische aanvalscapaciteit waarmee verrassing kan worden bereikt omdat ze vanuit simpele lanceerplatforms zoals vrachtwagens of scheepscontainers kunnen worden afgevuurd. Dit zal westerse eenheden kunnen dwingen de afstand tot het front te vergroten.

Ook op strategisch niveau worden consequenties verwacht. Westerse landen moeten er van uitgaan dat zij de relatieve immuniteit tegen aanvallen verliezen. Civiele infrastructuur zoals havens, energiecentrales en vliegvelden kan worden bedreigd door *long-range drones*, *containerized weapons on commercial ships*, *sea mines*, en *submersible drones*, middelen die ook niet-statale actoren kunnen verkrijgen. Bases worden eveneens kwetsbaar. Dat betekent ook dat het gebruikelijke westerse vermogen om met militaire middelen tegen slechts geringe operationele risico's invloed uit te oefenen – *power projection* ten behoeve van bijvoorbeeld humanitaire interventies – wordt ondermijnd. Dergelijke interventies worden ook bemoeilijkt omdat tegenstanders op tactisch niveau drones en raketten makkelijk kunnen verschuilen in verstedelijkte gebieden. Tegelijkertijd zal het

46 Christian Brose, 'A New Revolution in Military Affairs. War's Sci-Fi Future', *Foreign Affairs*, mei-juni 2019.

47 Michael O'Hanlon, *Forecasting Change in Military Technology, 2020-2040* (Washington, D.C., Brookings Institution, 2019).

48 Michael Raska, 'The sixth RMA wave. Disruption in Military Affairs?' *Journal of Strategic Studies*, 44 (4) (2020) 456-479. Zie: <https://doi.org/10.1080/01402390.2020.1848818>.

49 Thomas Hammes, *Deglobalization and International Security* (Amhurst, Cambria Press, 2019).

detecteren van deze kleine objecten en uitschakelen ervan juist vanaf veel grotere afstand moeten gebeuren om buiten het bereik van dergelijke lange-afstandswapens te blijven.

Meer conceptueel gezien lijkt het defensief dominant te worden ten opzichte van het offensief ten gevolge van *the return of mass*: de geringe kosten van raket- en dronesystemen maken het mogelijk om met grote aantallen tegelijk westerse schaarse en dure verdedigende systemen te verzadigen. Er ontstaat een asymmetrische attritie-acceptatie: anders dan de tegenstander die duizenden goedkope systemen kan inzetten en verliezen kan het Westen attritie van complexe dure wapensystemen niet lang kan volhouden noch politiek accepteren. Oorlog wordt, met het toenemende arsenaal aan *remote killing*-capaciteiten, abstracter, klinisch, en met wellicht een geringer risico voor verlies aan eigen troepen. Militair geweld wordt daardoor waarschijnlijk lichtzinniger en sneller ingezet. Die wetenschap zal er toe leiden dat meerdere actoren kiezen voor asymmetrische strijdmethoden, zo nodig tegen de burgerbevolking van een tegenstander.

Dreigende destabilisatie

Destabilisatie is een grote zorg. Vijandelijke actoren kunnen middels hard- en soft-cyber-aanvallen percepties beïnvloeden, desinformatie verspreiden en kritieke infrastructuur saboteren,

en zodoende westerse maatschappijen ontwrichten. Daarnaast kan het militariseren van *dual-use* technologieën vergaande gevolgen hebben. De vrees dat een behaalde militaire voorsprong wordt verloren of dat technologie opposenten asymmetrische voordelen zal bieden kan leiden tot agressie en preventieve aanvallen. Doordat onzekerheid heerst kunnen foute interpretaties van acties van een rivaal en overdreven dreigingspercepties, gekoppeld aan vertrouwen in eigen militair vermogen, leiden tot escalatie en oorlog. Ook op nucleair gebied stijgt dit risico. Preventieve aanvallen worden aantrekkelijker, en dus waarschijnlijker, wanneer de indruk ontstaat dat een tegenstander de capaciteiten heeft en dreigt te verkrijgen om met de nieuwe middelen zowel een 'first' als 'second strike' capaciteit uit te schakelen.

Destabilisering wordt ook in de hand gewerkt doordat er geen of nauwelijks mogelijkheden zijn tot normering en wapenbeheersings-overeenkomsten. Dit is het gevolg van het toenemende aantal actoren dat toegang heeft tot nieuwe technologieën en het dual-use-karakter daarvan. Ook het tempo van de ontwikkelingen speelt een rol. Staten kunnen met verrassende ontwikkelingen geconfronteerd worden en zullen moeite hebben het innovatietempo bij te benen. Al met al betekent dit dat traditionele statelijke instituten die regelgeving ontwikkelen en de naleving ervan handhaven aan invloed zullen inboeten.

Er worden ook nuances geuit. Ten aanzien van drones en AWS wordt onderkend dat de lage kosten, de massaliteit en de toegenomen transparantie op het gevechtssveld waardevolle kenmerken zijn, maar verschillende factoren kunnen de voordelen juist reduceren. Ten eerste kan door de proliferatie snel pariteit ontstaan op het slagveld zodat er geen sprake meer zal zijn van een asymmetrisch voordeel. Ten tweede worden steeds effectievere counter-drone systemen ontwikkeld en ingevoerd. Ten derde wordt verwacht dat, naarmate drones meer reikwijdte en effectieve lading krijgen, zij ook groter zullen worden en daardoor zich zullen gedragen als gewone vliegtuigen en kruisraket-

Traditionele statelijke instituten die regelgeving ontwikkelen en de naleving ervan handhaven zullen aan invloed inboeten

ten. De snelheid zal daarbij relatief beperkt zijn. Zij zullen dan ook kwetsbaar zijn voor bestaande luchtverdedigingssystemen. Het is daarom maar de vraag of drones iets betekenen voor de balans tussen offensief en defensief.⁵⁰ Ook ten aanzien van de destabiliserende werking van hypersonische wapensystemen bestaan twijfels. Wanneer beide rivalen beschikken over dergelijke capaciteiten zal er zeer waarschijnlijk weer sprake zijn van pariteit. Deterrence stability wordt daardoor niet aangetast.⁵¹ Wat betreft AI en andere data-gerelateerde ontwikkelingen bestaat er nog te weinig empirisch materiaal verkregen uit experimenten of daadwerkelijke inzet onder operationele omstandigheden.

Technologie in context: een kleurrijk palet aan verwachtingen over de toekomst van oorlog

Tot aan de winter van 2022 deed op basis van deze verwachte technologische en geopolitieke ontwikkelingen, in combinatie met de recente operationele ervaringen, een waaier van toekomstbeelden de ronde over veiligheidspolitieke dreigingen en verwachte operationele contexten waar westerse krijgsmachten mee te maken zouden krijgen. Deze context wordt bepaald door het type actor (statelijk of niet-staatelijk), strijdmethode (regulier of irregulier) en de locatie van verwachte conflicten.⁵²

Eén visie ziet een toekomst vol met 'sophisticated barbarism' en irreguliere oorlogvoering. Een toekomst met conflicten waarin gewelddadige niet-staatelijke actoren de boventoon voeren. Volgens auteurs zoals Hammes, Kilcullen, Jones en McFate zullen deze groeperingen, zoals hierboven aangestipt, in toenemende mate in staat zijn om ook westerse landen schade toe te brengen via cyberaanvallen, diverse soft-cyber-beïnvloedingsmethoden, de inzet van grote aantallen raketsystemen en drones. Het strijdveld zal steeds vaker de stad zijn, een omgeving waarin het moeilijk opereren is voor westerse militairen. Een 'durable disorder' zal het gevolg zijn, aldus Sean McFate.⁵³ Dit betekent voor westerse krijgsmachten nadruk op langdurige inzet in instabiele regio's bij counterinsurgency en counter-terrorisme acties.⁵⁴ Deze zal vooral bestaan uit SOF, training van *proxy forces*, verkenningsmiddelen die in staat zijn langdurig gebieden te observeren, en bewapende drones.⁵⁵

Surrogate Warfare dus: oorlog voeren met minimale fysieke presentie en dus minimaal politiek risico voor het Westen.⁵⁶

Anderen richten zich juist op de geopolitieke rivaliteit tussen de VS (met Europa), Rusland en China. Hier worden langdurige ondermijnende activiteiten verwacht die schuil gaan onder labels zoals hybride dreigingen, *total warfare*, *political warfare* en *gray-zone warfare*.⁵⁷ Ze omvatten economische spionage via cyberaanvallen, economische sancties en *financial warfare*, en intimidatie en corrumperen van politici.⁵⁸ Het is Cool War of Soft War⁵⁹ waarin *troll armies* vanuit Rusland en China beïnvloedingsoperaties uitvoeren via coole social media inclusief de verspreiding van *fake news*.⁶⁰ Hackers, troll armies, tech-bedrijven, media-organisaties, banken, kenniscentra en energie-leveranciers spelen alle een rol.^{61,62}

50 Michael Horowitz e.a., 'Separating facts from fiction in the debate on drone proliferation', *International Security*, 41 (2) (2016) 7-42.

51 *Emerging Military Technologies. Background and Issues for Congress Updated* (Washington, D.C., CRS Report, 10 november 2020).

52 Deze sectie is mede gebaseerd op Frans Osinga, 'Visions on Future War. The War in Ukraine as Litmus Test', *Militaire Spectator* 193 (2024) (2) 99-107.

53 Sean McFate, op cit.

54 Seth Jones, 'The Future of Warfare is Irregular', *The National Interest* (26 augustus 2018).

55 Daniel Byman, 'Why States are Turning to Proxy War', *The National Interest* (26 augustus 2018).

56 Andreas Krieg en Jean-Marc Rickli, 'Surrogate warfare. The art of war in the 21st century?', *Defence Studies* (2018); Thomas Waldman (2019) *Strategic Narratives and US Surrogate Warfare*, *Survival*, 61:1, 161-178

57 Michael Mazarr e.a., *What Deters and Why* (Santa Monica, RAND, 2018); King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica, RAND, 2018); Michael C. McCarthy e.a., *Detering Russia In The Gray Zone* (U.S. Army SSI, maart 2019); Gregory Treverton e.a., *Addressing Hybrid Threats* (Swedish Defence University, 2018); Alina Polyakova en Spencer Boyer, *The Future Of Political Warfare. Russia, The West, and the Coming Age Of Global Digital Competition* (Washington, D.C., Brookings Institution, 2017).

58 Todd Helmus, e.a., *Media Influence Understanding Russian Propaganda in Eastern Europe* (Santa Monica, RAND, 2018); Michael Mazarr e.a., *Hostile Social Manipulation Present Realities and Emerging Trends* (Santa Monica, RAND, 2019).

59 David Rothkopf, 'The Cool War', *Foreign Policy* (20 februari 2013); Noah Feldman, *Cool War. The Future of Global Competition* (New York, Random House, 2013).

60 Peter Singer, *LikeWar. The Weaponization of Social Media* (Boston, Eamon Dolan, 2018).

61 Elie Perot, 'The Blurring of War and Peace', *Survival*, Vol. 61, No.2 2019) 101-110

62 Sean Monaghan (red.), *Countering Hybrid Warfare* (Shrivenham, DCDC, 2018); Lyle Morris e.a., *Gaining Competitive Advantage in the Gray Zone, Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, RAND, 2019); Linda Robinson e.a., *Modern Political Warfare. Current Practices and Possible Responses* (Santa Monica, RAND, 2018); Elizabeth Troeder, *A Whole-Of-Government Approach To Gray Zone Warfare* (Carlisle Barracks, U.S. Army SSI, 2019).

De meest vergaande visies vrezen de terugkeer van grootschalige oorlog.⁶³ Niet *AirLand Battle* maar *Multi Domain Battle* beschrijft de gecoördineerde inzet van middelen in de vijf operationele domeinen,⁶⁴ en middels *Cross Domain Deterrence* – een combinatie van militaire en niet militaire middelen, kinetische acties, economische maatregelen, en informationele methoden – wordt effectieve afschrikking nagestreefd.⁶⁵ Zwermen van drones en AWS zullen worden ingezet en dit zal een impuls geven tot de ontwikkeling van verdedigingsmiddelen op het gebied van onder meer elektromagnetische pulssystemen en geavanceerde EOV-capaciteiten. Hypersonische wapensystemen zullen hun intrede doen.

AI analyseert grote hoeveelheden data die door een netwerk van commerciële en militaire sensoren en satellieten worden gegenereerd. AI en quantum computing versnellen besluitvorming, en geven middels simulaties inzicht in de merites van militaire opties en de timing van inzet van wapensystemen, inclusief de lancering van een antisatellietwapen.⁶⁶ Oorlog zal een ongekend hoog tempo kennen. De toekomst is *hyperwar*.⁶⁷

Het Europese perspectief: politieke inertie

De geopolitieke schok van 2014 dwong ook Europa, samen met de VS, de confrontatie met andere grootmachten weer te verdisconteren in veiligheids- en defensiebeleid. De VS, met zorg kijkend naar de afbrokkelende militaire superioriteit, investeerde in EDT's. Europese landen deelden dezelfde zorgen, verkenden nieuwe technologieën, en publiceerden gedegen studies met aanbevelingen om de Russische militaire dreiging na 2014 te pareren. In 2016 publiceert de EU een waarschuwendende nieuwe veiligheidspolitieke visie waarin zij stelt dat Europa geconfronteerd wordt met existentiële dreigingen. Europa moet, in het licht van hybride dreigingen, weerbaar worden en ook militair zelfstandiger (een reflectie van de veranderende trans-Atlantische relatie onder de eerste regering-Trump). De A2/AD-problematiek staat centraal en met name de problemen van het Westen op het gebied van lucht- en raketverdediging. Herstel vereist investeringen zodat er weer een gelaagd en geïntegreerd verdedigingsstelsel ontstaat, en capaciteiten om de Russische luchtafweermiddelen offensief te neutraliseren, zoals middelen voor elektronische oorlogvoering, kruisraketten, SEAD-munitie en meer stealthy gevechtsvliegtuigen.⁶⁸ Deze debatten en verwachtingen vinden ook in Nederland hun reflectie in de jaarlijkse strategische monitors die HCSS en Clingendael publiceren. Deze wijzen sinds 2014 op de destabiliserende geopolitieke tendensen, de toenemende defensie-uitgaven in Rusland en China en de stagnatie daarvan in Europa. De WRR volgt in 2017 en in 2018 informeert het Nederlandse ministerie van Defensie het parlement dat de Russische modernisering betekent dat de NAVO niet meer kan vertrouwen

63 Michael Mandelbaum, 'Is Major War Still Obsolete?', *Survival*, Vol. 61, No. 5 (2019) 65-71; Michael Mandelbaum, *The Rise and Fall of Peace on Earth* (New York, Oxford University Press, 2019).

64 Daniel Fiott, 'A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap', *Journal of Strategic Studies*, Vol. 40, No. 3 (2017) 417-437; Kevin Woods en Thomas Greenwood, 'Multidomain Battle Time for a Campaign of Joint Experimentation', *Joint Forces Quarterly* 88 (1st Quarter 2018) 14-21; David Perkins en James Holmes, 'Multidomain Battle. Converging Concepts Toward a Joint Solution', *Joint Forces Quarterly* 88 (1st Quarter 2018) 54-57; David Perkins, 'Multi-Domain Battle Driving Change to Win in the Future', *Military Review* (juli-augustus 2017) 6-12; *Multi-Domain Battle. Evolution of Combined Arms for the 21st Century* (US Army TRADOC, Carlisle Barracks, 2018); David Johnson, *Shared Problems, The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle* (Santa Monica, RAND, 2018).

65 King Mallory, *New Challenges in Cross-Domain Deterrence* (Santa Monica, RAND, 2018).

66 Kenneth Payne, *Strategy, Evolution and War, From Apes to Artificial Intelligence*, (Washington, D.C., Georgetown University Press, 2018); Paul Scharre, 'The Real Danger of an AI Arms Race', *Foreign Affairs*, (mei/juni 2019) 135-144; Robert Latiffe, *Future War. Preparing for the New Global Battlefield* (New York, Vintage Books, 2017).

67 Amir Husain e.a., *Hyperwar. Conflict and Competition in the AI Century* (Austin, SparkCognition Press, 2018); Mick Ryan, *War Transformed. The Future of Twenty-First-Century Great Power Competition and Conflict* (Annapolis, U.S. Naval Institute Press, 2022); David Patraeus en Andrew Roberts, *Conflict. The Evolution of Warfare from 1945 to Ukraine*, (Londen, Willam Collins, 2023).

68 Het investeringsniveau blijft, ondanks waarschuwendende rapporten, in Europese landen echter achter bij de ambitie. Zie: Stephan Frühling en Guillaume Lasconjarias, 'NATO, A2/AD and the Kaliningrad Challenge', *Survival*, 58:2 (2016) 95-116; Alexander Lanoszka en Michael Hunzeker, 'Confronting the Anti-Access/Area Denial and Precision Strike Challenge in the Baltic Region', *The RUSI Journal*, 161:5 (2016) 12-18; Fabrice Pothier, 'An Area-Access Strategy for NATO', *Survival*, 59:3 (2017) 73-80; Richard Hooker, *How to Defend the Baltic States* (Washington, D.C., The Jamestown Foundation, 2019); Billy Fabian e.a., *Strengthening the Defense of Nato's Eastern Frontier* (Washington, D.C., Center For Strategic And Budgetary Assessments, 2019); Paul van Hooft en Lotje Boswinkel, *Surviving the Deadly Skies. Integrated Air and Missile Defence 2021-2035* (Den Haag, HCSS, 2021); Wayne Schroeder, *NATO at seventy. Filling NATO's critical defense-capability gaps*, Atlantic Council (4 april 2016). Zie: <https://www.atlanticcouncil.org/in-depth-research-reports/report/nato-at-seventy-filling-nato-s-critical-defense-capability-gaps/>.

op westerse militaire superioriteit, zeker wanneer de steun van de VS niet meer gegarandeerd lijkt te zijn. De Nederlandse krijgsmacht-delen nemen deze ontwikkelingen ter harte en publiceren toekomstvisies vol innovatie-aspiraties waarin stand-off wapens, sensoren, netwerken, big data, en robotica een prominente rol spelen. De realiteit in Europa is echter dat de geringe defensie-uitgaven weinig ruimte bieden om daadwerkelijk te investeren in de militaire modernisering en EDT's. Ook vertragen maatschappelijke debatten rond onder meer drones en AI het aannemen ervan.

In Europa wordt ook veel minder dan in de VS gesproken over een mogelijke RMA. De RMA van de jaren 90 werd geconstateerd *nadat* de contouren – en de strategische en operationele voordelen – duidelijk werden tijdens Desert Storm. De Amerikaanse krijgsmacht zette bewust gericht in op technologieën om die RMA verder te exploiteren. Vanuit het Amerikaanse perspectief waren operaties Enduring Freedom en Iraqi Freedom de validering van dit beleid. De VS was onbetwist meester in de traditionele domeinen. Stealth-technologie, kruisraketten, een groeiend en evoluerend arsenaal aan accurate munitie met meerdere typen geleidingsmechanismen en toenemend bereik, datalinks en de digitalisering van commando-voering processen, het zijn enkele militaire technologische trends die de VS deze dominantie verschafte. Een hoog operationeel tempo, accuratesse, escalatie-dominantie en risicoreductie werden de kenmerken van de New American Way of War, een nieuwe manier van optreden die voorafgaande aan Desert Storm niet voor mogelijk was gehouden.

Europa was minder overtuigd van ofwel de effectiviteit, dan wel de noodzaak in het post-Koude Oorlog tijdperk en deinsde ook terug voor de kosten gemoeid met investeringen in *high end*-capaciteiten die vooral geschikt leken voor grootschalige interstatelijke oorlogvoering, een scenario dat onwaarschijnlijk werd geacht. De interventies in de Balkan demonstreerden al de misvatting daarvan, en na 9/11 benadrukten de langdurige stabilisatiemissie en de COIN en counter-terrorisme operaties in Afghanistan dit nogmaals. Dalende defensie-uitgaven leidden er echter toe dat omarming van de nieuwe

Het discours in Europa is voornamelijk gericht op ethische en juridische schaduwzijden van specifieke potentiële technologieën

technologieën langzaam verliep en bestond uit geleidelijke vervanging van oudere systemen. Dit werd niet gekoppeld aan een bewuste ontwikkeling van een New Way of War.

En hoewel het veiligheidsbeleid van Europese landen sinds 2014 getuigt van het besef dat een er een paradigmaverschuiving is opgetreden te midden van versnellende technologische ontwikkelingen die forse investeringen in hoogwaardige defensiecapaciteiten vereisen, wordt weinig gerept van een mogelijke RMA. Dat is voornamelijk een Amerikaans thema en waar het in Europa ter sprake komt, is dit in denktanks en binnen beperkte kringen van academici. Het discours in Europa is, ondanks diverse *technology trend*-rapporten en waarschuwendes studies van de NAVO en de EU, voornamelijk gericht op ethische en juridische schaduwzijden van specifieke potentiële technologieën. En anders dan in de jaren 90 is er tot februari 2022 slechts weinig empirisch materiaal dat de stellingen over een op handen zijnde RMA kan onderbouwen. Grootschalige oorlog op Europees grondgebied lijkt voor vele Europese regeringen nog steeds onwaarschijnlijk, getuige ook het feit dat slechts zes van de 29 EU-lidstaten, acht jaar na de annexatie van de Krim, de 2-procentnorm heeft gehaald.⁶⁹ Een scepsis die voortduurt tot 24 februari 2022. ■

69 Zie: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf.