Schrijftalent gezocht!

In deze Militaire Spectator is plaats gemaakt voor twee gastcolumns. M. Schaake gaat in op digitale vrijheid en cybersecurity,terwijl T. Burgers pleit voor een breder debat over de Digital and Robotic Revolution in Military Affairs.
De redactie van de Militaire Spectator daagt ook andere lezers uit om een gastcolumn te schrijven. Het thema is vrij, maar moet passen binnen de formule van het tijdschrift. De boodschap moet relevant zijn voor de lezers. Het moet gaan om een gefundeerde eigen mening, om een logisch opgebouwd betoog en de feiten moeten kloppen en verifieerbaar zijn. Een bijdrage mag maximaal duizend woorden tellen. U kunt uw gastcolumn sturen naar de bureauredactie (zie colofon). De redactie wacht uw bijdrage met belangstelling af.

De hoofdredacteur

Defensie in een online verbonden wereld

*M. Schaake**

Waar lange tijd het wapenarsenaal en aantal troepen een graadmeter voor de kracht van een leger leek, wordt weerbaarheid tegenwoordig gemeten aan de mate waarin digitale vrijheid, of cyber-security, kan worden gewaarborgd.
Technologie leidt tot nieuwe vragen over vrede, vrijheid en veiligheid, en raakt bijna elk aspect van onze samenleving. Maar de nieuwe digitale realiteit wordt nog te veel in militaire termen benaderd, terwijl een civiele aanpak ook essentieel is. In beleid ontbreken essentiële maatregelen om Europese belangen veilig te stellen. Zo moeten we de hand in Europese boezem steken en ervoor zorgen dat digitale wapens niet zonder controle worden geëxporteerd naar landen die mensenrechten schenden of onze strategische positie willen ondermijnen.

De Amerikaanse minister van Defensie waarschuwde vorig jaar voor een 'cyber-Pearl Harbor' en er wordt steeds vaker gesproken van een cyber-Koude Oorlog, waarbij het epicentrum niet langer in Moskou, maar in Azië ligt. Dergelijke zware metaforen worden regelmatig gebruikt om de omvang van de dreiging van cyber-aanvallen aan te geven. Ook lijken ze bedoeld om de zwaarst mogelijke reactie te legitimeren. Een cyber-wapenwedloop dreigt, terwijl de juridische kaders nog onduidelijk zijn.

Zowel de NAVO als de verschillende lidstaten zoeken naar doctrines waarin het mandaat voor offensieve capaciteit, maar ook cyber-defensie moet passen. Dat is niet eenvoudig. Zo is het heel lastig om met zekerheid vast te stellen wie een cyber-aanval heeft uitgevoerd; een regering, *hackers* of een terroristische organisatie, of via de computers van mensen die niet weten dat hun computer is geïnfecteerd.
Dat maakt het antwoord op de vraag wat een juiste respons zou zijn dan ook niet evident. De NAVO heeft bijvoorbeeld nog niet besloten of artikel 5 van het Verdrag van Washington ook geldt voor cyber-aanvallen. Over de vraag of cyber-aanvallen met kinetische wapens mogen worden beantwoord, is de politieke discussie nog niet eens volwassen. De EU presen-

* De auteur is Europarlementariër voor D66 en lid van de commissie Buitenlandse Zaken en Internationale Handel. Ze schreef de eerste strategie voor digitale vrijheid in het buitenlandbeleid van de EU.

teerde een cyber-security strategie, maar ze ontweek deze cruciale vraag. Hoe preventie eruit ziet en of preventieve aanvallen daarbij passen, is onderwerp van debat en speculatie. Een bekend voorbeeld van zo'n preventieve cyber-aanval was Stuxnet, waarvan men aanneemt dat de VS en Israël via dit virus het Iraanse atoomprogramma aanvielen.

Steeds meer landen hebben een 'elektronisch leger'. In Syrië wordt dat ingezet om dissidenten op te sporen of om de bevolking te onderdrukken, maar ook voor aanvallen op online doelen van tegenstanders. Verschillende westerse media werden door het Syrisch elektronische leger gehackt. In China is online surveillance een bloeiende industrie: honderdduizenden Chinezen verdienen hun brood met het controleren waar hun medemens online gaat en staat. Activistenbewegingen als Anonymous zijn nieuwe spelers op het wereldtoneel, onvoorspelbaar en grillig, maar ze kunnen ook rekenen op een brede maatschappelijke sympathie.

Nieuwe digitale technologieën leiden gelukkig niet alleen tot vragen over veiligheid en defensie, maar zorgen wereldwijd ook voor veranderingen binnen samenlevingen. Veel van die veranderingen zijn positief en gaan over ontwikkeling, individuele vrijheid, ontplooiing, economische kansen, het delen van kennis of het eenvoudiger maken van diensten. Met behulp van nieuwe technologieën is het voor individuen gemakkelijker om hun mensenrechten, zoals vrije expressie of toegang tot informatie, op te eisen. Ook worden met behulp van mobiele telefoons schendingen van mensenrechten vastgelegd en gedeeld. De wereld is met één druk op de knop ooggetuige van oorlogen.
Een constante factor in de discussies over digitale vrijheid en cyber-security is dat de traditionele concepten van jurisdictie, gevestigd in de natiestaat en de zwaardmacht van de staat, niet langer gelden. Grote delen van onze kritieke infrastructuur zijn in private handen. De wederkerige relatie tussen soevereine staten en de online grenzeloosheid leidt zowel tot kansen als bedreigingen. Toch overlappen publieke en private belangen niet altijd.

Waar er enerzijds macht van regeringen naar individuen vloeit, zijn het vooral bedrijven die steeds meer invloed krijgen. Ze hebben een ongekend invloedrijke positie op het internet. In deze verbonden wereld worden bedrijven zelf ook steeds vaker geconfronteerd met vragen die voorheen alleen aan diplomaten of overheden waren voorbehouden. Toen de video *The Innocence of Muslims* in verschillende landen leidde tot gewelddadige demonstraties, vroeg het Witte Huis aan Google om deze video van haar dienst *YouTube* af te halen. Tegelijkertijd wil het Amerikaanse ministerie van Buitenlandse Zaken juist niet dat de digitale vrijheid van mensen wordt beperkt door censuur.

Terwijl de technologie zich razendsnel ontwikkelt, lopen wet- en regelgeving en veiligheidsdoctrines achter. Als die niet worden aangepast aan een online verbonden realiteit, verliezen we relevantie en geloofwaardigheid. Om te beginnen moet de EU-regelgeving over de export van de meest agressieve technologieën worden aangescherpt. Massasurveillance, massacensuur, maar ook hackingtechnologie of kwetsbaarheden in veelgebruikte software worden momenteel zonder toezicht verhandeld. Dat staat in schril contrast met de bescherming die de EU handhaaft als het gaat om producten als speelgoed, voedingsmiddelen en chemicaliën. Het heeft weinig zin om cyber-verdediging te versterken terwijl vijandelijke spelers hun producten kopen van Europese bedrijven. Deze digitale wapenhandel moet stoppen. We moeten dit gat snel dichten en die verantwoordelijkheid ligt niet alleen bij defensie. Politiek leiderschap en maatschappelijke betrokkenheid zijn onmisbaar.

Omdat in principe ieder mens ter wereld nieuwe technologieën kan gebruiken, moet de verdediging van open internet en van kritieke informatie-infrastructuur een gedeelde verantwoordelijkheid zijn van overheid, bedrijfsleven en de maatschappij als geheel. Afspraken over democratische controle moeten helder worden gemaakt. Metaforen over een cyber-Koude Oorlog wekken te gemakkelijk de suggestie dat defensie alléén kan zorgen voor digitale vrede en veiligheid. ■

Meer dan killer robots? Alternatieve toepassingen voor gerobotiseerde (wapen)systemen

T.J. Burgers

Een analyse van zowel het Nederlandse als het internationale debat van het laatste decennium over de *Digital and Robotic Revolution in Military Affairs* (DRRMA), leert dat de discussie gedomineerd wordt door mogelijke offensieve toepassingen van *remotely piloted aircraft* (RPA): gerobotiseerde vliegende (wapen)systemen.
In het bijzonder de inzet van unmanned *combat aerial vehicles* (UCAV's) – onder een breder publiek beter bekend als bewapende *drones* – bepaalt grotendeels de richting van het debat.[1]

Hoewel Israël deze UCAV's al gebruikt heeft bij conflicten, riep de inzet van dergelijke toestellen in de oorlogen in Afghanistan en Irak – waar deze wapensystemen op grote schaal werden ingezet – vragen op over de ethische en juridische implicaties. Het debat werd ook nog eens verhevigd door de controversiële *targeted killing*-campagne van de CIA in Pakistan, Jemen en Somalië, om met gewapende UCAV's mogelijke terroristen uit te schakelen.
Deze aanvallen waren vaak gebaseerd op uiterst minimaal en veelal discutabel verkregen bewijs en vonden plaats buiten elke vorm van internationaal recht.[2] Deze uiterst omstreden campagne domineert sindsdien grotendeels de discussie over de inzet van gerobotiseerde vliegende wapensystemen. Deze eenzijdige focus heeft negatieve implicaties voor het bredere debat over de DRRMA. De controverse over de campagne van de CIA leidt ertoe dat de algemene ontwikkeling van de DRRMA, zoals bijvoorbeeld de inzet van RPA's in conventionele oorlogvoering, met steeds meer scepsis bekeken wordt.
Niet alleen in het publieke debat zijn RPA's inmiddels een controversieel thema, ook onder verantwoordelijke politici en internationale organisaties is vanwege de CIA-campagne een grote scepsis ten opzichte van de DRRMA ontstaan.[3] Hoewel president Obama recentelijk aankondigde de CIA-campagnes te zullen herzien vanwege de maatschappelijke kritiek en omdat er twijfel is over de effectiviteit, kunnen we voorspellen dat de controverse rondom de inzet van (gewapende) RPA's zal aanhouden.
De aanvallen gaan immers nog steeds door en het ziet er zodoende naar uit dat het gewapende RPA de komende tijd het *weapon of choice* voor de Verenigde Staten blijft.[4] Daardoor valt het te betwijfelen of het debat over de ontwik-

1 Ook de term Remotely Piloted Vehicle (RPV) wordt gebruikt. Dit is de officiële term bij de meeste luchtmachten.

2 In het bijzonder de signature strikes, waarin mogelijke doelwitten werden geïdentificeerd en aangevallen na analyse van mogelijke gedragspatronen, leidden tot de nodige controverse omdat de CIA in veel gevallen de definitie voor mogelijke doelwitten bijzonder ruim interpreteerde; elke mannelijke persoon in de leeftijd tussen 18 en 65 in de regio waar al-Qaida en aanverwante organisaties actief zijn is een mogelijk doelwit. Voor een verdere evaluatie van de drone strikes zie: Micah Zenko, Reforming US Drone Strike Policies (Council on Foreign Relations Special Report, No 65).

3 www.ipsnews.net/2013/02/drone-a-dirty-word-in-the-u-n-lexicon.

4 Het spectrum van mogelijkheden die de regering-Obama heeft om terroristische netwerken in Pakistan, Jemen en Somalië te bestrijden is relatief gering. In dit spectrum blijven drones naar alle waarschijnlijkheid het weapon of choice: het (politieke) risico is een stuk lager vergeleken met de inzet van grondtroepen – de andere meest voordehand liggende optie. Daarnaast zijn drones relatief goedkoop en hebben ze de afgelopen jaren hun effectiviteit aangetoond, want al-Qaida is er als organisatie door gedicimeerd. Voor verdere informatie zie ook: www.foreignaffairs.com/articles/139453/daniel-byman/why-drones-work en www.foreignpolicy.com/articles/2013/05/24/indispensible_weapon_drones_obama?page=full.

keling van de DRRMA in de komende maanden en jaren ruimer gevoerd gaat worden. En dat is te betreuren, omdat er wel degelijk alternatieve applicaties van de DRRMA mogelijk zijn en zelfs al gebruikt worden, maar deze blijven onderbelicht in het huidige debat. Nu is bijvoorbeeld de inzet van RPA's voor surveillance en inlichtingen niet nieuw. De Predator – misschien wel de icoon onder de drones – werd voor deze taken al operationeel ingezet in Bosnië in 1995.
Sindsdien zijn drones frequent ingezet – zowel onbewapend als bewapend[5] – maar in bijna alle gevallen ter ondersteuning van conventionele militaire missies.

Het spectrum van mogelijke toepassingen zou echter geografisch, dimensionaal en inhoudelijk verbreed moeten worden. Een goed voorbeeld hiervan is de inzet van de eerste RPA's in de MONUC-missie in Congo en de missies in Tsjaad en Libanon, waar RPA's de potentiële meerwaarde van de inzet van gerobotiseerde systemen in onconventionele (militaire) operaties aantoonden. Verder kunnen gerobotiseerde systemen niet alleen op het gebied van vredesoperaties een 'revolutie' op gang brengen; ook in de humanitaire sector zou dit mogelijk zijn. Want als bijvoorbeeld Amerikaanse mariniers in afgelegen gebieden in Afghanistan logistiek bevoorraad kunnen worden door onbewapende K-MAX robothelikopters, zou dit ook mogelijk moeten zijn voor afgelegen gebieden waar humanitaire organisaties hulp leveren of dat proberen. Helikopter-RPA's zoals de K-MAX zouden uitstekend geschikt zijn voor dergelijke 'dangerous, dirty and by time routine' humanitaire taken. Een bijkomend voordeel is dat er minder levensgevaar dreigt voor bemanningen en dat de inzet van onbemande helikopters economischer lijkt dan de inzet van bemande toestellen. Daarom moeten de academische en militaire gemeenschap hun invloed aanwenden om te zorgen dat het debat in de komende jaren weer verbreed wordt. Mede gelet op hun technologische voorsprong en expertise op dit gebied zouden de Verenigde Naties en ook Europese landen hierin het voortouw kunnen nemen. Mijn inziens levert dit een win-win situatie op waarin westerse landen wederom op grotere schaal betrokken worden bij vredesoperaties en waarin de VN de effectiviteit van haar vredesoperaties zou kunnen vergroten. Het spreekt voor zich dat bovenstaand scenario in een juridisch en ethisch raamwerk ingebed moet worden. De VN zou hiertoe de aanzet kunnen geven in het kader van haar operaties.

Dat RPA's al succesvol logistiek zijn ingezet in de hedendaagse asymmetrische oorlogvoering toont aan dat de potentiële meerwaarde van de DRRMA niet enkel beperkt is tot kinetische taken in een conventionele oorlogvoering.

Het debat over de *digital and robotic revolution in military affairs* moet breder zijn dan alleen de inzet van gewapende drones

Ook op andere gebieden kan de DRRMA voor een 'revolutie' zorgen door alternatieve toepassingen en inzetmogelijkheden. Gezien de duidelijke meerwaarde van zulke alternatieve applicaties is een breder debat niet alleen wenselijk, maar noodzakelijk. Daarom pleit ik voor diepgaand(er) onderzoek naar de alternatieve toepassingen van RPA's en in een breder verband van de DRRMA. Een onderzoek en een debat dat zich niet enkel richt op de CIA-campagnes en *killer robots*, maar waarin alle mogelijke applicaties van *remotely-piloted systems* in alle typen militaire en niet-militaire missies onderzocht worden. Het is duidelijk dat de DRRMA humanitaire meerwaarde heeft en vanuit dat oogpunt de volle aandacht verdient. ■

5 In de oorlog in Afghanistan werden gewapende drones voor het eerst ingezet. Zie ook Frank Morring Jr., 'Blame Game', in: *Aviation Week & Space Technology* (maart 2004).
6 http://articles.washingtonpost.com/2013-01-08/world/36210223_1_laboratory-for-intelligence-devices-surveillance-drones-peacekeeping-missions.
7 Zie: www.washingtontimes.com/news/2013/may/7/us-marines-employ-drone-copters-afghan-war.
8 Idem.