Schrijftalent gezocht!

In deze uitgave is plaats gemaakt voor drie gastcolumns. De redactie daagt andere lezers uit om ook een column te schrijven voor de Militaire Spectator. De keuze van het thema is vrij, maar het moet wel passen binnen de formule van het blad. Voorwaarde voor plaatsing is dat de redactie uw boodschap relevant acht voor de lezers. Verder moet uw verhaal in niet meer dan duizend woorden voor het voetlicht worden gebracht.

U kunt uw bijdrage sturen naar de bureauredactie (zie colofon). Wij zijn erg benieuwd wie zich geroepen voelt om te reageren. Uiteraard zijn we ook nieuwsgierig naar de thema's die u onder de aandacht van de lezers wilt brengen. Uw bijdrage wachten we dan ook met belangstelling af.

De hoofdredacteur

Defensie moet zich houden aan de nationale milieudoelstellingen

...maar doet dat nu niet

KTZT bd M. Hendriks Vettehen – voorzitter Defensie Kennisnetwerk Energie

Het kabinet-Rutte heeft de Europese milieudoelstellingen overgenomen. In 2020 moet onder meer de CO_2-uitstoot 20 procent lager zijn dan in 1990. De maatregelen hebben tot doel de temperatuurstijging aan het eind van deze eeuw te beperken tot maximaal twee graden. Het verminderen van de CO_2-uitstoot met 20 procent is een enorme opgave, maar niet onhaalbaar.

Defensie stelt nauwelijks eisen aan het energieverbruik van toekomstig materieel

Het helpt natuurlijk niet wanneer sommige sectoren van die verplichting worden ontheven. Dat het ministerie van Defensie zo'n ontheffing heeft voor het operationele deel van de organisatie is ogenschijnlijk verdedigbaar. Het beschikbare materieel is immers niet eenvoudig aan te passen en de veiligheid van het personeel mag niet onnodig in gevaar worden gebracht.

Defensie lijkt die ontheffing gemakshalve ook maar te betrekken op nieuwe investeringen. Aan nieuw materieel worden nauwelijks eisen gesteld als het gaat om het verminderen van het energieverbruik. Nieuwe wapensystemen zouden in overeenstemming met de nationale milieudoelstellingen gewoon 20 procent minder energie moeten gebruiken dan hun voorgangers. Welke mogelijkheden zijn er? Laten we, bij wijze van gedachte-experiment, naar drie voorbeelden kijken.

Defensie doet onderzoek naar nieuwe oppervlakteschepen die in de toekomst de huidige LCF- en M-fregatten moeten vervangen. Mogelijkheden om minder energie te gebruiken

liggen vooral in een operationeel concept waarbij de maximale snelheid wordt beperkt tot 20 knopen. Een hogere snelheid, zoals die van de huidige fregatten (30 knopen), lijkt tegenwoordig zowel tactisch als strategisch maar beperkte toegevoegde waarde te hebben.

Los van de huidige financiële en/of organisatorische overwegingen om de tanks af te stoten, lijkt de toekomst van dat wapen sowieso twijfelachtig. Ze zijn gewoon te zwaar in een tijdsgewricht waar vloeibare fossiele brandstoffen schaars worden. Om 20 procent minder brandstof te gebruiken moeten nieuwe landsystemen vooral lichter worden dan hun voorgangers. Dat kan alleen door andere vormen van bepantsering en bescherming te ontwikkelen of door deze gedeeltelijk achterwege te laten.

Bij een mogelijke keuze voor de *Joint Strike Fighter* (JSF) als vervanger van de F-16 wordt zelfs een toestel geïntroduceerd dat waarschijnlijk meer brandstof gebruikt dan zijn voorganger. Dat heeft natuurlijk ook consequenties voor de grootte van de tankercapaciteit. In het dossier 'Vervanger F-16' heeft het brandstofverbruik tot nu toe te weinig aandacht gekregen. Wanneer Nederland toch voor de JSF kiest, moeten andere wapensystemen nog energie-efficiënter worden om defensiebreed aan de milieudoelstellingen te voldoen.

Er zijn drie redenen te bedenken op grond waarvan Defensie zich bij nieuwe investeringen zou mogen onttrekken aan de nationale milieudoelstellingen. Als eerste kan worden betoogd dat 'veiligheid' een essentiële waarde is, die niet mag worden gecompromitteerd door (energie)beperkingen. Dat is geen houdbaar argument omdat de energieschaarste niet aan de krijgsmacht voorbij gaat. Bovendien komt die energie voor het overgrote deel uit niet-democratische en instabiele regio's. De veiligheid is meer gebaat bij energiezuinige wapensystemen dan bij energieverslindende wapensystemen.

Het tweede argument is dat fossiele brandstoffen in de toekomst worden vervangen door biobrandstoffen en de energiekwestie zich dan vanzelf oplost. Biobrandstoffen kunnen inderdaad voor een deel de fossiele brandstoffen vervangen, maar in geen enkel toekomstig energiescenario is die vervanging ook maar bij benadering toereikend.

Het derde argument luidt dat Defensie door de verkleining van de krijgsmacht al minder energie gebruikt en daarmee vanzelf aan de nationale milieudoelstelling voldoet. Dit is een twijfelachtige redenering omdat bij oplopende spanningen de aantallen wapensystemen weer toenemen. Juist op het moment dat de energiekrapte nijpend wordt, neemt de energiebehoefte van Defensie meer toe dan nodig door het ontbreken van energie-efficiënte vervangers.

De argumenten om zich te onttrekken aan nationale milieudoelstellingen zijn op zijn best twijfelachtig

Kortom, Defensie moet zich zonder uitzondering committeren aan de nationale milieudoelstellingen. Dat is niet alleen nodig om de gevolgen van klimaatverandering tegen te gaan, maar is ook in het belang van de toekomstige krijgsmacht. Bij nieuwe investeringen moeten nieuwe wapensystemen 20 procent minder energie gebruiken dan hun voorgangers. Nieuwe wapensystemen, hoe geavanceerd en effectief ook, die dat niet kunnen, zijn inmiddels achterhaald. ■

Veelzijdig inzetbaar?

Kolonel drs. P.J.E.J. van den Aker

'… en pas in de laatste plaats in de operationele capaciteiten'. Hoe vaak heeft het personeel van de krijgsmacht deze 'toverformule' vanaf de jaren negentig al gehoord? Vele reorganisaties hebben al plaatsgevonden. Bezuinigingen op de begroting van Defensie zouden in de eerste plaats worden gezocht in de besturing en de bedrijfsvoering van dit overheidsinstituut. Zo ook nu weer. De ambitie blijft evenwel een 'veelzijdig inzetbare krijgsmacht'.

Dit noopt tot het stellen van essentiële vragen. Hoe veelzijdig is een krijgsmacht zonder maritieme patrouillevliegtuigen, mijnenvegers, bevoorraders, tanks, zonder voldoende munitie, kleding, gevechtsuitrusting of reservedelen? Kan zo'n krijgsmacht haar taken nog wel uitvoeren? En kan dat dan ook altijd in het volledige intensiteitsspectrum, onder alle weersomstandigheden en in alle soorten terrein? Hebben we dat wellicht zelf in de hand of moeten we terugvallen op onze bondgenoten? Wie wordt het meest geraakt? Wie is hiervoor verantwoordelijk?

De antwoorden op deze vragen zijn niet eenvoudig te geven, maar laat ik het hier eens proberen. Er blijft nog veel 'bruikbaars' over om te worden ingezet in het kader van onze drie hoofdtaken. De krijgsmacht kan natuurlijk met datgene wat overblijft de meeste taken nog wel uitvoeren. Maar niet meer alle taken! Echt 'vechten om te winnen' lijkt in het allerhoogste geweldsspectrum niet goed meer mogelijk. Escalatiedominantie, *force protection* en slagkracht is met het verdwijnen van de tanks veel minder aanwezig. Daardoor kan Nederland niet altijd meer op eigen kracht deelnemen aan militaire operaties of aan gevechtsacties hoog in het geweldsspectrum. Zie hiervoor onder meer het artikel van De Jonge en Vermeulen in *NRC Handelsblad*.[1] De exacte gevolgen hiervan moeten nog worden uitgewerkt, maar zijn wel al vaak uitgebreid geschetst in de media. Ook de Vaste Commissie voor Defensie van de Tweede Kamer is goed op de hoogte gebracht van de gevolgen, zoals iedereen via internet kort geleden heeft kunnen zien.[2]

Toch is nu al te vrezen dat ten minste Nederlands militaire imago zal verslechteren. De minister van Defensie van de Verenigde Staten Gates hekelde onlangs immers in ongemeen felle bewoordingen de Europese NAVO-partners en 'voorspelde als het bondgenootschap zo zou doorgaan, een sombere, of zelfs deerniswekkende toekomst'.[3] En daarmee neemt de politieke invloed van de Europese landen, waaronder Nederland, af.

De economische effecten daarvan zullen goed merkbaar zijn. De emotionele effecten als gevolg van eventueel grotere verliezen zullen deze economische gevolgen veruit overtreffen. Zelfs onze bondgenoten zullen naar verwachting Nederland niet zomaar te hulp komen. Daar moet voortaan expliciet vooraf om gevraagd worden. Dat moet dan bovendien besproken zijn, en dat kan vrijwel uitsluitend als belangrijke politieke, ambtelijke, economische en militaire belangen parallel lopen. Nog beter is dat dit past in een Europees veiligheids- en defensiebeleid. Maar aangezien dat er nog

1 J.H. de Jonge en J.L. Vermeulen, 'Red onze tanks!' *NRC Handelsblad*. 3 juni 2011, 7.
2 23 Mei jl.
3 J. Eijsvoogel, 'Keiharde boodschap van Gates aan Europa'. *NRC Weekend*. 11-12 juni 2011, 13.

niet is, lijkt het mij aannemelijk dat eenzijdig nationale bezuinigingen – hoe noodzakelijk en onvermijdelijk ook – niet in het belang zijn van Europa. Kortom, van een 'veelzijdig inzetbare krijgsmacht' kan van nu af aan nauwelijks meer sprake zijn!

Wie wordt daardoor het meest geraakt? Dat is zonder twijfel in de eerste plaats ons loyale personeel. Onze militairen en burgers zijn jarenlang bezig geweest zich verder te professionaliseren, zodat zij ieder moment konden worden ingezet in het belang van Nederland, Europa en de rest van de wereld. Zij hebben vanaf de jaren negentig aan de ene na de andere reorganisatie en bezuiniging meegewerkt, en hebben die ook trouw gerealiseerd. Nu lijkt een groot deel van hen opnieuw slachtoffer te worden van één van de grootste opgelegde bezuiniging aller tijden. En het is vaak zo dat juist de 'verkeerde' mensen de krijgsmacht verlaten, met een verlies aan ervaring en wellicht een *'braindrain'* als gevolg. Ten tweede raken de vooral uit financiële overwegingen opgelegde maatregelen de Nederlandse ambities, en dus het Nederlands belang. Nederland zal als grotere economische macht niet meer zo snel met de groten der internationale politiek aan tafel mogen zitten. Dat kost aanzien en, zoals eerder aangegeven, invloed en geld.

Wie is daarvoor verantwoordelijk? Het politiek wenselijk antwoord zou natuurlijk zijn: in eerste instantie de regering en de minister van Defensie, die hiervoor in het parlement een meerderheid achter hun plannen hebben gekregen. Maar helaas straalt die verantwoordelijkheid ook af op de ambtelijke top en de belangrijkste militaire adviseur(s) van de minister: de Commandant der Strijdkrachten, die weer afgaat op de adviezen van de commandanten van de Operationele Commando's. Ook zij gaan de geschiedenis in als 'de mensen die afscheid moesten nemen van doorslaggevende wapensystemen in het hoogste deel van het geweldsspectrum'.

Dat daarnaast extra geïnvesteerd zal worden in *cyberwarfare* is een schrale troost en is bovendien voor de hand liggend. Nu kunnen de hiervoor genoemde functionarissen, of misschien ook anderen, natuurlijk zeggen 'dat het nog veel erger had gekund' of 'dat we door het oog van de naald zijn gekropen'. Natuurlijk, ook bij hen heeft het water tot aan de lippen gestaan. En wellicht zijn zij hierbij ook tegen belangrijke (deel)besluiten geweest, maar dat neemt niet weg dat zij keuzes gemaakt hebben en dat de geschiedenis over hen zal oordelen. Het tekent hen als leiders en mensen met karakter dat ze daarvoor niet zijn weggelopen. Evenzo tekent het de rest van ons militairen en burgers dat ze de genomen besluiten wederom loyaal zullen gaan uitvoeren.

Maar dat men als één van de eerste maatregelen operationele eenheden permanent heeft stilgezet (overigens omdat besturing en bedrijfsvoering niet genoeg opleverden) en dat de krijgsmacht door deze bezuinigingen aan slagkracht heeft ingeboet, laat zien dat er wel degelijk is gesneden in de operationele capaciteiten van die krijgsmacht. Veelzijdig inzetbaar? Ik betwijfel het. ■

Cyberontwikkelingen in vogelvlucht

Maj (R) Ron van Doorn

De FBI heeft de tien meest voorkomende cybercriminelen benoemd, uitgaand van het specialisme van de actoren en de strafbare feiten die ze plegen.[1] Cybercriminelen kunnen hun kennis en vaardigheden inzetten voor cybercrime, cyberspionage of cyberwar. Ik kies echter voor een andere invalshoek, meer gericht op de staatsveiligheid.

Onder aan de ladder staan dan de *sciptkiddies*, pubers die met 'knippen en plakken' gebruikmaken van al bestaande *malware*. Daarna komen de ontwikkelaars van de hack-technologieën en methodes, gevolgd door anoniem samenwerkende personen of groepen die vaak op ad hoc-basis cyberacties uitvoeren. Boven aan de ladder staan staten met offensieve cyberwarfare capaciteiten, waarvan in beginsel de grootste dreiging uitgaat. Er is een speciale groep staat-hackers, interessant vanuit militair oogpunt. Deze hackers vallen uiteen in drie subgroepen: sympathisanten van een staat, die volledig autonoom cyberacties ondernemen richting tegenstanders van de eigen staat; *state-sponsored* hackers, die met enige vorm van (in)directe steun van een staat cyberacties ondernemen richting tegenstanders van die staat; en de laatste subgroep, waarvoor ik nog geen goede term tegengekomen ben, maar die ik de *cyberrunners* noem.

De cyberrunner is een persoon of groep personen die in het geheim, in opdracht van een staat, specialisten en/of groepen inhuurt (runt) om specifieke cyberaanvallen en/of cyberspionage in een andere staat en/of strategische sector uit te voeren, zonder dat er een (onomstotelijke) link of spoor naar de opdrachtgevende staat is. Aanvallen waarbij een cyberrunner is ingezet en waarbij een staat op de achtergrond acteert, zijn er mogelijk al geweest. Een geval is de cyberaanval op Georgië door *StopGeorgia.ru*. Het *Project Grey Goose* heeft onderzoek gedaan naar deze aanval.[2] Hun conclusie is dat er veel lijnen naar de Russische overheid zijn. De inzet van een cyberrunner kan tal van ernstige, internationale juridische complicaties opleveren en uiteindelijk leiden tot een fysieke, militaire vergelding.

Cyberdreigingen

De dreiging van digitale spionage neemt toe en cybercrime wordt ieder jaar geavanceerder en gerichter.[3] Een kleine, willekeurige greep uit een aantal incidenten van de laatste vier maanden toont dat aan. Zo vond een aanval plaats op de EU en diverse ministeriële netwerken in Canada, Frankrijk en Australië. Saillant detail is dat de Australiërs gealarmeerd zijn door de Verenigde Staten. Hoe weten zij dit? Daarnaast was er een grote aanval op een Noors militair computersysteem. Zelfs ICT *security*-bedrijven worden ogenschijnlijk met het grootste gemak gehackt. Deze twijfelachtige eer viel te beurt aan HBGary, Comodo, RSA en Ashampoo.

1 Zie: http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.
2 Project Grey Goose, *Phase I Report* (2008) & Project Grey Goose, *Phase II Report* (2009).
3 Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 (Den Haag, GOVCERT.NL).

Rijksoverheid.nl en Rabobank-internetbankieren gingen plat door een DDoS-aanval. Uitgebreid in het nieuws was de hack van het Sony Playstation-netwerk. Minder bekend is dat er – ik ben de tel kwijt – daarna nog circa acht netwerken van Sony zijn gehackt.

De indruk bestaat dat spionage of pogingen daartoe doorgaans buiten de pers blijven, maar dat er wel degelijk veel activiteiten zijn op dit gebied. De AIVD waarschuwt voor digitale spionage in zijn laatste jaarverslag. Een voorbeeld van cyberspionage is *Night Dragon*, gericht op heimelijke informatievergaring bij energie-multinationals zoals Shell en BP en meer recentelijk bij Lockheed Martin, de bouwer van de JSF.

Advanced Persistent Threat-aanvallen zoals Aurora (2009) en Stuxnet (2010) zijn niet opgemerkt door beveiligingssoftware. Sommige systemen waren langer dan een jaar geïnfecteerd. De aanvaller heeft alle tijd gehad om in het systeem te kijken of sabotage te plegen. Een aanvalstechniek waar nog nauwelijks iets over is geschreven, is hardware met een *backdoor* voor spionage of een aanval, maar dit gaat ongetwijfeld veranderen in de toekomst.

In beginsel is geen enkel systeem, on- of offline, immuun voor een cyberaanval. Het is dan ook niet voor niets dat Debora Plunkett, hoofd *Information Assurance Directorate* van het Amerikaanse *National Security Agency*, eind 2010 bevestigde wat veel beveiligingsexperts al vermoedden: de dienst werkt continu vanuit de veronderstelling dat het eigen netwerk gehackt is.

Bestrijding

Essentieel bij de bestrijding is (inter)nationale samenwerking tussen inlichtingendiensten, militaire cybereenheden en politie. De grote verscheidenheid aan cyberdreigingen en -aanvallen en de gecompliceerde technieken vereisen een uitgebreid palet aan experts om adequaat te kunnen optreden. Het werven en behouden van gekwalificeerd personeel zal een hele uitdaging worden. De VS en veel Europese overheden hebben hier om tal van redenen grote problemen mee. Een *cyber warrior* dient over meer vaardigheden te beschikken dan alleen goede analytische eigenschappen, die van belang zijn bij inlichtingendiensten. Eigenschappen als *out of the box*-denken, creatief, vastberaden, inlevingsvermogen en geduld horen eerder bij een opsporingsambtenaar dan bij een militair. Hackers beschikken over de juiste kennis en vaardigheden, maar laten het doorgaans afweten op het gebied van integriteit en loyaliteit. Het vinden van geschikt personeel en het opbouwen van een goed ingespeeld team kost jaren. Een flexibele, lerende cybereenheid moet daarom per direct van start gaan. Als belangrijkste taak voor Defensie zie ik, naast cyberwarfare, het voorkomen en de opsporing van (bedrijfs)spionage en aanvallen op nationale, vitale infrastructuur.

> In beginsel is geen enkel systeem immuun voor een cyberaanval

In het nog op te richten Nationale Cyber Security Centrum (NCSC) wordt straks alle dreigingsinformatie, kennis en expertise uitgewisseld. Hoe dit zich verhoudt tot het platform cybersecurity CPNI, onderdeel van TNO en voorheen het NICC, is mij nog niet duidelijk. De huidige situatie vraagt om directe actie en het gevaar van een besluiteloze vergadercultuur ligt op de loer. De *bad guys* staan riant voor, met als complicerende factoren een geringe pakkans en een groot scala aan te misbruiken beveiligingslekken. De kunst is nu om de achterstand niet verder op te laten lopen en langzaam terrein te heroveren. Preventie is volstrekt onvoldoende. Bestrijden is voorlopig de belangrijkste oplossing. Om met beveiligingsexpert Bruce Schneier af te sluiten: '*In cyberspace, the balance of power is on the side of the attacker. Attacking a network is much easier than defending a network*'. ■