Cyberoperaties: naar een juridisch raamwerk

Defensie zal de komende jaren investeren in cyberoperaties. Deze operaties zullen ingebed zijn in de strategische Cybervisie Defensie, de Nationale Cybersecurity Strategie en de Nationale veiligheidsstrategie. De krijgsmacht zal cyberactiviteiten vanuit de drie hoofdtaken moeten ontplooien. Daarbij is een juridisch raamwerk onmisbaar. Dit raamwerk bestaat enerzijds uit de grondslagen voor nationale en internationale inzet: de rechtsbases. Anderzijds zullen cyberoperaties – net als andere operaties – moeten worden uitgevoerd binnen de van toepassing zijnde rechtsregimes. Beide componenten van dit raamwerk vertonen nog lacunes, onduidelijkheden of tegenstrijdigheden. Deze bijdrage inventariseert en analyseert de componenten en brengt een aantal vraagstukken in kaart.

dr. P.A.L. Ducheine – kolonel van de Militair Juridische Dienst
*mr. J.E.D. Voetelink – luitenant-kolonel van de Koninklijke Luchtmacht**

Wikileaks' recente publicaties van diplomatieke documenten werden door de VS opgevat als '*an attack on America's foreign policy interests [and] an attack on the international community*'.[1] Als 'verdediging' op deze 'aanval' bepleitte een voormalig adviseur van de Canadese minister-president om WikiLeaks oprichter Julian Assange te vermoorden.[2]

Aanvallen?

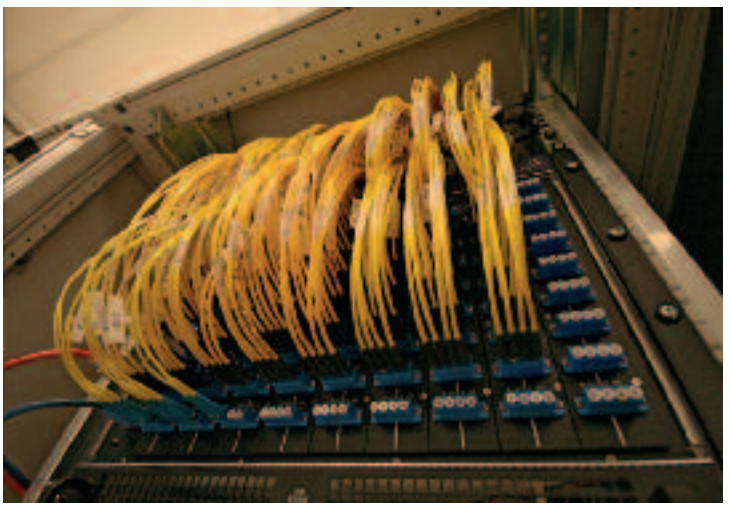
Het gaat hier om acties in het digitale domein die ons als aanval worden gepresenteerd. Is dit louter demagogisch taalgebruik of is er inderdaad sprake van aanvallen? Zijn dit uitzonderingen? Kennelijk niet, zoals de volgende voorbeelden demonstreren.

Aan de vooravond van de publicatie meldde *WikiLeaks.org* dat ze zelf slachtoffer was geworden van een cyberaanval op haar website: een *Distributed Denial of Service* (DDoS) *attack*.[3] Sympathisanten van WikiLeaks voerden op hun beurt cyberaanvallen uit tegen bedrijven of instellingen die WikiLeaks (financieel) dwarszaten.[4] Het strijdtoneel verplaatste zich ook naar Nederland: als reactie op de arrestatie van een Nederlandse hacker werd de website van het Openbaar Ministerie vervolgens platgelegd.[5]

Deze aanvallen over en weer staan niet op zichzelf. In september 2010 moest Iran een cyberaanval incasseren via de computerworm *Stuxnet*,[6] die gericht leek te zijn tegen het Iraanse kernenergieprogramma.[7] Oudere en bekende voorbeelden zijn de cyberaanvallen op Estland[8] en Georgië.[9] Minder bekend is de explosie in

* De auteurs zijn universitair (hoofd)docent aan de Faculteit Militaire Wetenschappen (FMW) van de Nederlandse Defensie Academie (NLDA).

1 *Remarks to the Press on the Release of Confidential Documents*, 28 november 2010, www.state.gov/secretary/rm/2010/11/152078.htm.
2 'Flanagan regrets WikiLeaks assassination remark', *CBC News*, 1-12-2010,' www.cbc.ca.
3 'WikiLeaks: slachtoffer van cyberaanval'. *NRC Handelsblad*, 28-10-2010.
4 'Duizend sites kopiëren alles van WikiLeaks'. *NRC Handelsblad*, 8-12-2010.
5 'Website OM plat na arrestatie hacker', *de Volkskrant*, 10-12-2010.
6 'Iran: cyberaanval met computerworm afgewend', *NRC Handelsblad*, 27-9-2010.
7 'Kernreactors Iran mogelijk doelwit Stuxnet-worm', *NRC Handelsblad,* 16-11-2010. 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, 15 januari 2011.
8 S.W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, Oxford: OUP, 2009, p. 3-6
9 S.W. Korns en J.E. Kastenberg, 'Georgia's Cyber Left Hook', in: *Parameters*, 2009, p. 60.



Het cyberdomein is vooralsnog sterk afhankelijk van civiele partijen, waaronder providers

een Siberische oliepijpleiding in 1982: de door Rusland (in Canada) gestolen software zou door de CIA zijn 'bewerkt', waardoor het controlesysteem van de pijpleiding ontregeld werd.[10]

Cybersecurity in Nederland

Operaties in de vijfde dimensie, het cyberdomein, staan ondertussen ook in Nederland op de politieke én militaire agenda.[11] Via de motie Knops c.s. oefende het parlement druk uit op de regering om te komen tot een interdepartementale *cybersecurity* strategie en 'actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO'.[12] De regering heeft deze *Nationale Cybersecurity Strategie* (NCSS) op 22 februari jongstleden aan de Tweede Kamer aangeboden.[13]

Deze ontwikkelingen in de vijfde dimensie hebben ook voor Defensie implicaties. Dat betreft de bedreigingen enerzijds en de (actieve of passieve) bescherming tegen die bedreigingen of aanvallen anderzijds. De regering neemt met de NCSS alvast een voorschot op het – inmiddels opgestarte – strategische besluitvormingsproces binnen Defensie aangezien '[de] responscapaciteit om ook in het digitale domein effectief te kunnen opereren wordt versterkt, onder andere bij Defensie'.[14]

Daarnaast zal de minister van Defensie binnenkort de Beleidsvisie [Cybersecurity] Defensie lanceren, waarin 'cyberintensiveringen' een plaats hebben.[15] In de nota *Defensie na de kredietcrisis: een kleinere krijgsmacht in een onrustige wereld* gaf de minister van Defensie aan dat 'Defensie haar digitale weerbaarheid de komende jaren [zal] versterken en het vermogen [zal] ontwikkelen tot het uitvoeren van cyber operations'.[16]

Parallel aan deze ontwikkelingen zal een strategisch raamwerk verder moeten worden ontwikkeld. Tettero & de Graaf braken in dit blad een lans voor een (strategisch) raamwerk voor cyberoperaties.[17] De Britse studie *On Cyber Warfare* onderstreept dit pleidooi en beschouwt het ontbreken van een strategisch raamwerk als een voedingsbodem en uitgelezen kans voor vijandige cyberoperaties.[18]
Hoewel het belang ervan allerminst miskend wordt, is het juridische raamwerk waarbinnen onze eigen cyberoperaties vorm moeten krijgen in beide publicaties evenwel onderbelicht gebleven. Tettero en De Graaf spraken in mei 2010 de verwachting uit dat een militaire cyberstrategie 'de definiëring en uitwerking van het juridische kader' zou bevatten.[19]

Doel en opbouw artikel

Met dit artikel willen we een voorschot nemen op de gedachtevorming over dit juridische raamwerk. Voordat we op dit juridische kader ingaan, zullen we eerst aandacht moeten besteden aan de strategische context van militaire cyberoperaties. Hierbij benoemen we negen kenmerken van (militaire) cyberoperaties en besteden aandacht aan de strategische en

10 'Cyberwar: War in the fifth domain', *The Economist*, 1 juli 2010.
11 Vijfde dimensie naast land, water, lucht en ruimte ('space'). Zie M.A.D. Tettero & P. de Graaf, 'Het vijfde domein voor de krijgsmacht', in: *Militaire Spectator* 179 (2010) 5, pp. 240-248. Zie voor een oudere agendering: NL ARMS 1999, *Information Operations*, J.M.J. Bosch, H.A.M. Luiijf & A.R. Mollema (red.).
12 *Kamerstukken* II 2009/10, 32 123 X, nr. 66. Voortgang in 32 123 X, nr. 89; 26 643, nr. 149 en 164. Zie ook de motie Hernandez, *Kamerstukken* II 2010/11, 32 500X, nr. 76.
13 *Kamerstukken* II, 2010/11, 26 643, nr. 174.
14 *Kamerstukken* II, 2010/11, 26 643, nr. 174.
15 *Kamerstukken* II, 2010/11, 26 643, nr. 174.
16 *Kamerstukken* II, 2010/11, 32 733, nr. 1, p. 19.
17 Tettero & De Graaf, t.a.p.
18 P. Cornisch, D. Livingstone, D. Clemente & C. Yorke, *On Cyber Warfare*, Chatham House, 2010, p. 21-22.
19 Tettero & De Graaf, p. 247.

grondwettelijke inbedding van deze militaire operaties. Daarna gaan we in op de elementen van een juridisch raamwerk voor cyberoperaties. We benoemen daarbij de verschillende rechtsbases en toepasselijke rechtsregimes. We ronden ten slotte af met conclusies.

Strategische context

De Nederlandse doelstelling voor de NCSS is uitdagend, aangezien veiligheid in het cyberdomein zeer diverse kenmerken heeft. Om de (juridische) implicaties van de vijfde dimensie goed te kunnen bevatten, worden hierna negen kenmerken aangestipt.

Eerst zullen we de kenmerken van cyberbedreigingen kort herhalen. Daarna benoemen we kenmerken die van belang zijn voor de bescherming tegen deze bedreigingen. Vervolgens bezien we kenmerken van het cyberslagveld die zowel op eigen cyberoperaties als die van onze tegenstanders van invloed zijn. Ten slotte gaan we in op de strategische en grondwettelijke inbedding van militaire cyberoperaties.
We ronden dit deel af met een typering van mogelijke militaire cyberoperaties.

Bedreigingen

Cyberbedreigingen zijn zeer allereerst zeer divers van aard en/of intentie. Het gaat om een (combinatie van) ideologische, criminele, financiële, politieke, economische en militaire inbreuken op onze nationale en internationale veiligheid.[20] Achter die inbreuken gaan – ten tweede – zowel statelijke actoren als een veelkleurig palet aan niet-statelijke actoren schuil. Die laatste groep bestaat onder meer uit (combinaties van) criminelen, activisten, actiegroepen, terroristen, rebellen en commerciële bedrijven.

Deze inbreuken kunnen – ten derde – openlijk dan wel heimelijk van aard zijn. Heimelijke acties zullen eerder regel dan uitzondering zijn. Mede door het heimelijke karakter en vanwege de lange transnationale (om)weg die digitale data aflegt, is – ten vierde – attributie (herleiden en toerekenen) van aanvallen een van de grootste obstakels voor adequate respons.

Bescherming en respons

De voorgestane cybersecurity strategie bestrijkt logischerwijs meerdere beleidsterreinen en kent een verscheidenheid aan 'bestrijders'.[21] Niet alleen het integrale karakter maar vooral de diversiteit aan bedreigingen vraagt daarom. Cybersecurity is dus – ten vijfde – multidisciplinair en vraagt om een interdepartementale (*interagency*) aanpak. Het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 is bijvoorbeeld door drie ministers ondertekend.[22]

De bedreigingen (en het slagveld) zijn echter van dien aard dat de overheid niet in haar eentje tot adequate bescherming in staat is. Het cyberdomein is vooralsnog sterk afhankelijk van civiele partijen (waaronder providers). Cybersecurity vraagt daarom – ten zesde – om een combinatie van publieke en private inspanningen.

Publiek-private samenwerking tekent zich sinds 2006 af in de 'informatieknooppunten' van het programma NICC (Nationale Infrastructuur ter bestrijding van CyberCrime).[23] Ten zevende is een internationale aanpak onvermijdelijk: het wereldwijde web en digitale communicatie zijn typisch voor globalisering en het vervagen van (fysieke) grenzen.

Het virtuele slagveld

Het virtuele slagveld is van invloed op eigen én oppositionele cyberoperaties. Het cyberdomein wordt – ten achtste – nauwelijks door fysieke of soevereine grenzen gehinderd. Cyberoperaties vinden plaats binnen een niet-fysieke dimensie, waar de staatsgrenzen amper relevant zijn: 'Cyberaanvallen en -verstoringen overschrijden in een oogwenk landsgrenzen, culturele en juridische stelsels', aldus de NCSS.

Cyberoperaties maken gebruik van een structuur van onderling verbonden netwerken: het

20 Tettero & De Graaf, p. 242.

21 Idem.

22 *Kamerstukken* II 2010/11, 28 684, nr. 292: de ministers van Veiligheid & Justitie; Economische Zaken, Landbouw & Innovatie; en Defensie. Het Trendrapport is als bijlage bij dit kamerstuk opgenomen.

23 *Kamerstukken* II 2009/10, 30 821, nr. 10, p. 3-4.

internet. Een aantal landen bevindt zich in een kwetsbare positie omdat zij zogeheten internetknooppunten ('hubs') herbergen.[24] Deze knooppunten spelen een cruciale rol in het wereldwijde internetverkeer.

Cyberaanvallen overschrijden landsgrenzen, en culturele en juridische stelsels

Cyberoperaties hebben – ten negende – met elkaar gemeen dat de strijdmethoden niet-kinetisch zijn. Dit sluit niet uit dat de gevolgen wel degelijk van fysieke aard kunnen zijn. Een cyberverstoring van een energiecentrale kan daadwerkelijk dezelfde fysieke (indirecte) gevolgen hebben als een kinetische bomaanval op een transformatorstation.

Naast deze negen kenmerken zijn twee andere elementen van belang voor de (nog te finaliseren) Cybervisie Defensie: de bestaande strategische inbedding en de grondwettelijke doelomschrijving van de krijgsmacht.

Strategische inbedding

De NCSS zou logischerwijs moeten passen in een brede, integrale veiligheidsstrategie. Nederland ontbeert echter deze overkoepelende '*Grand Strategy*' voor binnen- en buitenlands veiligheidsbeleid. In plaats daarvan moeten we ons behelpen met de *Nationale Veiligheidsstrategie*,die primair een binnenlandse focus heeft.[25]

Deze deelstrategie noemt bovendien slechts vijf vitale nationale belangen[26] en mist ten onrechte

Cover van het rapport 'On Cyber Warfare'

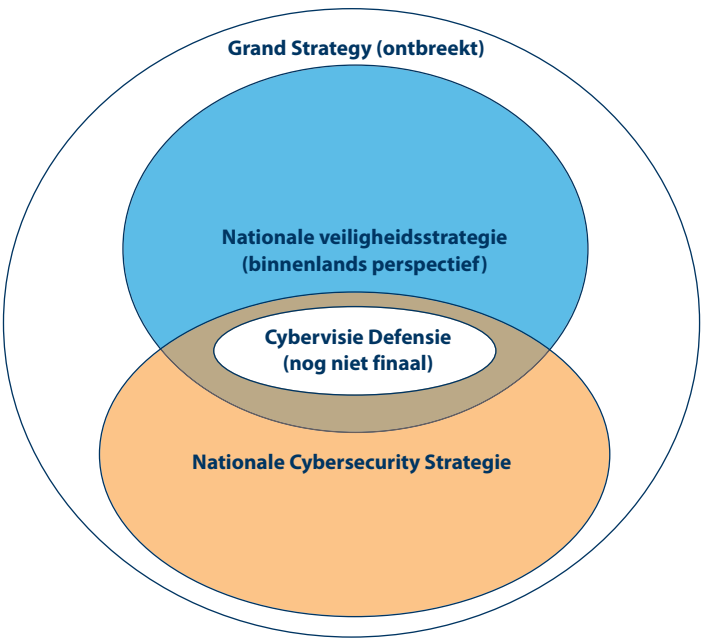
de 'internationale rechtsorde' als zesde vitaal belang.[27] Deze dubbele lacune is gezien de grondwettelijke taakopdracht aan de regering om 'de ontwikkeling van de internationale rechtsorde' te bevorderen, opmerkelijk:[28] 'als zestiende economie en negende exportland ter wereld heeft Nederland zelf alle belang bij internationale veiligheid', aldus *NRC Handelsblad*.[29] Dit gebrek in ons strategische raamwerk zou vijandige cyberoperaties in de hand kunnen werken.[30] Recente gebeurtenissen in Noord-Afrika en het Midden Oosten tonen de effecten van sociale en digitale media op de politieke stabiliteit en de internationale rechtsorde.

Defensie zal desondanks haar cybervisie moeten ontwikkelen. Deze zal een afgeleide moeten zijn van de NCSS én de *Nationale Veiligheidsstrategie*. Zoals uit figuur 1 blijkt, kan het ontbreken van een volwaardige *Grand Strategy* de ontwikkeling van een Defensievisie hinderen, gezien het overkoepelend karakter van die strategie.

24 Zo behoort de Amsterdam Internet Exchange tot een van de grotere ter wereld.
25 *Kamerstukken* II 2006/07, 30 821, nr. 1.
26 Territoriale, fysieke, ecologische, economische veiligheid en politieke & sociale stabiliteit.
27 P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding* (diss. UvA) Nijmegen: Wolf Legal Publishers, 2008, p. 20. Zie ook artikel 90 Grondwet.
28 Art. 90 Grondwet.
29 *NRC Handelsblad*, Commentaar, 8-4-2011.
30 Onderzoekers wijzen erop dat het ontbreken van een (adequate) nationaal strategisch raamwerk een voedingsbodem kan zijn voor vijandige cyberoperaties: Cornish c.s., *On Cyber Warfare*, p. 21-22.

Grondwettelijk inbedding: welke operaties?
De Cybervisie Defensie wordt m`ede bepaald door de grondwettelijke doelomschrijving (art. 97): 'Ten behoeve van (1) de verdediging en (2) ter bescherming van de [andere vitale] belangen van het Koninkrijk, alsmede ten behoeve van (3) de handhaving en de bevordering van de internationale rechtsorde, is er een krijgsmacht'. Deze doelomschrijving impliceert dat Defensie cyberoperaties binnen haar drie hoofdtaken moeten kunnen uitvoeren.

De consequentie hiervan is dat de krijgsmacht in een breed spectrum cyberoperaties zal moeten kunnen uitvoeren. Deze operaties zijn zowel passief/defensief als actief/offensief van aard. Ze kunnen als zuiver militaire dan wel als (ondersteunend aan) civiele operaties worden getypeerd en omvatten logischerwijs ook het (digitaal) verzamelen van (digitale) inlichtingen.[31]



Figuur 1: Strategische inbedding

Tettero & De Graaf boden een duidelijk overzicht van de strijdmethoden. In het NAVO-jargon gaat het om *Computer Network Operations*, waaronder het verzamelen van digitale inlichtingen, *Computer Network Attacks* (CNA), *Computer Network Defence* (CND) en *Computer Network Exploitation* (CNE).[32] Het begrip 'cyberoperaties' moet naar onze mening daarom ruim worden opgevat. Namelijk als operaties en conflicten in het vijfde (digitale) domein, die zowel bestaan uit offensieve, defensieve, passieve en (pro)actieve activiteiten, alsmede uit het verzamelen van inlichtingen.

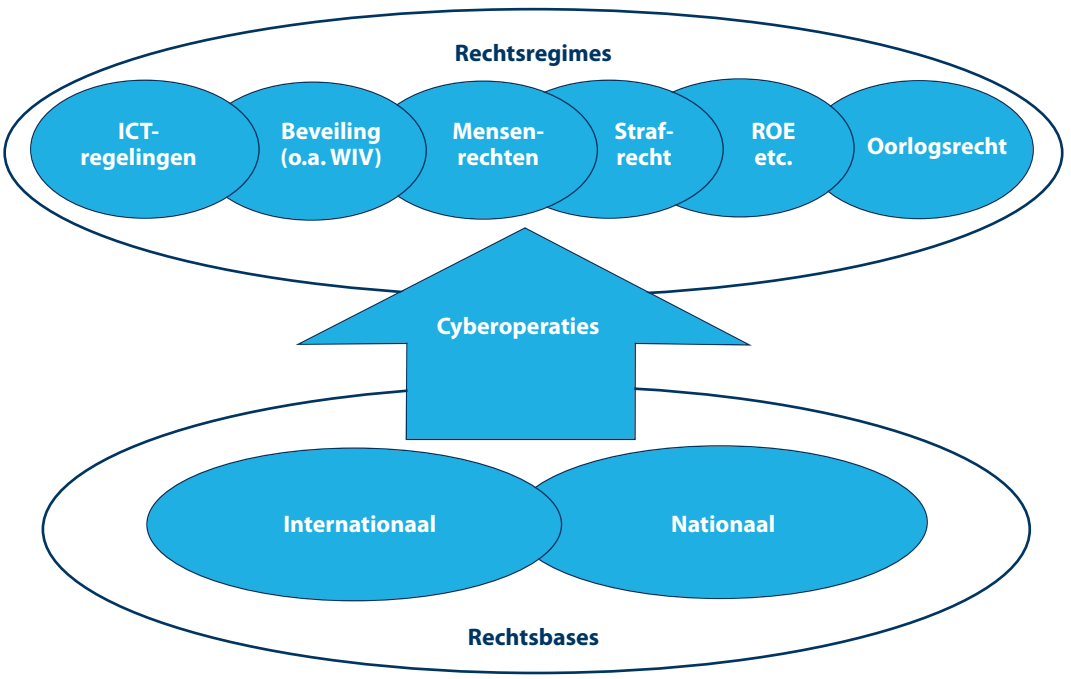
Juridisch raamwerk

Met de hiervoor beschreven strategische context van militaire cyberoperaties in het achterhoofd, volgt hier een schets van het juridische raamwerk. Dit raamwerk bestaat uit twee delen: de grondslagen van militaire cyberoperaties (de rechtsbases) en de regels die van toepassing zijn tijdens de uitvoering van deze operaties (de rechtsregimes).

Rechtsbases en rechtsregimes
Het juridische kader zelf is opgebouwd uit twee herkenbare componenten: rechtsbases en rechtsregimes.[33] Zoals bij andere (militaire) operaties is allereerst een 'adequate' rechtsgrondslag of rechtsbasis benodigd, vóórdat tot een operatie besloten kan worden. Die basis vinden we in het nationale recht dan wel in het internationale recht (het *ius ad bellum*), zoals de Wet op de Inlichtingen- en Veiligheidsdiensten voor operaties in het binnenland of een VN-mandaat bij een crisisbeheersingsoperatie in het buitenland.

Het tweede deel van het raamwerk bestaat uit de regels die de uitvoering van cyberoperaties beheersen: de rechtsregimes. Hierbij kan worden gedacht aan *Rules of Engagement* (ROE), oorlogsrecht en mensenrechten, evenals het nationale strafrecht en nationale 'geweldsinstructies'. Beide componenten – rechtsbases en rechtsregimes – vormen samen het juridische raamwerk voor cyberoperaties. Dit raamwerk dekt

31 Tettero & De Graaf, p. 241.
32 AJP-3.10, para 0129. Idem: *The National Military Strategy for Cyberspace Operations*, Chairman of the Joint Chiefs of Staff, DoD, december 2006. Nederland voegt daar inlichtingen aan toe.
33 Zie ook de tweedeling in de *Land Doctrine Publicatie – Militaire doctrine voor het landoptreden* (LDP-1), Koninklijke Landmacht, 2009, p. 42, § 2702.



Figuur 2: Het juridische kader van cyberoperaties

het totale spectrum van cyberoperaties af (zie figuur 2).

De uitdaging

De uitdaging bestaat uit het herkennen, definiëren, interpreteren en zo nodig aanvullen van de elementen van het juridische kader. Dit is geen eenvoudige onderneming. De rol die bijvoorbeeld het (internationaal) informatierecht, dat het (internationale) dataverkeer reguleert, speelt is tot nu toe relatief onderbelicht bij reguliere militaire operaties. Op dit vakgebied schiet de standaard militair-juridische kennis voorlopig nog te kort.

De implicaties van dit rechtsgebied zullen dan ook verder onderzocht moeten worden. Internationale verdragen, EU-richtlijnen, directieven van de Raad van Europa, beslissingen en resoluties van andere internationale organen, zoals de VN, de Veiligheidsraad, G8, OECD, OSCE, NAVO en (W)EU, zullen eveneens een rol in het juridische raamwerk kunnen spelen.

Cyberoperaties onderscheiden zich ook anderszins van meer traditionele militaire operaties[34] en vragen om een aanvulling of herinterpretatie van het bestaande juridische raamwerk. Op dit moment is het specifieke juridische raamwerk voor het 'jonge' cyberdomein nogal beperkt: het recht is immers vaak instrumenteel en volgt bijvoorbeeld technologische of maatschappelijke ontwikkelingen.

Totdat het recht op het gebied van cybersecurity is geactualiseerd, zullen cyberoperaties via bestaande kaders moeten worden geïnterpreteerd en toegepast. Deze exercitie is niet ongebruikelijk bij vernieuwingen: operaties tegen terrorisme zijn daar een recent voorbeeld van.[35] Net als dit fenomeen trekt ook 'cyber' zich overigens weinig aan van landsgrenzen of het primaat van statelijke actoren in het internationaal recht.

Binnen het bestek van deze bijdrage kunnen we slechts enkele elementen van het juridische raamwerk belichten. We selecteren daarbij die delen die naar onze mening interpretatie of aanpassing behoeven. Soms zullen we moeten volstaan met het aanduiden van een lacune.

34 G.H. Todd, 'Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition', in: *Air Force Law Review*, 2009, p. 68.

35 Ducheine (2008).

We bezien de volgende elementen: nationale en internationale rechtsbases, en nationale en internationale rechtsregimes.

Nationale rechtsbases

Wet inlichtingen en veiligheidsdiensten 2002
Naast de AIVD beschikt de MIVD via de Wet inlichtingen en veiligheidsdiensten 2002 (WIV) over de bevoegdheid om onderzoek te doen naar opponenten en landen.[36] Het verzamelen van inlichtingen geschiedt deels via open bronnen en deels door middel van zogeheten bijzondere bevoegdheden (art. 18 Wiv 2002). Zo mag de MIVD bijvoorbeeld elektronisch berichtenverkeer en dataverkeer tussen computers aftappen en opnemen (art. 25), satellietcommunicatie uit of naar andere landen onderscheppen (art. 26 en 27) en geautomatiseerde systemen binnendringen (art. 24).

Een belangrijk kenmerk van de WIV is het feit dat ze géén zogeheten extraterritoriale werking kent.[37] Dat wil zeggen dat, hoewel de MIVD wel een taak heeft om onderzoek te doen *naar* andere landen, de Nederlandse wet geen expliciete basis of bevoegdheden schept voor operaties *in* het buitenland.[38]

Een ander kenmerk is dat de WIV taken en bevoegdheden schept ten aanzien van inlichtingenverzameling; ze is dus vooral defensief ingesteld. Een belangrijke vraag is of de WIV de diensten ook de mogelijkheid biedt om offensieve cyberoperaties uit te voeren, bijvoorbeeld door een virus of wormen achter te laten of door *Computer Network Exploitation* (CNE) te faciliteren. Voorlopig lijkt dit laatste niet het geval te zijn.

Bewaking militaire objecten
De Rijkswet geweldgebruik bewakers militaire objecten is tot stand gekomen om geweldgebruik bij de bewaking- en beveiliging van militaire objecten te legitimeren.[39] De wet omschrijft geweld als: 'elke dwangmatige kracht van meer dan geringe betekenis, uitgeoefend op personen of zaken'.[40] De belangrijkste toepassing van de Rijkswet behelst de fysieke bewaking/beveiliging van die militaire objecten, waaronder 'militaire radiostations, peilgebouwen, antenneparken, zenderparken en verbindingscentra'.[41]
Het valt op dat deze opsomming klassiek verbindings-technisch van aard is. Het valt echter te bezien of datacenters, servers en internethubs die Defensie gebruikt en die op civiele locaties zijn ondergebracht, onder deze noemer vallen.[42]

Een andere vraag is of een defensieve cyberoperatie, bijvoorbeeld om een vijandige cyberaanval op eigen datasystemen af te slaan, onder de werking van de wet zou kunnen vallen. Ze moet dan als geweldgebruik kunnen gelden en als geweldmiddel zijn toegelaten. Vooralsnog gaat de Rijkswet er primair van uit dat bij geweld (slechts) de voorgeschreven – klassieke, fysieke – geweldsmiddelen worden gebruikt en dat slechts fysieke objecten beveiligd kunnen worden.[43]

Politiewet 1993
Via de taakstelling in de Politiewet 1993 is de Koninklijke Marechaussee (KMar) onder meer belast met de politietaak voor Nederlandse strijdkrachten en op plaatsen onder beheer van Defensie (art. 6). Tot die politietaak hoort ook het opsporen en voorkomen van strafbare feiten, zoals cybercrime, spionage, chantage, schenden van geheimhoudingsplichten, et cetera.[44] Strafbare feiten in deze sfeer zijn bijvoorbeeld: *hacking*,[45] *spamming* of DDoS *(bombing)*,[46] het installeren van *ettercaps*

36 Art. 7 WIV.
37 Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, Verslag studiemiddag CTIVD 'Inlichtingenactiviteiten in het buitenland', p. 1, zie: www.ctivd.nl.
38 Zie o.a. CTIVD, *Jaarverslag 2006-2007*, p. 54.
39 Art. 1 en 2 Rijkswet. *Stb* 2003, 134.
40 Art. 1 Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak, 2003-06-17, *Stb* 2003, 282 (hierna: Besluit geweldgebruik).
41 Bijlage A(7) bij Rijksbesluit houdende aanwijzing van te bewaken en te beveiligen objecten, *Stcrt* 2000, 185, p. 16.
42 Art. 2 Rijksbesluit houdende aanwijzing van te bewaken en te beveiligen objecten biedt de mogelijkheid om objecten tijdelijk aan te merken; zie hierover: Ducheine, P.A.L., (2005), 'Geweldgebruik op grond van de Rijkswet geweldgebruik bewakers militaire objecten: de definitie van een "militair object" en extraterritoriale werking?', in: 98 *Militair Rechtelijk Tijdschrift* (2), p. 45-55.
43 Art. 3 junto art. 6 Besluit geweldgebruik.
44 Zie ook het dossier Cybercrime: www.ejure.nl.
45 Computervredebreuk, art. 138a Sr.
46 Art. 138b Sr.

(hulpmiddelen waarmee netwerkverkeer wordt 'afgeluisterd' of verstoord)[47] en het vernielen van data door *defacing* van een website, het verspreiden van virussen, wormen en Trojaanse paarden.[48]

FOTO AVDD, H. KEERIS

Ook voor het luchtwapen ontbreekt een specifiek verdrag voor de strijd in de derde dimensie

Via militaire bijstand kunnen de KMar en andere onderdelen van de krijgsmacht civiele politiekorpsen ook in het cyberdomein ondersteunen (art. 58-60 Politiewet). Zo zouden ISTAR-middelen[49] tijdelijk in dienst van de politie kunnen worden gesteld voor de opsporing, preventie of beëindiging van cybercriminaliteit of -terrorisme.

47 Vernielen van een geautomatiseerd werk, artt. 161sexties en 161 septies Sr. Zie: www.win.tue.nl/~aeb/linux/hh/cybercrime.html.

48 Vernielen van computerdata, artt. 350a en 350b Sr.

49 Intelligence, Surveillance, Target Aquisition & Reconnaisance.

50 Zie o.a. Ducheine (2008), p. 130-131; J. Barkham, 'Information Warfare and International Law on the Use of Force', in: *New York University Journal of Internationale Law and Politics*, 2001, 34, p. 71.

51 P. Ducheine & E. Pouw, *ISAF operaties in Afghanistan*, Nijmegen: Wolf Legal Publishers, 2010, p. 10.

52 D. Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', in: *Harvard International Law Journal*, 2006, p. 187. Verder is wel een meer strafrechtelijke benadering voorgesteld die aansluit bij het ontstaan ('*genesis*') van een cybervoorval; Todd, p. 70.

Samenvattend: Nationale rechtsbases
De huidige nationale grondslagen voor cyberoperaties zijn hoofdzakelijk defensief georiënteerd en gericht op rechtshandhaving. Een rechtsbasis voor offensieve operaties in binnen- of buitenland is in beginsel niet in het nationale recht aanwezig.

Wel is er een variatie aan (pro-)actieve, preventieve en repressieve mogelijkheden. De actualiteit van cybersecurity is in een aantal gevallen nog niet vertaald in aangepaste regelgeving.

Internationale rechtsbases

Grensoverschrijdende (offensieve en defensieve) militaire operaties zijn in het volkenrecht, het *ius ad bellum*, vanwege het interstatelijke geweldsverbod in principe niet toegestaan. Het geweldverbod is vastgelegd in artikel 2(4) van het VN-Handvest.

> *In hun internationale betrekkingen onthouden alle Leden zich van bedreiging met of het gebruik van geweld tegen de territoriale integriteit of de politieke onafhankelijkheid van een staat, en van elke andere handelwijze die onverenigbaar is met de doelstellingen van de Verenigde Naties.*

Dit geweldsverbod verbiedt extraterritoriale militaire operaties (inclusief cyberoperaties) voor zover die als geweldgebruik kunnen worden opgevat. Deze kwestie is problematisch omdat een definitie van geweldgebruik ontbreekt. Duidelijk is dat het gewapend, lees militair, fysiek geweld betreft.[50]
De omvang van dit geweld speelt daarbij geen rol.[51] Acties worden beoordeeld naar de resultaten of effecten:[52] wanneer zij rechtstreeks materiële schade, doden of gewonden veroorzaken zijn het vormen van geweldgebruik.

Gewapend geweld?
De hamvraag is natuurlijk of cyberoperaties als 'gewapend geweld' gelden en onder het geweldsverbod vallen. Zo ja, dan zijn die cyberoperaties vanwege het geweldsverbod verboden. Deze eenvoudige vraag levert vooralsnog een probleem op.

Cyberoperaties zijn namelijk – gelet op de dimensie waarin zij plaatsvinden – moeilijk te vergelijken met traditionele, kinetische militaire operaties in de fysieke ruimte. Bovendien is de schade veelal niet fysiek van aard. Schmitt bedient zich daarom van enkele indicatoren als: de ernst van de gevolgen van het geweldgebruik, de mate van onmiddellijkheid, doordringendheid, directheid, verantwoordelijkheid of meetbaarheid.[53] Hiermee kan worden bepaald in hoeverre de voorzienbare gevolgen van cyberoperaties op gewapend geweld lijken.[54] Dit zal van geval tot geval moeten worden bezien.

Niet elke cyberactiviteit kwalificeert zich als geweldgebruik: sommige cyberoperaties houden dus geen schending van het geweldsverbod in. Deze zijn toegestaan, zo lang ze geen andere regels van het internationaal recht schenden.[55]

Cyberoperaties die wel gewapend geweld impliceren en onder het geweldsverbod vallen, zijn verboden tenzij een staat zich kan beroepen op één van de drie uitzonderingen die het volkenrecht biedt: instemming, militaire dwangmaatregelen onder Hoofdstuk VII van het VN-Handvest, en zelfverdediging tegen een gewapende aanval (zie hierna).

Deze drie uitzonderingen op het geweldsverbod vormen het zogeheten 'adequate volkenrechtelijke mandaat'. Deze opvatting is volledig in lijn met de opvatting van de Nederlandse regering, zoals onder meer naar aanleiding van het Irak-onderzoek door de Commissie Davids nog eens duidelijk werd.[56]

Instemming

Cyberoperaties kunnen in het buitenland altijd met instemming van de betreffende staat worden uitgevoerd, ook als ze geweldgebruik omvatten.[57] Tijdens crisisbeheersingsoperaties kan het gastland die toestemming verlenen in een statusovereenkomst (*Status of Forces Agreement*) of *Memorandum of Understanding*. Het spreekt vanzelf dat de uitvoering van die operaties aan de restricties en het recht van het gastland zijn onderworpen. Deze restricties zijn dan weer bepalend voor het rechtsregime dat de uitvoering van de operaties beheerst, bijvoorbeeld in de vorm van ROE.

Militaire dwangmaatregelen

Indien toestemming voor de uitvoering van cyberoperaties ontbreekt (en de cyberoperaties geweldgebruik omvat), is een andere uitzondering op het geweldsverbod noodzakelijk. Primair zal dan bezien moeten worden of de VN-Veiligheidsraad militaire dwangmaatregelen autoriseert gebaseerd op Hoofdstuk VII van het VN-Handvest.

De Veiligheidsraad kan militaire operaties autoriseren bij 'een bedreiging van de vrede, verbreking van de vrede of daad van agressie'.[58] Het oordeel of een *vijandelijke* cyberoperatie een bedreiging et cetera inhoudt, is aan de Veiligheidsraad.
De autoriserende Veiligheidsraadresolutie met daarin de frase '*to use all necessary means*' impliceert dat militair geweld (met inbegrip van cyberoperaties) kan worden aangewend tijdens buitenlandse operaties, ook tegen de wil van de betrokken partijen in.

Zelfverdediging

Bij gebrek aan instemming of een autorisatie van de VN-Veiligheidsraad kan een staat zich in sommige specifieke situaties beroepen op 'het inherente recht tot individuele of collectieve zelfverdediging in geval van een gewapende aanval'.[59] Zelfverdediging is slechts onder strikte voorwaarden toegestaan. Daarbij doen zich in het cyberdomein meerdere knellende vragen voor.

Allereerst moet er sprake zijn van een 'gewapende aanval'. Dit is een van de meest controversiële kwesties in het *ius ad bellum,* onder

53 Zie uitgebreid: M.N. Schmitt (1999). 'Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework', in: *Columbia Journal of Transnational Law,* 37, p. 885-937, zie p. 914.
54 Ibid., p. 916.
55 Zoals bijvoorbeeld het soevereiniteits- of non-interventiebeginsel uit het VN-Handvest.
56 Regeerakkoord *Samen Werken, Samen Leven*, kabinet Balkenende IV, uitgewerkt in *Kamerstukken II* 2006/07, 29 521, nr. 41, p. 2 e.v.
57 Hierdoor vormen deze operaties geen inbreuk op soevereiniteit, het non-interventiebeginsel en het geweldsverbod.
58 Art. 39 VN-Handvest.
59 Art. 51 VN-Handvest.

meer omdat ook hier een definitie ontbreekt.[60] Ruys gebruikt de volgende definitie:

> *An armed attack consists in the deliberate use of armed force against a State, producing, or liable to produce, serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property.*[61]

Ook een plotselinge overweldigende dreiging van een gewapende aanval die geen moment van reflectie en geen keuze van andere middelen (dan zelfverdediging) toelaat, valt doorgaans onder de definitie.[62] Een reeks van meerdere kleinere aanvallen kan cumulatief in onderlinge samenhang soms ook als een gewapende aanval gelden.[63]

De kwestie van de gewapende aanval is weinig problematisch als vijandelijke staten of niet-statelijke actoren een klassieke aanval uitvoeren, waarna het slachtoffer zichzelf (onder meer via een cyberoperatie) verdedigt. De crux is natuurlijk of vijandelijke cyberoperaties als 'gewapende aanval' kunnen worden bestempeld: slechts dan is zelfverdediging mogelijk. De cyberoperaties tegen Letland en Georgië golden in ieder geval *niet* als zodanig.
Zodra de kwalificatie als gewapende aanval duidelijk is, duikt een tweede kwestie op. Cyberactiviteiten laten zich, zoals ook de Stuxnet-aanval tegen Iran demonstreert, moeilijk tot een auteur of aanvaller herleiden. Attributie (toerekening) is – net als bij terreuraanslagen – zeer problematisch van aard. De vraag is tegen wie een eventuele reactie zich kan of moet richten? Logischerwijs is dat tegen de aanvaller, mits deze kan worden aangeduid uiteraard.[64]

Nationale rechtsregimes

In het nationale domein zien we vaak functionele wetgeving die zowel de rechtsbasis voor, als het rechtsregime tijdens inzet biedt.[65] Zo zullen de AIVD en MIVD niet alleen de bevoegdheid tot optreden ontlenen aan de WIV (zijnde de rechtsbasis), maar deze wet bepaalt tevens het rechtsregime waarbinnen deze bevoegdheden mogen worden toegepast.
Een zelfde situatie doet zich voor bij de bewakings- en beveiligingstaak van militaire objecten en de politietaken van de KMar. Voor zover cyberoperaties worden uitgevoerd, zullen de geweldsinstructies de uitvoering van de cyberactiviteiten beheersen. Vanwege de primaire focus op kinetisch geweldgebruik zal dit bij offensieve operaties niet zonder slag of stoot te realiseren zijn.

Geweld is in beide gevallen gedefinieerd als 'elke dwangmatige kracht van meer dan geringe betekenis uitgeoefend op personen of zaken'.[66] Voor politietaken van de KMar is het Wetboek van Strafvordering van belang. Verder zullen militairen die bijstand aan die politie verlenen, binnen de grenzen en (gewelds)instructies van de politie moeten blijven. Ook privacybepalingen waarbinnen politie en justitie opereren, alsmede eisen aan verslaglegging en archivering, spelen hier een rol.

Het mag duidelijk zijn dat niet al deze aspecten binnen dit artikel kunnen worden uitgewerkt. We volstaan met de constatering dat het rechtsregime binnen Nederland vaak afhankelijk is van de basis waarop de operatie berust, divers is en soms ook gekenmerkt wordt door een preoccupatie op kinetisch geweldgebruik.

Internationale rechtsregimes

Tot de internationale rechtsregimes die we binnen het bestek van dit artikel kunnen bezien rekenen we oorlogsrecht, Rules of Engagement, statusverdragen en mensenrechten. De zeer uitgebreide categorie van internationaal informatierecht die vanuit de Europese Unie en via verdragen van invloed is op cyberacties laten we kortheidshalve buiten beschouwing.

60 Zie o.a. T. Ruys, *'Armed Attack' and Article 51 of the UN Charter – Evolutions in Customary Law and Practice*, Cambridge: University Press, 2010.
61 Ruys, 2010, p. 542, gebaseerd op Y. Dinstein, (2005). *War, Aggression and Self-Defence,* Cambridge: University Press, p. 193.
62 In dat laatste geval is sprake van pre-emptieve zelfverdediging.
63 Ducheine (2008), p. 221.
64 Ducheine (2008), Stellingen en p. 570.
65 Daarnaast spelen grondrechten nog een belangrijke rol.
66 Art. 1 van resp. Ambtsinstructie voor de politie, de Koninklijke Marechaussee en de buitengewoon opsporingsambtenaar; en Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak.

FOTO AVDD, R. GIEING

De fysieke bewaking en/of beveiliging van militaire objecten is duidelijk omschreven. Maar het is de vraag of civiele datacenters, servers en internethubs daar ook onder vallen

Oorlogsrecht

Oorlogsrecht is tot stand gekomen vóórdat er cyberoperaties bestonden. Dat brengt – ook op dit vlak – interpretatievraagstukken met zich mee. Dat euvel doet zich niet voor het eerst voor: hoewel het luchtwapen al tijdens de Eerste Wereldoorlog tot ontwikkeling kwam, ontbreekt een specifiek verdrag voor de strijd in de derde dimensie. Toch staat het buiten kijf dat het humanitaire recht op de strijd in de lucht van overeenkomstige toepassing is. Deze analogie is goed op de vijfde dimensie toepasbaar.

Het oorlogsrecht heeft zich altijd adaptief opgesteld. Vanwege het vangnet van de grondbeginselen – militaire noodzaak, humaniteit, proportionaliteit, onderscheid en 'eerlijkheid en goede trouw' – die in alle gevallen van gewapend conflict gelden, is het oorlogsrecht feitelijk techniek onafhankelijk en daarmee toepasbaar op nieuwe ontwikkelingen, zoals cyberoperaties.[67]
Desondanks levert toepassing van het oorlogsrecht op cyberoperaties verschillende vraagstukken op. De belangrijkste vraag is uiteraard of het oorlogsrecht van toepassing is op cyberoperaties. Dat blijkt in twee situaties het geval te zijn. Ten eerste als cyberoperaties sec een 'gewapend conflict' vormen. Ten tweede als cyberoperaties deel uitmaken van een gewapend conflict en als vijandelijkheden kunnen worden beschouwd. We werken beide opties uit.

• Cyberoperaties sec: gewapend conflict?
Zodra er sprake is van een gewapend conflict is het oorlogsrecht automatisch van toepassing op de partijen bij het conflict.[68]
De hamvraag is: wanneer is er een gewapend conflict?[69] Ook dit cruciale begrip is niet gedefinieerd. Of er sprake is van een gewapend conflict moet aan de hand van de feiten worden vastgesteld.

De mening van de betrokken partijen omtrent het bestaan van een gewapend conflict is daarbij relevant maar niet doorslaggevend.[70] Uit de jurisprudentie van het Joegoslavië-tribunaal blijkt dat aan twee cumulatieve voorwaarden moet zijn voldaan.[71] Het gaat om (1) feitelijke vijandelijkheden van een zekere geweldsintensiteit, bestaande uit aan elkaar gerelateerde gewapende 'incidenten', die uitgevoerd worden door (2) tegenover elkaar staande georganiseerde gewapende groepen die over het vermogen beschikken om over een langere periode militaire operaties te ondernemen.

Het spreekt voor zich dat het non-kinetische karakter van cyberoperaties van invloed zal zijn op de vraag of cyberoperaties sec de drempel overstijgen en als een gewapend conflict gelden, waardoor het oorlogsrecht van toepassing is.

67 P.J.J. van der Kruit (red.), *Handboek militair recht*, Nijmegen: Wolf Legal Publishers, 2009, p. 450 e.v.
68 ICTY (1995), *Tadic (Appeal: jurisdiction)*, § 70.
69 Zie ICRC (2008b).
70 Ducheine & Pouw, 2010, p. 46.
71 Zie uitgebreid: Ducheine (2008), p. 474.

• Cyberoperaties tijdens gewapend conflict?
Indien cyberoperaties als onderdeel van een bestaand gewapend conflict worden uitgevoerd, is een volgend knelpunt of cyberoperaties als vijandelijkheden kunnen worden gezien. De meeste regels voor het voeren van vijandelijkheden[72] gaan uit van het centrale begrip 'aanvallen'. Dat laatste begrip is gedefinieerd als: 'daden van geweld gericht tegen de tegenstander, hetzij offensieve hetzij defensieve'.[73] Aanvallen kunnen vanuit land, zee en lucht worden uitgevoerd.[74]

De hamvraag is natuurlijk of cyberoperaties als 'gewapend geweld' gelden en onder het geweldsverbod vallen

Twee kwesties dringen zich op. Ten eerste of (alle) aanvallen in de vijfde dimensie ook door de algemene bepalingen over vijandelijkheden worden bestreken. Dat zou gelet op de doelstelling van het oorlogsrecht logisch zijn. Ten tweede of cyberoperaties als 'daden van geweld' moeten worden gezien. Als dat niet het geval zou zijn, dan zou een aantal bepalingen over vijandelijkheden niet van toepassing zijn. Gesteld dat cyberoperaties als aanvallen gelden en onder de algemene regels voor vijandelijkheden vallen, levert toepassing van deze regels ook weer hindernissen op. We bezien de toepassing van de beginselen van onderscheid en proportionaliteit. Vervolgens ronden we af met enkele opmerkingen over neutraliteit.

• Onderscheid en militaire doelen
Strijdende partijen moeten onderscheid maken tussen burgers en combattanten, en tussen militaire doelen[75] en burgerobjecten. In de praktijk is dit onderscheid soms lastig. *Dual use* objecten, zoals infrastructuur, radiostations, elektriciteitscentrales, communicatiesatellieten en computernetwerken, kunnen zowel een militaire als een civiele functie bezitten.

Bij cyberoperaties staat er nog meer druk op dit beginsel. Cyberoperaties tegen dual use objecten, zoals het internet, zijn daar een sprekend voorbeeld van.

• Proportionaliteit en *collateral damage*
Het verbod op disproportionele aanvallen verplicht de aanvallende partij de methode, tijd en plaats van een cyberaanval goed te overwegen en een *collateral damage assessment* uit te voeren.[76] Deze proportionaliteitstoets is tijdens normale operaties al lastig.[77] Cyberoperaties vormen daarop geen uitzondering, waardoor normvervaging op de loer licht.

Sommige cyberoperaties zullen minder burgerslachtoffers en schade veroorzaken dan een traditionele, kinetische aanval. Vooral bij dual use objecten kan dit aspect een overweging zijn om een cyberaanval te lanceren die anders (bij kinetische of traditionele operaties) vanwege de beginselen van onderscheid en proportionaliteit niet zouden mogen worden uitgevoerd.[78]

• Neutraliteit
Cyberoperaties zullen voor een belangrijk deel plaatsvinden via internet en zullen – vanwege die structuur en het dataverkeer daarlangs – via infrastructuur en netwerkknooppunten in neutrale staten kunnen verlopen.[79] Het oorlogsrecht (uit 1907!) bepaalt dat het grondgebied van de 'onzijdige Mogendheden' onschendbaar is en niet door een oorlogvoerende staat kan worden gebruikt.[80] Het gebruik van internetfaciliteiten (vanwege doorvoer van dataverkeer) in of via een neutrale staat zou dan strijdig zijn met dit neutraliteitsrecht.

Mogelijk biedt een uitzondering in het Haagse verdrag uitkomst: 'telegraaf- of telefoonkabels, alsmede van de toestellen voor telegrafie

72 Zie sectie API, Deel IV Burgerbevolking – Sectie I Algemene bescherming tegen de gevolgen van de vijandelijkheden.
73 Art. 49(1) API.
74 Art. 49(3) API.
75 Artikel 52, tweede lid, Aanvullend Protocol I.
76 Vgl. artikel 51, vijfde lid, onder b, Aanvullend Protocol I.
77 Zie: W. Baron & P.A.L. Ducheine, 'De luchtaanval in Kunduz – Targeting en oorlogsrecht', in: *Militaire Spectator* 179 (2010) 10, pp. 493-506.
78 Kelsey, t.a.p.
79 Kelsey, p. 1441.
80 Artikel 1 en 2 van het *Verdrag (V) nopens de rechten en verplichtingen der onzijdige Mogendheden en personen in geval van oorlog te land*; 's-Gravenhage, 18 oktober 1907, Stb 1910, 73.

FOTO AVDD, R. GIEING

Cyberoperaties onderscheiden zich van meer traditionele militaire operaties en vragen om een aanvulling en herinterpretatie van het juridische raamwerk

zonder draad' die in particuliere handen zijn, mogen wel worden benut.[81] Gebruik van internetknooppunten en verbindingen in een andere staat zou dan geen inbreuk zijn op de neutraliteit.[82]
Georgië zocht tijdens de cyberaanval in de oorlog in 2008 zijn toevlucht tot het buitenland om de internetactiviteiten te kunnen voortzetten.[83] Hiervoor werd gebruik gemaakt van lokale faciliteiten van civiele bedrijven in het buitenland zonder de expliciete instemming of de toestemming van de betrokken staten.[84] Met deze actie pareerde Georgië de cyberaanval en kon het de verbindingen met – onder meer – zijn troepen in stand houden.

ROE en SOFA's

Het tweede rechtsregime betreft *Rules of Engagement* (ROE). In de NATO ROE catalogus – MC 362 – komen we 'cyber' ROE (nog) tegen in de vorm van *Information Operations* en *Electronic Warfare*. De Amerikaanse *Standing Rules of Engagement* bevatten sinds 2000 specifieke instructies voor cyberoperaties.[85] Een van de vraagstukken op dit gebied is het (geografische) toepassingsbereik van ROE. Bij cyberoperaties zouden informatiesystemen van niet-betrokken partijen bij het conflict of de operatie kunnen worden gebruikt. De vraag is of de normale voorgeschreven ROE die de *Area Of Operations* definieert, dit toestaat.
Afspraken over de (juridische) status van troepen in het buitenland en hun privileges, zoals het gebruik van de ether, worden meestal in statusovereenkomsten, *Status of Forces Agreements* (SOFA's), vastgelegd.[86] Bestaande, langlopende SOFA's (bijvoorbeeld de NAVO-SOFA) hebben nog geen rekening kunnen houden met cyberoperaties. Het spreekt voor zich dat technologische ontwikkelingen de juridische praktijk inhalen. Cyberoperaties zullen daarom hun sporen achterlaten in toekomstige statusverdragen.

Mensenrechten

De verplichtingen uit de mensenrechtenverdragen zijn primair beperkt tot het *territoir* van

81 Idem, Art. 8.
82 Vgl.: W.A. Owens, K.W. Dam, & H.S. Lin (Eds.), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, D.C: The National Academies Press, 2009, p. 270.
83 Estland, Polen en de VS; Korns en Kastenberg, p. 60.
84 Ibid., p. 66-67.
85 Zie de bijlage over Information Operations. Tegenwoordig: SROE/SRUF (*Standing Rules for the Use of Force*).
86 Dit geldt voor situaties waarin staten niet met elkaar zijn verwikkeld in een gewapend conflict. In conflictsituaties volgt de status van troepen op vijandelijk grondgebied uit het humanitair oorlogsrecht.

de Verdragspartijen in kwestie. In toenemende mate beïnvloedt echter ook *extraterritoriaal* gedrag van staten de mensenrechten van individuen. Een belangrijke vraag daarbij is of cyberoperaties binnen het toepassingsbereik van mensenrechten vallen.

Dat lijkt zo te zijn indien een staat als gevolg van militaire operaties effectieve controle over een bepaald gebied uitoefent. Die controle kent verschillende verschijningsvormen.[87] Ten eerste als een bezettende mogendheid in de zin van het oorlogsrecht. Ten tweede als een staat met instemming van een andere staat publiek gezag uitoefent dat normaliter door die andere staat zelf wordt uitgeoefend.[88] Ten derde via een mandaat van de VN-Veiligheidsraad, zoals het geval was bij KFOR en UNMIK in Kosovo.

Zodra er geografisch effectieve controle bestaat, worden alle militaire operaties in dat gebied door mensenrechten bestreken. Dat geldt ook voor cyberoperaties, waarbij mensenrechten zoals privacybepalingen van invloed zullen zijn op die operaties.

Conclusie

Nederland is reeds geconfronteerd met operaties in het cyberdomein. Uit de strategische context van cyberoperaties vallen zeer diverse kenmerken af te leiden die (in)direct van invloed zijn op het juridische raamwerk voor militaire cyberoperaties.

Een compleet strategisch raamwerk is hard – en snel – nodig, en met de *Nationale Cybersecurity Strategie* is hiertoe een eerste aanzet gegeven. Het strategische raamwerk is echter incompleet zolang een overkoepelende *Grand Strategy* voor binnen- én buitenlands veiligheidsbeleid ontbreekt. De wel beschikbare *Nationale Veiligheidsstrategie* heeft een binnenlandse focus; de 'internationale rechtsorde' als vitaal nationaal belang ontbreekt.

De Defensievisie op militaire cyberoperaties zal op beide bestaande strategische concepten moeten worden afgestemd. Ze zal zeker rekening moeten houden met het vitale belang van de internationale rechtsorde: niet alleen vanwege de grondwettelijke verankering, maar ook vanwege de tweede grondwettelijke hoofdtaak.

Het juridische raamwerk zelf bestaat enerzijds uit rechtsbases als grondslag voor operaties en anderzijds uit rechtsregimes die van toepassing zijn tijdens operaties. Daarbij kan een operatie vanuit meerdere rechtsbases worden ingezet. De uitvoering kan weer door meerdere rechtsregimes bestreken worden.

Het raamwerk is regelmatig gebaseerd op klassieke, defensieve, reactieve taakstellingen en blijkt ook betrekkelijk monodisciplinair te zijn. Veel militair relevante wetgeving of verdragen zijn kinetisch georiënteerd, omdat 'cyber' zijn intrede nog niet (overal) heeft gedaan. In nationale rechtsbases en rechtsregimes vraagt dit op een aantal punten om herbezinning en aanpassing, bijvoorbeeld waar het beveiliging en inlichtingen betreft.

Internationale rechtsbases en rechtsregimes zijn naar hun aard adaptiever en flexibeler. Het non-kinetische karakter van cyberoperaties genereert ook hier serieuze vraagstukken. Binnen het *ius ad bellum* spelen twee vragen een rol: vallen cyberoperaties onder het geweldsverbod? En gelden ze als gewapende aanval, waardoor staten in zelfverdediging kunnen reageren?

In het oorlogsrecht spelen er vergelijkbare kwesties. Wanneer heeft een cyberoperatie voldoende 'geweldsintensiteit' en is dus sprake van een gewapend conflict? Of gelden cyberactiviteiten wel als 'vijandelijkheden', en hoe pakt een *collateral damage assessment* uit?

Met cyberoperaties betreedt de krijgsmacht een nieuwe dimensie, een nieuw strijd- en tijdperk. Ondanks alle vraagstukken die dit oproept, blijkt in ieder geval duidelijk dat ook dit nieuwe slagveld niet rechteloos is: ook tijdens oorlog geldt immers het recht.[89] ■

87 Ducheine (2008), p. 405.

88 Deze situatie is hiervoor als derde normale uitzondering genoemd.

89 Naar het motto van de MJD: *et inter arma vigent leges.*