TOESPRAAK

Legal framework for military cyber operations

Toespraak gehouden ter gelegenheid van het Defensie Cyber Symposium
gehouden op 27 juni 2012 te Breda

DOOR KOLONEL DR. PAUL DUCHEINE[1]

Excellenties, generaals, dames, mijne heren,

Het is mij een genoegen vandaag met u van gedachten te kunnen wisselen over het juridische raamwerk voor militaire cyber operaties.

Dat wil zeggen: die 'gedachten-wisseling' pakt voorlopig éénzijdig uit, omdat ik het komende half uur vooral mijn gedachten zal uitdragen, terwijl u de rol van (ik hoop: een actieve) toehoorder hebt. Na de koffiepauze is er gelukkig een moment van revanche: tijdens de paneldiscussie is ruimte voor uw gedachten en ideeën.

Om uw actieve inbreng te bevorderen zal ik hier en daar prikkelende stellingen (en beelden) hanteren. Stellingen en beelden die uiteraard geheel voor mijn rekening komen, en alleen een constructieve discussie beogen. Het is dan ook eigenlijk overbodig te benadrukken dat mijn presentatie niet per se de mening van de minister van Defensie vertegenwoordigt (al valt dat natuurlijk niet uit te sluiten).

Het doel van mijn presentatie vandaag is tweeledig: ik wil de ratio én de grove lijnen van het juridisch raamwerk voor militaire cyber operaties schetsen. En ik wil daarnaast enkele aspecten en opvallende zaken in dat raamwerk toelichten.

Dames en heren,

Sprekend over het juridische raamwerk voor militaire cyber operaties, doe ik dat met een bepaalde achtergrond: niet alleen die van militair en jurist, maar, zoals sommigen van u ook weten, ook als oud-Genist. Ik leg dat kort uit zodat eenieder weet wat dat voor mij betekent.

Genisten, leden van het 264 jaar oude regiment genietroepen (het oudste regiment van de Koninklijke Landmacht 15 mei 1748), dragen zorg voor:

- mobiliteit ten eigen faveure (beweging),
- contra-mobiliteit ten nadele van onze opponent (hindernissen dus),
- en bescherming.

Naar mijn stellige overtuiging hebben militair-juristen (zoals ik) diezelfde drieledige taak, hoewel het instrumentarium uiteraard verschilt: in plaats van pikhouweel en schop,

[1] Kolonel P.A.L. Ducheine is universitair hoofddocent Cyber Operations aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie

gebruiken mijn collega's en ik wetten, verdragen, en **vooral** het vermogen om toepassingsgericht die regelgeving te kunnen interpreteren. Ik ben dus een op de praktijk (= op militaire operatiën) en op effectiviteit gerichte militair-jurist.

Deze driedeling slaat niet alleen op mijn huidige professie, ze past - zoals luitenant-generaal Schnitger in november 2011 in zijn voordracht voor de Koninklijke Vereniging tot Beoefening van de Krijgswetenschappen (KVBK) concludeerde - óók op militaire cyberoperaties:

Ik citeer: "Zo zijn onze taken in Cyber te vergelijken met taken van de Genie:

- Via Cyber kunnen en moeten wij ons beschermen;
- Cyber biedt mogelijkheden om tegenstanders in hun bewegingen te belemmeren: contra-mobiliteit;
- En ten slotte is Cyber een operationeel vermogen waarmee we eigen mobiliteit genereren."[2] Einde citaat.

Met andere woorden: ik sta dus – ook in het cyber domein – voor deze driedeling: mobiliteit, contra-mobiliteit en bescherming. Dat gezegd hebbende, wordt het tijd om de inhoud van mijn presentatie toe te lichten.

Om met onze gedachten – nu en straks – op één lijn te zitten wil ik ter introductie twee onderwerpen aanstippen. Ten eerste (beknopt): wat verstaan we (of in ieder geval: wat versta ik) onder militaire cyberoperaties. En ten tweede (uitgebreider): wat is de ratio van een juridisch raamwerk.

Daarna zal ik militaire cyberoperaties in een context plaatsen. Ik doe dat door de grondwettelijke doelomschrijving voor de krijgsmacht te analyseren, en door strategische documenten te gebruiken.

De kern van mijn betoog bestaat uit een houtskoolschets van het juridische raamwerk zelf. Ik zal me tot de hoofdlijnen beperken. Aan de hand van enkele voorbeelden belicht ik afzonderlijke delen van dit raamwerk. Deze voorbeelden bieden aanknopingspunten voor gaten, onduidelijkheden, of issues die de komende tijd aandacht verdienen. Ik kom daar in mijn conclusies op terug.

1. Introductie

Dames en heren, als eerste dus een korte introductie om het onderwerp van deze presentatie helder te maken.

Militaire cyber operaties

Militaire cyber operaties zijn in mijn ogen:

- operaties die zich afspelen in het digitale domein;
- waarbij militairen betrokken zijn, hetzij onder verantwoordelijkheid van de minister van Defensie dan wel onder civiel gezag;

[2] S. Schnitger, 21 Nov 2011 voordracht voor KVBK, Den Haag, in: *Intercom*, 2011-4, p. 17-20, zie <www.vovklict.nl/index.php/intercom/intercom-2011>.

- (in binnen dan wel in buitenland);
- die een passief, reactief, proactief of actief kenmerk kunnen hebben;
- en die (in de Nederlandse invulling) dus: defensieve en offensieve maatregelen, alsmede het vergaren van inlichtingen betreffen.[3]

Voor de definitie van het digitale domein sluit ik aan bij het gezamenlijke rapport van de AIV (= Adviesraad Internationale Vraagstukken) en de CAVV (= Commissie van Advies inzake Volkenrechtelijke Vraagstukken) *Digitale Oorlogvoering*[4] waarin dit omschreven is: *"Het geheel van ICT-middelen en ICT–diensten. Hierbij horen ook alle niet met internet verbonden netwerken of andere digitale apparaten".*[5]

Deze definitie is breder dan die van *cyber warfare* (digitale oorlogvoering) zoals het AIV die gebruikt. Digitale oorlogvoering of *cyber warfare is: "het uitvoeren van militaire operaties die erop zijn gericht om met digitale middelen computersystemen of netwerken van een tegenstander te verstoren, misleiden, veranderen of vernietigen".*[6]

Dat heeft in ieder geval twee consequenties. Ten eerste: in mijn optiek is er in cyber operaties bijvoorbeeld óók ruimte voor het gebruik van *social media* om strategische boodschappen of narratives uit te dragen, bijvoorbeeld ter ondersteuning van / of zelfs als alternatief voor een militaire actie, zonder dat daarbij aan het schadecriterium uit de AIV-definitie is voldaan. En ten tweede: mijn definitie omvat ook de inzet van cyber middelen ter ondersteuning van civiele autoriteiten: bijvoorbeeld in bijstand aan de Nederlandse politie onder gezag van de Officier van Justitie (en waardoor deze inzet in deze analyse van het juridische kader moet worden meegenomen).

Zoals bij elke definitie – en bij ieder thematisch symposium – bestaat ook hier het gevaar van overfixatie. Door de focus op het onderwerp, kan de context uit het oog verloren worden. Onze dagvoorzitter, commodore prof. Frans Osinga heeft dit eens getypeerd als 'Kijken door een rietje'.

Ik wil dit gevaar pareren: voordat de krijgsmacht (of ikzelf) wordt beticht van een coup-poging of het kapen van het cyber domein, is het goed te realiseren dat militaire cyberoperaties slechts een klein deel van het totale cyber security[7] spectrum bestrijken (zie figuur 1).

---

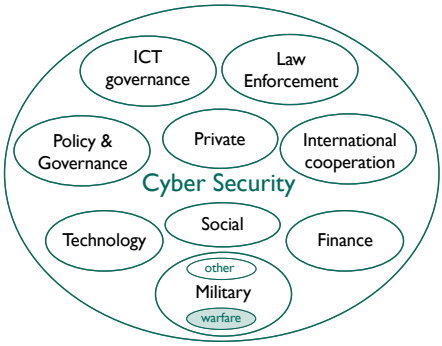
[3] Vergelijk: P.A.L. Ducheine & J.E.D. Voetelink (2011) 'Cyberoperaties: naar een juridisch raamwerk', in: Militaire Spectator, Vol 180, nr. 6, p. 273-286, p. 276.

[4] Hierna: het AIV-rapport.

[5] Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV (2011): Digitale oorlogvoering, Den Haag: AIV no. 77; CAVV no. 22, zie <www.aiv-advice.nl>, Bijl. III.

[6] Idem, p. 8.

[7] Digitale veiligheid of cyber security: het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van informatie- en communicatietechnologie (ICT) of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie. Zie *Kamerstukken* II, 2010/11, 26 643, nr. 174: Nationale Cyber Security Strategie (2011).



Figuur 1: Maatregelen in cyber security

Het gros van de cyber security activiteiten of maatregelen is namelijk a. privaat en b. civiel van aard. Zonder uitputtend te willen zijn, betreft cyber security vooral governance in algemene zin, governance in cyber space, rechtshandhaving, internationale samenwerking (o.a. verdragen) danwel financiële en technologische maatregelen (o.a. voor Research & Development). M.a.w.: slechts een *klein* deel van cyber security betreft militaire cyberoperaties, en slechts een *fractie* daarvan betreft Cyber Warfare of digitale oorlogvoering. Oftewel: van een coup is dus geen sprake, en ondanks het belang van ons werk, doen we er als militairen (op de werkvloer) goed aan een bescheiden positie in te nemen, die past bij ons beperkte aandeel in cyber security.

Legitimiteit en het Legal Framework

Deze relativering brengt me bij de ratio van een legal framework.[8] Ik doe dat aan de hand van drie vragen: waarom is dit belangrijk? Voor wie? En wanneer? De antwoorden zoek ik aan de hand van het beginsel van legitimiteit.[9]

Legitimiteit kennen we als een van de grondbeginselen van militair optreden. Legitimiteit kent een sociale én een juridische component (zie figuur 2).[10] De sociale component betreft het draagvlak voor een missie. De juridische component betreft (1) een adequate rechtsgrondslag voor militaire interventie – de rechtsbasis – en vraagt daarnaast (2) om de naleving van regels die de uitvoering van de operatie beheersen: de rechtsregimes.[11] Juridische en sociale legitimiteit zijn nauw met elkaar verbonden: juridische legitimiteit draagt bij aan de sociale legitimiteit en omgekeerd. Bovendien is draagvlak nodig om bijvoorbeeld een rechtsregime te wijzigen. Maar vooral draagt legitimiteit op korte en lange termijn bij aan de effectiviteit van operaties.

---

[8] Zie onder andere: Paul Ducheine & Eric Pouw (2012). 'Legitimizing the use of force' (pp. 33-46) en 'Controlling the use of force' (pp. 67-80). In: Beeres, vd Meulen, Soeters, Vogelaar (Eds.), *Mission Uruzgan - Collaborating in Multiple Coalitions for Afghanistan* Amsterdam: University Press; P.A.L. Ducheine & T.D. Gill (2011). De legitimering van statelijk geweldgebruik na 9/11. In F. Osinga, S. Soeters & W. van Rossum (Eds.), *Nine eleven: tien jaar later* (pp. 216-234). Amsterdam: Boom.

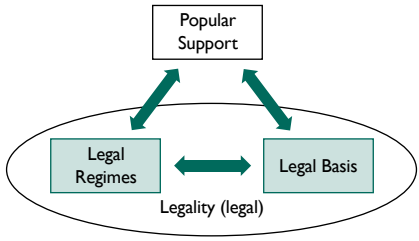
[9] Zie onder andere: P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding; Een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme* (diss. UvA), Nijmegen: Wolf Legal Publishers (2008).

[10] Koninklijke Landmacht (2009). *Land Doctrine Publicatie: Militaire Doctrine voor het Landoptreden (LDP I)*. Amersfoort: OTC Operatiën 107.

[11] Ducheine (2008). *Krijgsmacht, Geweldgebruik & Terreurbestrijding*, Nijmegen: Wolf Legal Publishers , p. 24-28.

Minstens zo belangrijk is de rol van legitimiteit als een beginsel van de democratische rechtsstaat. De krijgsmacht maakt deel uit van die 'rechts-staat' en moet die rechtsstaat zelfs beschermen, maar wel binnen de spelregels van die rechtsstaat.

In figuur 2 heb ik de relatie tussen de verschillende componenten van legitimiteit geschetst. Ik wil de samenhang én de ratio aan de hand van een voorbeeld demonstreren.



Figuur 2: Legitimiteit van militaire operaties

U zult zich allemaal goed herinneren dat na 9/11 de militaire reactie van de VS (en bondgenoten) tegen Al Qaida en Afghanistan – Operation Enduring Freedom en de Global War on Terror – op een breed draagvlak kon rekenen. In binnen- en buitenland. De rechtsbasis voor Enduring Freedom – zelfverdediging naar aanleiding van een gewapende aanval in de zin van het VN Handvest – werd breed onderschreven. Denkt u maar aan resolutie 1368 en 1373 van de Veiligheidsraad die dit beroep op zelfverdediging als grondslag (rechtsbasis) impliciet erkenden. Echter, dit brede draagvlak begon scheurtjes te vertonen, toen enkele rauwere kanten van de zogeheten 'Global War on Terror' (GWoT) zichtbaar werden, bijvoorbeeld in Guantanamo Bay. De toepassing van het oorlogsrecht en mensenrechten in de uitvoering van de GWoT stond ter discussie, waarmee het draagvlak afkalfde.

Dit draagvlak leed vervolgens zwaar onder de omstreden operatie Iraqi Freedom die een adequate rechtsbasis miste. De miljoenen betogers die begin 2003 wereldwijd de straat opgingen, getuigen daarvan. En het draagvlak kalfde verder af in de uitvoering van de operatie toen foto's van de omgang met gevangen in 'Abu Ghraib' in de media verschenen.

Met de erosie van het draagvlak kwam de GWoT als geheel uiteindelijk onder grote druk te staan, en het is dan ook niet vreemd dat deze term tegenwoordig niet meer (in officiële publicaties) gebruikt wordt.

Terug naar de ratio achter dit alles. Dit historische voorbeeld is niet uniek: de legitimiteit van moderne militaire operaties staat dus nadrukkelijk in de schijnwerpers, ook in Nederland. Of zoals onze minister het verwoordde:

> *"Voor iedere staat geldt dat geweldstoepassing en uitzending van militairen in overeenstemming dient te zijn met het [nationale en] internationale recht. Nederland kent aan deze eis extra zwaar gewicht toe, in het licht van o.a. de grondwettelijke verplichting voor de regering de ontwikkeling van de internationale rechtsorde te bevorderen en de reputatie van Den Haag als «juridische hoofdstad van de wereld».»*[12]

[12] *Kamerstukken* II 2006-07, 29 521, nr. 41, p.3. Zie ook o.a. Ducheine & Gill (2011), 'De legitimering van statelijk geweldgebruik na 9/11', in: F. Osinga, S. Soeters, W. van Rossum (eds.), *Nine Eleven. Tien jaar later* (NL ARMS 2011), Amsterdam: Boom, p. 216 e.v..

Terugkomend op de 'waarom' vraag, is met deze voorbeelden duidelijk dat legitimiteit (inclusief de juridische component) cruciaal is voor de effectiviteit van militaire operaties. Anders gezegd: zonder respect voor het juridisch kader geen legitimiteit (en geen draagvlak), en zonder draagvlak geen operaties, laat staan effectieve. En zonder draagvlak geen krijgsmacht trouwens.

De volgende vraag is: voor wie is dat juridische kader relevant? Hierover kan ik kort zijn:
- voor iedereen die betrokken is bij de besluitvorming over operaties;
- voor iedereen die militaire operaties (en dus ook militaire cyberoperaties) uitvoert of leidt;
- dit geldt voor burgers en militairen op alle nationale en internationale niveaus (politiek-strategisch, militair-strategisch, operationeel en tactische niveau).

Het gaat dus om de regering, de minister van Defensie, de CDS en de Directeur Operaties, maar ook om de commandant van het cyber detachement die daadwerkelijk acties uitvoert, én de militair die aan de knoppen zit.

Na dit antwoord op de tweede vraag rest de derde: wanneer? Het antwoord hierop is nog korter: altijd - continue.

Zowel in de *besluitvorming* omtrent inzet van militaire cyberoperaties, waarbij het accent op de rechtsbasis zal liggen, als tijdens de *uitvoering* van operaties zelf, waarbij vooral aandacht zal bestaan voor de rechtsregimes die op uitvoering toezien. Bovendien dient voor, tijdens en na operaties *verantwoording* te worden afgelegd:
- op de verschillende niveaus (politiek-strategisch tot tactisch)
- over zowel besluitvorming als uitvoering (bevelvoering)
- op allerlei gebied: politiek, operationeel, publiek, strafrechtelijk, moreel etc.
- niet in de laatste plaats ook achteraf; soms jaren later, zoals ook het rapport van de Commissie Davids[13] of Srebrenica (NIOD)[14] duidelijk maakte.

2. Context

Dames en heren, hiermee heb ik voldoende gezegd over de ratio van het raamwerk. Het wordt tijd om stil te staan bij de context hiervan. Ik bespreek twee aspecten: (1) de constitutionele inbedding, die mij vervolgens in een vloeiende beweging brengt bij de (2) de strategische inbedding van militaire cyberoperaties.

Constitutionele inbedding

Militaire cyberoperaties worden primair bepaald door de grondwettelijke doelomschrijving van artikel 97, en ik heb hem iets anders verwoord dan u mogelijk gewend bent:

> *"Ten behoeve van (a) de verdediging, en (b) de handhaving en de bevordering van de internationale rechtsorde, alsmede (c) ter bescherming van de [andere vitale] belangen van het Koninkrijk, is er een krijgsmacht".*

Voor deze drie doelen kan de krijgsmacht – ook in cyber – worden ingezet. Om ook hier al te ambitieus gedrag van defensie de kop in te drukken is het goed te beseffen wat de Grondwetgever bedoeld heeft.

[13] Commissie van Onderzoek Besluitvorming Irak (W.J.M. Davids, voorzitter), Amsterdam: Boom (2010).
[14] Nederlands Instituut voor Oorlogsdocumentatie, *Srebrenica, een 'veilig' gebied,* Amsterdam: Boom (2002).

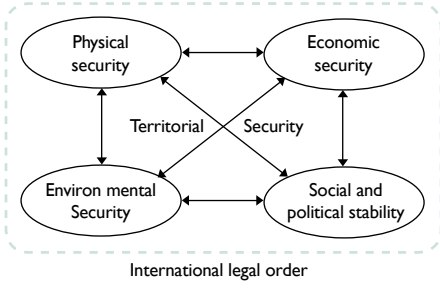
De eerste twee doelomschrijvingen spreken voor zich: ze vormen de basis voor de 1e en 2e hoofdtaak: de algemene verdedigingstaak en (populair gezegd) crisisbeheersingsoperaties. Het gaat daarbij meestal om buitenlandse operaties.

De derde doelomschrijving is echter dusdanig ruim geformuleerd dat "het beschermen van de belangen van het Koninkrijk" op velerlei belangen zou kunnen slaan. Dat is echter schijn. Met belangen worden namelijk de "vitale belangen van het Koninkrijk" bedoeld.[15]

Maar wat zijn dan Nederlandse vitale belangen?

De *Nationale Veiligheids Strategie* uit 2006 definieert dit als volgt. Belangen zijn vitaal als *"door het deels of geheel verstoord raken of wegvallen van dat belang het functioneren v/d staat en samenleving in potentie of feitelijk in gevaar komt."* [16] Dat zal niet het geval zijn als Unilever's productielijn van Blue Band verstoord wordt, maar mogelijk wel als de aanvoer van ruwe aardolie richting Rotterdam stagneert, of als KPN volledig in buitenlandse handen valt.

Deze strategie benoemt *vijf* nationale vitale belangen die samen onze 'nationale veiligheid' bepalen: territoriale, fysieke, ecologische en economische veiligheid alsmede politieke & sociale stabiliteit. Deze strategie heeft echter één mankement: omdat dit een binnenlandse veiligheidsstrategie is, ziet ze één vitaal belang over hoofd: internationale rechtsorde (zie figuur 3).



Figuur 3: Vitale belangen van het Koninkrijk

Het missende belang vinden we in artikel 90 van de Grondwet dat de regering opdraagt "de ontwikkeling van de internationale rechtsorde" te bevorderen.[17]

Aangevuld met het vitale belang "internationale rechtsorde" levert dit het overzicht op van onderling afhankelijke vitale belangen, die zowel binnenlandse als internationale voelsprieten hebben: ook gebeurtenissen in het buitenland raken direct of indirect onze vitale belangen.[18]

---

[15] P.A.L. Ducheine, 'Parliamentary Involvement in the Netherlands' Military Operations Abroad', in: S. Hardt, L. Verhey & W. van der Woude (Eds.), *Parliaments and Military Missions, Groningen: Europa Law Publishing* (2012), pp. 15-32. Zie in die zin ook: Soetendal, E. (1997). 'Boeiend en geboeid, enige beschouwingen over de wijziging van de defensiebepalingen in de Grondwet'. In: Militair Rechtelijk Tijdschrift, Vol 90, nr. 9, pp. 285-297, p. 289-290. Soetendaal's analyse van de te beschermen belangen komt uit op (een aantal) van de vitale belangen uit de Nationale Veiligheidsstrategie (*Kamerstukken* II 2006-07, 30 821, nr. 1).

[16] Kamerstukken II 2006-07, 30 821, nr. 1.

[17] Art. 90 Grondwet.

[18] Zie P.A.L. Ducheine & J.E.D. Voetelink (2011) 'Cyberoperaties: naar een juridisch raamwerk', in: *Militaire Spectator,* Vol 180, nr. 6, pp. 273-286.

Nationale veiligheid

Het zou trouwens goed zijn dit zesde vitale belang aan de trits uit de Nationale Veiligheids Strategie toe te voegen, of in een – helaas nog niet bestaande en node gemiste – expliciete Nederlandse *grand strategy* neer te leggen.[19]

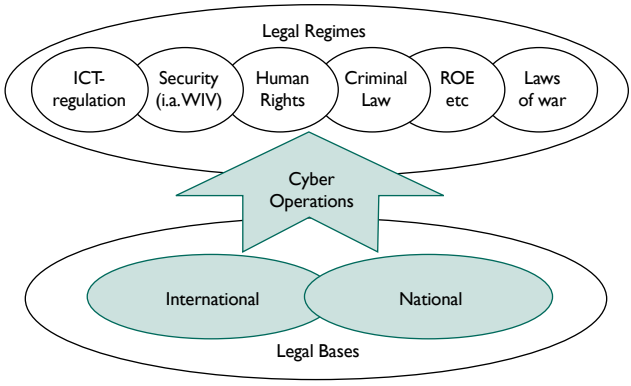
Hoe dit ook zij, kijkend naar de zes vitale belangen, valt de breedte van deze derde doelomschrijving op. Daarbij is het natuurlijk niet zo dat defensie zich opwerpt als verantwoordelijke voor het totale cyber domein. Dat is een misvatting.

Op grond van ons staatsrecht zullen de primair verantwoordelijke civiele bestuurders hun verantwoordelijkheden zo lang mogelijk dragen. Zelfs in staatsnood (en in het staatsnoodrecht) is dit het uitgangspunt.[20] Als daarbij bijstand gewenst is, zal defensie – net zoals in andere gevallen – bijspringen, zonder dat dit verantwoordelijkheden aantast.

Deze doelomschrijving impliceert in ieder geval dat defensie cyberoperaties binnen de drie hoofdtaken moet kunnen uitvoeren. Zowel in het buitenland, doorgaans in multinationaal verband, als in het binnenland, maar dan veelal onder civiel gezag.

3. Juridisch kader

Dames en heren, dit brengt me ten slotte bij het juridische kader zelf (zie figuur 4).



Figuur 4: Juridisch kader cyber operaties

Vóórdat over inzet besloten wordt dient er namelijk een rechtsbasis te bestaan, dat hebben we net gezien. En tijdens die operaties moet conform de vigerende normen worden gehandeld. En, om het nog maar eens te benadrukken, over het geheel wordt voortdurend – op alle niveaus verantwoording afgelegd. Met deze typering heb ik de kern van het raamwerk geschetst.

Eerst een opmerking over de rechtsbasis: die vinden we – afhankelijk van de opgedragen taak en context – in ons nationale recht (voor binnenlandse operaties) dan wel in het internationale recht (voor operaties in het buitenland). Om een voorbeeld te noemen, stel dat Nederland (of een bondgenoot) het slachtoffer is van een gewapende aanval (zoals 9/11 of een cyber variant) dan zal Nederland

[19] P.A.L. Ducheine (2008) *Krijgsmacht, Geweldgebruik & Terreurbestrijding. Een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme*, Nijmegen: Wolf Legal Publishers, p. 20.
[20] Ducheine (2008), pp. 103-119.

een beroep kunnen doen op het recht op zelfverdediging (uit het VN Handvest) om – in reactie – een cyber aanval te lanceren. De AIV heeft zich hier vorig jaar uitgebreid over uitgelaten. Andere bases zijn 'consent' of een autorisatie van de Veiligheidsraad, dan wel nationale bases, bijvoorbeeld op grond van de Wet op de Inlichtingen en Veiligheidsdiensten 2002 (WIV).

Nadat besloten is een cyberoperatie te starten, spelen rechtsregimes een belangrijke rol. En daarbij passen drie opmerkingen. Ten eerste kunnen tijdens één operatie meerdere regimes tegelijkertijd van toepassing zijn. Denkt u maar aan de cyber operaties tijdens een gewapend conflict, waarop zowel het oorlogsrecht, ROE en mensenrechten van toepassing zullen zijn.

Ten tweede kunnen meer operaties simultaan lopen, ieder vanuit een specifieke rol en ieder omkaderd door een of meer regimes. Bijvoorbeeld: de CDS stuurt een actie aan omkaderd door het oorlogsrecht, terwijl de MIVD flankerend in Nederland cyberbevoegdheden inzet omkaderd door de WIV en de KMar (al dan niet met bijstand op grond van de Politiewet uit het Joint ISTAR Commando) daarnaast een opsporingsonderzoek start in het strafrechtelijke domein.

Ten derde: de rechtsregimes zijn dus in een aantal gevallen sterk gekoppeld aan rollen (en aan rechtsbases), die weer te herleiden zijn op cyber security paradigma's zoals governance, beveiliging, rechtshandhaving, crisisbeheersing of in het uiterste geval: oorlogvoering.

Als u dit schema zo ziet, bekruipt u wellicht het gevoel dat ik u 'oude wijn in nieuwe zakken' aan het verkopen ben. Dat is juist! Maar: slechts ten dele. Ik leg dat uit.

Enerzijds is het waar dat dit stramien op alle activiteiten van de krijgsmacht (incl. MIVD en KMar) van toepassing is. Wat dat betreft niets nieuws. Houd ik dan een overbodig pleidooi? Het antwoord is zoals gezegd: neen. Er zijn namelijk – zoals altijd bij de invoering van nieuwe technologie, nieuwe methoden en middelen van oorlogvoering – inpassingen en aanpassingen nodig.

De algemene bepalingen in wetten of verdragen sluiten niet altijd naadloos aan op de invoering van het luchtwapen, de ontwikkeling van *drones* of de toekomstige toepassing van nanotechnologie. Dat is ook bij cyber het geval.

Neen, ik verkoop u dus naast **oude** wijn, óók **nieuwe**, sterker nog: vaak in **oude** zakken. Ik geef u drie redenen waarom ik dat doe.

Ten eerste moeten bestaande bepalingen in het licht van nieuwe beschikbare technologie opnieuw **geïnterpreteerd** worden. De AIV heeft daartoe een eerste aanzet gegeven door uit te leggen wanneer een cyber aanval als een gewapende aanval in de zin van het VN Handvest kan gelden.

Maar daarmee is het werk nog niet klaar. In een volgende slag zullen dit soort begrippen in doctrine en in operatieplannen moeten worden toegepast. We zullen er ook mee moeten oefenen. Met name ook in de toepassing van cyber in het oorlogsrecht. Om maar een paar andere voorbeelden te noemen.

- Welke cyberdoelen zijn (kinetisch) uit te schakelen? Neem bijvoorbeeld data centres. M.a.w. zijn dat militaire doelen in de zin van het oorlogsrecht? Met die vraag laait de oude discussie inzake *dual-use targets* (bv transformator) in het oorlogsrecht weer op.
- Vervolgens: als ze aan te vallen zijn: welke middelen moeten we dan gebruiken: gewone 500 ponders of alleen smart weapons, zoals we tegen transformatorstations ook bij voorkeur een carbon-fibre bomb, (de CBU-94 "Blackout Bomb") inzetten?
- En bovendien: welke bijkomende schade moeten we in een *collateral damage* assessment betrekken: alleen de 1e orde effecten (dataverlies) of ook 2e orde (zoals stroomuitval en daardoor crashende

servers) of zelfs 3e orde effecten (schade die soms zelfs maanden na-ijlt)?
- En: welke voorzorgsmaatregelen moeten we bij een cyber aanval treffen: moeten we voorafgaand aan de aanval de bevolking vragen een backup te maken, zodat *de collateral damage* beperkt blijft?

Het klinkt misschien gek, maar dit zijn serieuze vragen. Ik noem u er nog twee:
- Welke gebruiker van cyber is combattant (of wie neemt direct deel aan gevechtshandelingen) en wie is dat niet? Het ICRC heeft over deze kwestie een niet-onomstreden handleiding geschreven. Nederland moet hierover nog een standpunt innemen, maar onze commandanten werken er dagelijks mee. Hun beslissing of een Al Qaida handlanger die onze passwords steelt een combattant is of niet, maakt het verschil tussen leven en dood.
- En ten slotte: hoe gaan we om met cyberopponenten en cyber infra op neutraal grondgebied?

Ondanks deze brandende vragen is het een misvatting om te denken dat we nu – net als na 9/11 – het oorlogsrecht of het internationale recht intensief moeten **aanvullen of aanpassen**. Het bijzondere namelijk van het internationale recht is dat het vaak flexibel genoeg is om ontwikkelingen te accommoderen: kijk bijvoorbeeld naar het luchtwapen waarvoor nog steeds geen specifiek oorlogsrechtelijk verdrag bestaat.

Neen, integendeel, **kennis en interpretatie** zal vaak volstaan. Dat is ook precies de strekking van de 'Tallinn Manual' for International law in cyber operations waar Nederland en leden van onze Faculteit bij betrokken zijn.

Dat ontslaat ons allemaal niet van de plicht om nu al **keuzes te maken**!! Dat is de tweede reden waarom ik hier niet voor niets sta. Onze commandanten die straks op pad moeten, hebben dan namelijk weinig tijd om uitgebreide studies te plegen. Dat moet wij dus nú doen.

Los van mijn enthousiasme over de kracht van interpretatie (waarbij uiteraard een belangrijke rol voor militair juristen is weggelegd), zal er op een aantal punten inderdaad een **'gat' bestaan**.

Dat is de derde reden waarom mijn pleidooi niet overbodig is. Zo zullen we kennislacunes moeten dichten en zal hier en daar **aanpassing** van wetgeving, en mogelijk van verdragen nodig zijn. Ik geef u drie voorbeelden.
- Ten eerste, onze juridische adviseurs zijn beter thuis in het oorlogsrecht dan in de wereld van ICT-regulering. Daar zullen we iets aan moeten doen. Zelfstandig of in joint ventures.
- Ten tweede, de MIVD beschikt nu over de bevoegdheid om *niet*-kabelgebonden communicatie te onderscheppen (bijvoorbeeld via satelietontvangst). Kabelgebonden interceptie is slechts gericht toegestaan (via taps). Wat nog ontbreekt is de bevoegdheid om ongericht kabelgebonden communicatie te onderscheppen. B.v. emailberichten, tweets of blogs die (op enig moment) via glasvezelverbindingen lopen. Denkt u maar aan het monitoren op trefwoorden. Deze bevoegdheid is weliswaar beoogd, maar ze heeft het levenslicht nog niet gezien.
- Ten derde, de Rijkswet geweldgebruik bewakers militaire objecten voorziet nu alleen in de fysieke beveiliging door het toepassen van fysiek geweld voor de noodzakelijk verdediging van onze fysieke infrastructuur. Volgens mij moeten (en kunnen) we die bevoegdheid op drie punten aanvullen. Ten eerste om ook cyberacties ter beveiliging van onze data (die niet fysiek is) en digitale wegen toe te staan (vanwege cyber bedreiging).[21] Ten tweede moeten we de kring van 'bewakers en beveiligers' ruimer definiëren, zodat bijvoorbeeld speciaal personeel van DefCERT na een inbraak defensief

[21] Ter aanvulling van de recente aanpassing in *Staatscourant* 19 augustus 2008, nr. 159 / pag. 6, die nog steeds op "objecten" betrekking heeft.

'terug kan hacken'. En ten derde zouden we deze bevoegdheid ook in het buitenland moeten kunnen toepassen, zoals België dat in het strafrecht heeft gedaan.[22]

4. Conclusies

Dames en heren, het is tijd om conclusies te trekken.

Het juridische raamwerk omvat dus twee delen: de rechtsbasis en de rechtsregimes. Dit geldt ook tijdens cyberoperaties, vandaar het motto van mijn dienstvak: *et inter arma vigent leges*. Zoals gezegd is dit enerzijds 'business as usual'. Anderzijds is ook nog aanvulling nodig, en vooral interpretatie en keuzes voor de toekomst. Ik zou vijf zaken willen benadrukken:

Ten eerste is in dit raamwerk plaats voor meerdere rollen die de krijgsmacht in de breedte van de drie hoofdtaken vervult: multi-tasking dus.

Ten tweede: dit raamwerk bevat nog een paar blinde vlekken. Zo hebben we relatief weinig kennis van ICT regulering: van de governance van internet. Daar zullen we in moeten duiken, want anders is het alsof we geblinddoekt en gehandicapt in cyber manoeuvreren.

Ten derde: hoewel het weliswaar (vaak) militair juristen zijn die de interpretatie van dit juridische raamwerk ter hand zullen nemen, zijn het commandanten die cyberoperaties uitvoeren, keuzes maken, en daarover verantwoording afleggen.

Met andere woorden (ten vierde), niet alleen **mijn** bloedgroep (militair juristen) moet investeren in kennis van het cyber domein, ook officieren en aanstaande officieren zullen dat moeten doen. Officieren voorbereiden op de integratie van cyber in normale operaties is een activiteit die onder andere hier op de NLDA en de Faculteit plaats kan vinden.

Ten vijfde: voor dat onderwijs, en uiteindelijk om cyber operaties uit te kunnen voeren, doen we ook onderzoek. Dat doen bijvoorbeeld onze studenten. U ziet hiervan een voorbeeld van cadet-vaandrig Jelle van Haaster.[23] Onderzoek komt ook vanuit de faculteit zelf. Dat leidt weer tot publicaties en resultaten die voor het onderwijs en de praktijk te velde bestemd zijn.

Excellenties, generaals, dames mijn heren, ik besluit alsnog met een kleine coup door alvast uw aandacht te vestigen op de neerslag van ons Facultaire onderzoek. De jaarlijkse publicatie van de Faculteit (NL ARMS 2012) draagt deze keer de titel *'Cyber Warfare: critical perspectives'*. Het boek ziet op 30 augustus 2012 bij de Opening van het Academisch Jaar 2012-2013 in de Grote Kerk hier in Breda het levenslicht.[24]

Ik dank u voor uw aandacht, en ik verheug me op het tweede deel van deze gedachtenwisseling…..

---

[22] B.J. Koops, 2012, De dynamiek van cybercrimewetgeving in Europa en Nederland, in: Justitële Verkenningen, Veiligheid in Cyberspace, WODC 2012-1, p. 17-18.

[23] Jelle van Haaster, *Het digitale slagveld* 2.0, Bachelor thesis Krijgswetenschappen, Breda: NLDA (2012), zie < http://defbib.kma.nl/art2/pdf/ada/Haaster, J. van.pdf>.

[24] P. Ducheine, F. Osinga & J. Soeters (eds .), *Cyber Warfare: Critical Perspectives – NL ARMS 2012*, The Hague: TMC Asser Press (2012).