Mythen over digitale oorlogsvoering en recht

Ducheine, P.A.L.

Published in:
Militaire Spectator

'Je hoeft geen zwaard en schild te dragen om ridder te zijn'

Mythen over digitale oorlogvoering en recht

Paul Ducheine sprak onderstaande rede uit bij de aanvaarding van het ambt van hoogleraar 'Military Law of Cyber Security and Cyber Operations' aan de Faculteit der Rechtsgeleerdheid van de Universiteit van Amsterdam, en het ambt van hoogleraar 'Cyber Operations and Cyber Warfare' aan de Faculteit Militaire Wetenschappen van Nederlandse Defensie Academie. Op 27 januari hield hij in Amsterdam zijn oratie, die de redactie van de Militaire Spectator van belang acht voor de lezers en daarom integraal publiceert.

De hoofdredacteur

*Prof. dr. P.A.L. Ducheine - brigade-generaal van de Militair Juridische Dienst**

Aanleiding

Toen ik 33 jaar geleden hoorde dat ik aangenomen was op de Koninklijke Militaire Academie ging mijn jongensdroom in vervulling. Voor de zekerheid had ik me ook in Delft georiënteerd op mijnbouwkunde en civiele techniek. Maar sinds het najaar van 1974, toen het 45e Pantserinfanteriebataljon (RIOG) uit Steenwijk bij ons in Zeeuws- Vlaanderen met de hand aardappelen hielp rooien,[1] had ik mijn zinnen op 'de parel van het zuiden'[2] en de KMA gezet. Met weg- en waterbouw als studierichting, dat dan weer wel.

Vier korte opmerkingen hierover. Ten eerste, de militaire hulp bij de aardappeloogst in 1974 was de eerste keer dat ik in aanraking kwam met het fenomeen 'militaire bijstand en steunverlening'. Verder herinner ik me twee reacties op mijn geslaagde sollicitatie. Mijn vader voorspelde dat ik dan eindelijk ABN zou moeten leren. En mijn docente Nederlands zei kort: 'wat zonde!'. Los van haar licht pacifistische inslag, vond ze het jammer dat ik niet 'echt' zou gaan studeren. En ten slotte: ik had me voorgenomen nooit in het onderwijs te gaan werken. Dát was namelijk *echt* niets voor mij.

U ziet (en hoort) dat de cirkel 'mooi rond' is. Ik doceer hier in Amsterdam 'Krijgsmacht en Staatsrecht', waarin militaire bijstand aan civiele autoriteiten centraal staat. Ik sprak (dankzij de ongevraagde maar achteraf welkome hulp van mijn kamer- en jaargenoten op de KMA) in een mum van tijd ABN. Ik ben inmiddels *echt* afgestudeerd, twee keer zelfs.

* Dit is een aangepast versie van de gesproken tekst. De oratie is ook te volgen via het webcollege op <webcolleges.uva.nl/Mediasite/Play/bca07f4a8a77401d96da8bc0e-8de090d1d>. Een uitgebreidere verhandeling verschijnt in de UvA-Oratiereeks.
De auteur dankt prof. dr. Wim Klinkert, dr. Theo Brinkel, kolonel drs. Han Bouwmeester en mr. Celine Vossen voor de suggesties bij de tekst.

1 Martin Elands, *Het Regiment Infanterie Oranje Gelderland*, Amsterdam: Boom 2006, 124.

2 Zie het Bredase Volkslied: Louis de Morée (tekst) & Tony Smits van Waesberghe (muziek)'Te midden van de paarse heide', <nl.wikipedia.org/wiki/De_Paarse_Heide>.

Ten slotte ontdekte ik vanaf mijn eerste dag bij 41 Pantsergeniecompagnie in Seedorf dat ik als commandant vooral ook kennis moest overdragen. Oftewel dat ik onderwijs moest verzorgen. *It comes with the job*!

Twee werelden

Zoals admiraal Sir George Parr geen geheim maakt van zijn militaire achtergrond,[3] heb ook ik weinig te verbergen. De Amsterdamse en academische mores gebieden dat ik hier vandaag in toga voor u sta. Maar mijn militaire achtergrond – voor zover die onbekend was gebleven – kunt u nog steeds terugvinden in de knopen op de mouwen van deze toga. '*Ik draag een jas met goudgehelmde knopen*'.[4]

BRON AUTEUR

Toga Faculteit der Rechtsgeleerdheid UvA

Velen van u kennen deze strofe uit het lijflied van het 1e Regiment Genietroepen. Deze knopen zijn voorzien van een genie-helm, maar geheel volgens de universitaire tenuevoorschriften zwart uitgevoerd. Deze knopen verbinden mijn beide professionele werelden; de militaire en de academische. Om misverstanden over het primaat voor vandaag te voorkomen zal ik mijn universitaire baret ophouden.

Tijdens deze oratie wil ik u graag een inkijkje geven in mijn twee werelden. En u daarmee inzicht geven in de onderwerpen van mijn leeropdrachten. Ik ben blij dat ik die onderwerpen niet alleen hoef te behappen. Met de hulp van velen van u hier aanwezig, heb ik intussen een klein elftal om mij heen verzameld, waarvoor ik vele sponsoren dankbaar ben.

Als inleiding wil ik eerst met u spreken over *ridders.* Over hun verschillende functies, toen en nu. Daarna wil ik stilstaan bij *veiligheid* en de rol voor de overheid, waaronder de zwaardmacht. Overheidsoptreden dat ingrijpt in de rechten van burgers, dient de legitimiteitstoets te doorstaan. *Legitimiteit* bij het streven naar meer veiligheid vormt mijn verbinding met het recht.Als derde wil ik het digitale domein voor u toelichten: *cyberspace.*

Het vierde onderwerp, het hart van mijn beide leeropdrachten, vraagt om meer toelichting. Met de opkomst van cyberspace en de technologie waarop deze gebaseerd is, ontstaan veiligheidsvraagstukken. Mijn beide leeropdrachten betreffen het veiligheidsvraagstuk *cyber security.* En in het bijzonder de juridische kwesties waarmee defensieonderdelen vervolgens geconfronteerd worden.

Die kwesties verschillen naar gelang de rol die defensieonderdelen vervullen: het beschermen van onze personeelsbestanden vraagt immers om een andere benadering dan het vernietigen van de communicatiesystemen van ISIS. Deze rollen in cyber security koppel ik aan paradigma's: juridische en bestuurlijke kaders waarmee die rollen getypeerd kunnen worden. Ik zal enkele juridische vraagstukken binnen deze rollen beschrijven.

3 Bird and Fortune, *Interview admiral Sir George Parr* <www.youtube.com/watch?v=t0jgZKV4N_A>.

4 Strofe uit de *Kolonel Heemskerck van Beest defileermars* gecomponeerd door luitenant der Genie J. Zwart (periode 1915-1920) voor 1 Regiment Genietroepen, opgericht op 15 mei 1748 door kolonel Nicolaas François de Torcy, baron van Breda. De mars staat ook bekend als 'het Mineurslied', niettegenstaande het feit dat daarmee de andere regimentsonderdelen – pontonniers en sappeurs – tekort wordt gedaan <www.youtube.com/watch?v=n7zfJ3qB2JM>.

Als vijfde wil ik specifiek stilstaan bij *cyber warfare,* oorlog in het digitale domein, en een paar prangende juridische kwesties. Zij vormen het hart van mijn eigen werkzaamheden. Mijn operationele én juridische achtergrond gaan hier hand in hand.

Tot besluit kom ik terug op ridders en zal ik – voor zover dat nog nodig is - uw twijfel of nieuwsgierigheid over de titel van mijn oratie wegnemen. Ik verklap vast dat het een citaat is uit een boek dat ik – ondanks aanbeveling van een jonkvrouw – veel te laat ben gaan lezen. Het betreft *De brief voor de koning* van Tonke Dragt. De ondertitel – mythen over digitale oorlogvoering en recht – is een onderstroom in mijn verhaal. Ik zal een aantal mythen met u delen.

Over ridders….

Ik permitteer me enige vrijheden in deze academische plechtigheid, door in eigen bewoordingen de rol van het klassieke ridderschap samen te vatten. Waarschijnlijk schend ik daarmee de regels voor gedegen historisch onderzoek! Mijn historische collega's zullen het me vast vergeven, zeker die uit het katholieke zuiden.

Ridders hadden een drieledige taak. Allereerst moesten ze veiligheid brengen of bevechten, de draak verslaan. De draak bestond veelal uit vijandige legers. Daarnaast moesten ridders hun leen besturen, hun kasteel, hun gronden. En ten slotte fungeerde een ridder ook als boodschapper, als ambassadeur of gezant van zijn leenheer. Ridders waren zogezegd: krijgsheer, bestuurder én diplomaat. In culturele zin, waren ridders ook de verpersoonlijking van een ideaal; van 'ridderlijk gedrag' van *chivalry*.[5]

Deze drie rollen zien we tegenwoordig terug in wat het 'officiersprofiel' wordt genoemd. Binnen de krijgsmacht wordt de moderne officier getypeerd met de drieslag: krijger - manager – diplomaat.[6] Ik zie de officier van nu, als de ridder van toen. Inclusief het culturele aspect, *chivalry*.

St. Joris en de Draak, Paolo Uccello (1458-1460). Musée Jacquemart-André, Parijs

Het mag duidelijk zijn dat het moderne ridderschap in vele gedaanten komt: bereden, te voet, in de lucht, of op het water.

Veiligheid en legitimiteit

Ik kom op het tweede punt. Ik zal mij de komende jaren bezighouden met veiligheid in het digitale domein. En vooral met de rol(len) van de krijgsmacht daarbij. Legitimiteit van overheidsoptreden speelt daarbij een grote rol, en dit thema is ook de verbinding naar het juridische karakter van mijn leerstoel.

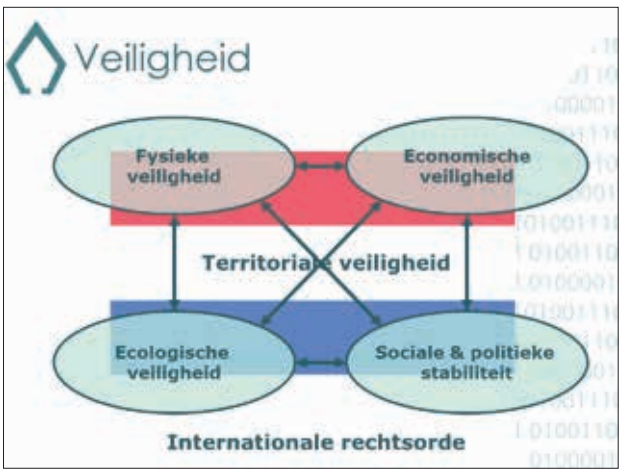
Veiligheid

De leerstoel richt zich op het publieke veiligheidsdomein. De Wetenschappelijk Raad voor het Regeringsbeleid typeert 'veiligheid bieden' als een van de klassieke en 'harde' taken van de overheid.[7] Deze functie wordt in sociale

5 Wat onder meer nog steeds geldt als een grondbeginsel in het humanitaire oorlogsrecht, zie o.a. Terry Gill, 'Chivalry: a Principle of the Law of Armed Conflict?', in: Mariëlle Matthee & Brigit C.A. Toebes, *Armed conflict and international law: in search of the human face. Liber amicorum in memory of Avril McDonald*, The Hague: Asser Press 2013, 33-51.

6 *Studiegids bacheloropleiding Krijgswetenschappen* (NLDA), Breda, augustus 2015, 17: 'Daarbij wordt van iedere officier, cq. leider, verwacht dat hij op zijn niveau competent kan functioneren als "krijger, manager en diplomaat"', via <www.defensie.nl/binaries/defensie/documenten/brochures/2015/09/03/studiegids-bachelor-krijgswetenschappen/STUDIEGIDS_KW_2015-2016.pdf>, benaderd 12-1-2016.

7 In de woorden van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) is veiligheid de belangrijkste functie van de overheid: 'het verzekeren, [...] van de fysieke veiligheid van de burgers'. Zie: WRR, *De toekomst van de nationale rechtsstaat*, Den Haag: Sdu uitgevers 2002, 53.



Figuur 1 Veiligheid

contracttheorieën verklaard. Burgers staan een deel van hun individuele rechten en aanspraken af aan de staat. Denkt u aan privacy, maar ook aan geld (bijvoorbeeld belastingen). In ruil hiervoor verschaft de staat veiligheid aan het collectief. Eigenrichting wordt vervangen door collectieve geschillenbeslechting met onafhankelijke rechters. En het geweldsmonopolie is in handen van de overheid.

Deze klassieke gedachte staat door ontwikkelingen, van economisch tot technisch, onder druk.[8] Alternatieve vormen van geschillenbeslechting zijn beschikbaar; eigenrichting via *Geen Stijl* en andere platforms floreert;[9] particuliere beveiligingsbedrijven (en *contractors*) hebben een opmars gemaakt, inclusief de lobby om daarbij geweld te mogen gebruiken.[10] En omdat veel digitale infrastructuur en diensten in private handen zijn moet de overheid digitale veiligheid onder meer via 'publiek-private' samenwerking realiseren.[11]

De rol en positie van de overheid inzake veiligheid is dus niet 'in beton gegoten' maar evolueert naar gelang noodzaak, mogelijkheden en opportuniteit.

De hedendaagse opvatting over veiligheid heeft zich na 9/11 gevormd. Tot die tijd hanteerden beleidsmakers een dichotoom veiligheidsconcept bestaande uit interne en externe veiligheid.[12] De terreuraanslagen van 15 jaar geleden maakten pijnlijk duidelijk dat externe gebeurtenissen wereldwijde effecten kunnen veroorzaken. Dit geldt trouwens ook voor andere sectoren, zie de kredietcrisis, het vluchtelingenvraagstuk of klimaatverandering.

Het huidige Nederlandse veiligheidsbegrip is gebaseerd op de noties 'nationale veiligheid' en 'vitale belangen'. Deze noties zijn in veiligheidsstrategieën verwoord. De essentie ziet u in de figuur. Vitale belangen zijn: territoriale, fysieke, economische, ecologische veiligheid, politieke en sociale stabiliteit,[13] en de internationale rechtsorde.[14] Deze vitale belangen werken op elkaar in.

De Nederlandse overheid staat uiteindelijk voor de klassieke taak Nederlands vitale belangen te beschermen, ook in het digitale domein. Dat vitale sectoren doorsneden zijn met digitale systemen, en dat deze laatste zelf meestal ook als vitaal aangemerkt zijn, mag helder zijn. Denk bijvoorbeeld aan telecommunicatie.

En daarmee doet zich iets interessants voor. Van oudsher kennen we vitale belangenorganisaties die dit belang als eerste behartigen, denkt u

8 Zie voor het pleidooi om veiligheid (daarom) weer een plaats in de Grondwet te geven: Marjolein van Asselt & Beatrice de Graaf, 'Veiligheid terug in onze Grondwet', in: *NRC Handelsblad*, 13-14 augustus 2013.

9 Zie bijvoorbeeld het Opiniestuk van de (toenmalige) korpschef van de politie Haaglanden, Henk van Essen, 'Het recht op privacy kun je ook verliezen', *Algemeen Dagblad* 20-4-2013, via <www.ad.nl/ad/nl/1012/Nederland/article/detail/3428739/2013/04/20/Het-recht-op-privacy-kun-je-ook-verliezen.dhtml>; 'Politie waarschuwt voor eigenrichting via sociale media', <www.beveiliging.nl/nieuws/politie-waarschuwt-voor-eigenrichting-via-sociale-media>, benaderd 13-1-2016.

10 Adviesraad Internationale Vraagstukken (AIV), *Piraterijbestrijding op zee. Een herijking van publieke en private verantwoordelijkheden* (Rapportnr. 72) 2010; Adviescommissie gewapende particuliere beveiliging tegen piraterij - Geweldsmonopolie en piraterij, *Kamerstukken II* 2011-12, 32 706, nr. 19.

11 Zie de Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie* (NCSS-1 2011), in: *Kamerstukken* II 2010-11, 26 643, nr. 174.

12 E.T. Brainich von Brainich Felth, *Het systeem van crisisbeheersing; bevoegdheden en verplichtingen bij de voorbereiding op en het optreden tijdens crises*, Den Haag: Boom 2004.

13 *Kamerstukken II* 2006-07, 30 821, nr. 2, Strategie Nationale Veiligheid, 3: 'Vitaal belang: belang dat bepalend is voor de instandhouding van de territoriale, fysieke, economische, ecologische veiligheid en voor de politiek en sociale stabiliteit en maakt dat door het deels of geheel verstoord raken of wegvallen van dat belang het functioneren van de staat en de samenleving in potentie of feitelijk in gevaar komt'.

14 *Kamerstukken II* 2012-13, 33 694, nr. 1, Internationale Veiligheidsstrategie – Veilige wereld, veilig Nederland; en *Kamerstukken II* 2014-15, 33 694, nr. 6 bijlage, Beleidsbrief Internationale Veiligheid – Turbulente Tijden in een Instabiele Omgeving.

maar aan de waterschappen voor onze ecologische veiligheid. Maar voor digitale veiligheid is deze belangenbehartiging verkaveld, tot grote zorg van menig digitaal deskundige.[15] Gelukkig betekent dit niet dat niemand zich druk maakt over digitale veiligheid. Integendeel, zo zal blijken.

Legitimiteit

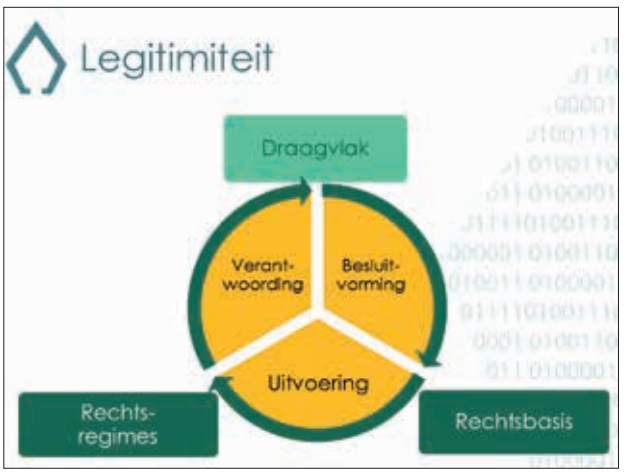
Tonke Dragt legt in *De brief voor de koning* de werking van legitimiteit prachtig vast in een gesprek tussen Tirillo de nar en één van 's konings ridders.

'Goed gesproken, ridder', zei de nar. 'Als u maar onthoudt dat u, als u tegen het kwaad vecht, zelf nog niet goed bent! Goed en kwaad zijn elkanders vijanden, maar ze kunnen dicht bij elkaar liggen.'[16]

In Tirillo's woorden ligt het legaliteitsbeginsel besloten. Ten eerste moet de ridder de goede dingen doen: het kwaad bevechten. Ten tweede dient dit op de juiste (strijd)wijze te gebeuren; zoniet dan verwordt de ridder zelf tot kwaad. De brug tussen veiligheid en recht wordt in de democratische rechtsstaat gevormd door 'legitimiteit'. Legitimiteit bestaat uit twee delen.[17] Het ('harde') legaliteitsbeginsel eist allereerst dat overheidsoptreden dat ingrijpt in de rechten van burgers (en bedrijven) een rechtsbasis heeft. Daarna moet dat overheidsoptreden de door de wetgever gestelde rechtsregels of regimes volgen. Bijvoorbeeld: de politie mag pas 'hacken' als de wetgever daarvoor een basis heeft gecreëerd, en als de politie daarbij alle procedures en randvoorwaarden naleeft.

Het 'zachtere' democratische aspect 'draagvlak' verlangt publieke of parlementaire steun voor zowel de rechtsbasis, de rechtsregimes *als* de uiteindelijke effecten van overheidsoptreden.

De interactie tussen draagvlak-rechtsbasis-rechtsregimes is voortdurend relevant:
- vóór, tijdens en ná *besluitvorming* bij creëren van een rechtsbasis en bijbehorende rechtsregels;
- tijdens de *uitvoering* en
- gedurende het *verantwoorden* van besluitvorming en uitvoering.



Figuur 2 Legitimiteit

En laat ik helder zijn: hoe ingrijpender het overheidsoptreden (huidig of beoogd), des te belangrijker draagvlak, verantwoording en toezicht worden.[18] Dat heeft de geschiedenis ons vele malen geleerd.

Veiligheid tot (w)elke prijs?

Legitimiteit als brug tussen veiligheid en recht brengt ook een ander spanningsveld in beeld. Collectieve veiligheid maakt economisch en sociaal welzijn en welvaart mogelijk. Maar veiligheid vraagt offers, en de vraag is *vanaf welke moment* en *tot welke prijs* wij als burgers veiligheid van de overheid verlangen.[19] En wat ons dit in termen van (individueel of collectief) *welzijn* oplevert.[20]

15 Zie het pleidooi van Ronald Prins (CEO Fox-IT), 'Nederland heeft een cybercommissaris nodig', in: Pim van de Dool, *NRC Handelsblad*, 12-12-2015 <www.nrc.nl/handelsblad/2015/12/12/nederland-heeft-een-cybercommissaris-nodig-1566649>.

16 Tonke Dragt, *De brief voor de koning*, Den Haag: Leopold 1987, 305.

17 P. Ducheine, 'Effectiviteit, legitimiteit en verantwoordelijkheid', in: A. Wagemaker & F. van Nijnatten, *Minuutschoten – Liber Amicorum voor Hans Bosch*, 2013, 25-28; of P.A.L. Ducheine en T.D. Gill, 'De legitimering van statelijk geweldgebruik na 9/11', in: F. Osinga, J. Soeters, W. van Rossum (reds.), *Nine eleven: tien jaar later*, Amsterdam: Boom 2011, 216-234 (ook verschenen als: NL ARMS 2011).

18 Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), *Reactie CTIVD op concept-wetsvoorstel Wiv 20XX,* 2015, p. 1, <www.ctivd.nl/actueel/nieuws/2015/09/03/reactie-ctivd-concept-wetsvoorstel>.

19 Ook zo: Dennis Broeders, *Het geheim in deinformatiesamenleving* (oratie EUR), Rotterdam 2015, 27, zie <www.wrr.nl/fileadmin/nl/Presentaties/Dennis_Broeders/Het_geheim_in_de_informatiesamenleving_Oratie_Dennis_Broeders_okt_2015.pdf>.

20 Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie-2 – Van Bewust Naar Bekwaam* (NCSS-2), Den Haag: NCTV 2013, 9.

Maar het betekent ook dat bij gebrek aan offers, veiligheid niet opgeëist kan worden. Ik betwijfel of iedereen hiervan doordrongen is. Hoewel het regelmatig voorkomt is het in mijn ogen vrij immoreel om *wél* veiligheid te vragen, daartoe zelfs ook taken toe te laten bedelen, maar daarbij *géén* middelen (budget en bevoegdheden) toe te kennen.

Laat ik dit uitleggen via het eenvoudige voorbeeld van een studentenfiets hier in Amsterdam. Stel: u studeert hier. Rechten of zo. Aan de UvA. U bent bekend met het feit dat uw mobiliteitsconcept voor anderen een essentiële schakel is in een malafide economisch businessmodel. Ondanks uw eigen voorzorgsmaatregelen – u had de fiets met een goed slot voor uw grachtenwoning vastgezet – wordt uw fiets ten derde male ontvreemd. Tot nu had u uw verlies genomen. Maar met de derde diefstal is de maat vol. U benadert de gemeente en eist – tezamen met uw straatbewoners die u via een app hebt gemobiliseerd – van uw overheid méér veiligheid.

Van een kloof tussen burger en overheid is deze keer geen sprake: uw lokale overheid doet u prompt een voorstel. Boven uw voordeur – met uitzicht op uw fietsenstalling – zal een camera worden geplaatst. Dat zal fietsendieven afschrikken en mocht dit falen, in ieder geval opsporing en vervolging vereenvoudigen. Denkend aan uw al dan niet 'wisselende contacten' die bij uw studentenleven horen, stelt u – wat mij betreft terecht – dat u 'niets te verbergen hebt, maar dat hoeft niemand te weten'.[21] Oftewel: u wijst een inperking van uw vrijheden, uw recht op privacy, af.

Uw overheid is niet voor één gat te vangen: ze biedt een alternatief. Aan het begin en einde van de gracht komt 24/7 een BOA te staan. De kosten, 100.000 euro, worden hoofdelijk over de straatbewoners omgeslagen en via gemeentelijke belastingen geïnd. Ook dit voorstel verwerpt u: een vijfde of zesde brikkie *of* een goede verzekering zijn goedkopere alternatieven. Het ongemak dat u wellicht nogmaals een lege fietsenstalling aantreft en uw 'mobiliteit' ernstige gebreken vertoont, neemt u op de koop toe.

Los van de individuele keuzeruimte is dit spanningsveld ook – of vooral – relevant voor de overheid zelf. In de democratische rechtsstaat is het immers *de wetgever* die bepaalt waar die balans tussen veiligheid – rechten – welzijn in collectief opzicht ligt. En de wetgever is nog steeds de regering en het parlement.[22] En dat zijn wij (het volk dus)! Hoezo nepparlement? Mocht u nog twijfelen aan het belang van doordachte verkiezingen, zie hier! Ik kom ook hier nog op terug.

Cyberspace

Als derde moet ik kort uitleggen wat ik onder het digitale domein versta. Ik beperk me hier tot de omschrijving die de Commissie Dessens gebruikte:

> 'Het cyberdomein [PD: digitale domein/cyberspace] is het conglomeraat van ICT-middelen en -diensten en bevat alle entiteiten die digitaal verbonden (kunnen) zijn. Het domein omvat zowel permanente verbindingen als tijdelijke of plaatselijke verbindingen evenals de gegevens (data, programmacode, informatie, etcetera) die zich in dit domein bevinden waarbij geen geografische beperkingen zijn gesteld.'[23]

In een wat schoolser overzicht gaat het om de volgende entiteiten – die zich stuk voor stuk tegelijkertijd op diverse locaties kunnen bevinden – en waarbij communicatie en informatie (transport, opslag, bewerking, etc.) centraal staan:

- personen (gebruikers, beheerders, etc.);
- digitale identiteiten (van deze personen of organisaties);
- digitale objecten, waaronder (a) protocollen,

21 Naar Loesje <www.loesje.nl/posters/nl1210_0/>.

22 Regering plus Staten-Generaal, zie art. 81 Grondwet. De wetgever is daarnaast belast met de allocatie van middelen (via begrotingswetten) waarmee (cyber security) beleid tot stand wordt gebracht.

23 C.W.M. Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 - Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 2014, in: *Kamerstukken II* 2013–14, 33 820, nr. 1 bijlage, 85.

firmware, operating systems, applicaties en (b) vooral ook data; en ten slotte
- fysieke objecten waarop deze digitale identiteiten en digitale objecten 'draaien' (servers, routers, zenders, kabels, computers, etc.).

Hoewel dit domein vooral eerbare bedoelingen kende toen de mens het tot stand bracht, denk aan *BOL.com*, *Amazon* of *Google*, kunnen de techniek en de verschillende entiteiten ook voor malafide doeleinden worden aangewend. Kijk maar naar de grote hoeveelheden spam in uw mailbox.
In zo'n geval dient zich een inbreuk op digitale veiligheid aan. En komt er een moment dat u – denkt u terug aan het verlies van uw studentenfiets – een beroep op uw overheid gaat doen… en meer veiligheid verlangt, digitale veiligheid.

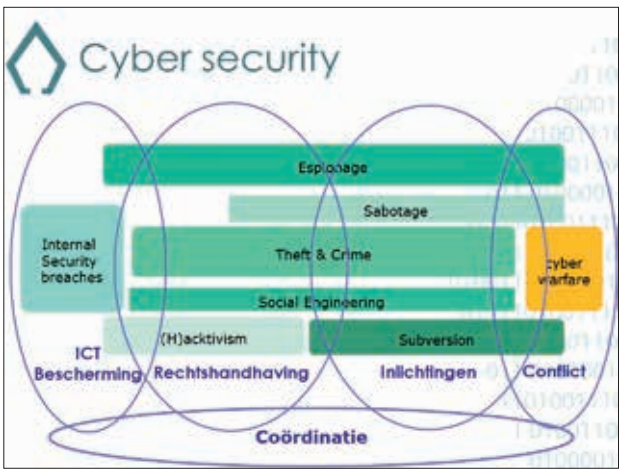
Cyber security paradigma's

Dit brengt mij op het vierde punt. Zodra burgers of bedrijven (of parlementariërs) voldoende appèl op de overheid doen of onveiligheid anderszins de beleidsagenda bereikt,[24] start een beleidscyclus. Ik zal die niet helemaal met u doorlopen. Ik beperk me tot facetten van de uitkomst.

Digitale (on)veiligheid
De regering definieert digitale veiligheid als:

> *'het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan'*.[25]

Inbreuken kunnen verschillende vormen aannemen.[26] Dit brengt mij op de eerste mythe [#1]: het is een misvatting dit gehele spectrum van inbreuken te karakteriseren als *cyber crime* of *cyber warfare*.[27] Deze generalisaties zijn bovenal verwarrend: het is beter naar de motieven achter de inbreuken te kijken. Deze variëren van vermaak,[28] treiteren,[29] activisme, chantage, tot economisch of militair gewin. Een grote verscheidenheid dus.[30] Het schema maakt dit duidelijk.
Het verbeteren van digitale veiligheid is rond

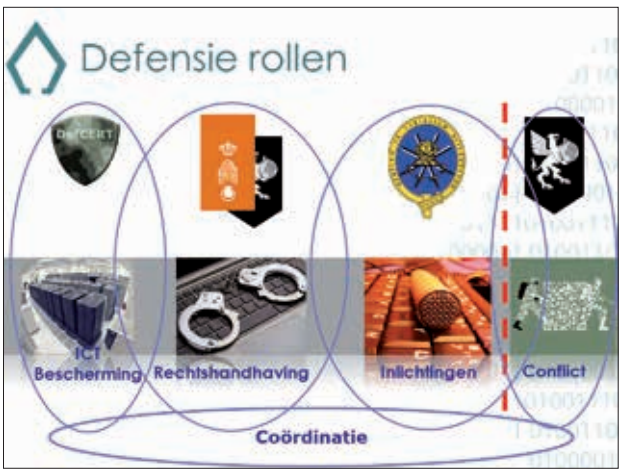


Figuur 3 Cyber security

vier paradigma's geconstrueerd: bescherming van ICT, rechtshandhaving, inlichtingen en conflict.[31] Deze paradigma's bieden een bestuurlijk, juridisch en organisatorisch kader waarbinnen de overheid en private partijen hun bijdrage leveren. De paradigma's bepalen allereerst de taak (inclusief de rechtsbasis daarvoor), het toe te passen rechtsregime, de gezagsrelaties en het toezichtmechanisme. Deze vier paradigma's maken dat verschillende departementen een rol bij *cyber security* spelen.

En om deze verschillende inspanningen onderling af te stemmen, is een vijfde paradigma, horizontale coördinatie, nodig.

24 Zie Maarten Rothman & Theo Brinkel, 'Of Snoops and Pirates: Competing Discourses of Cyber Security', in: P. Ducheine, F. Osinga and J. Soeters (eds.), *Cyber Warfare: Critical Perspectives* (NL ARMS 2012), The Hague: TMC Asser Press 2012, 49-72.
25 Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie-2 – Van Bewust Naar Bekwaam* (NCSS-2) Den Haag: NCTV 2013.
26 Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld Nederland 2015*, Den Haag: NCSC 2015.
27 Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet*, Tilburg: De Wereld 2013.
28 'Lulz': (voor de) lol.
29 'Trolling': het treiteren, plagen op internet, zie <www.360magazine.nl/politiek/4213/wat-beweegt-de-trol" \l ":VJ3Dhl4ABA">.
30 Waarbij het gros van de inbreuken uit spionage en strafbare feiten bestaat: Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld Nederland 2015*, Den Haag: NCSC 2015, 10.
31 P.A.L. Ducheine, 'The Notion of Cyber Operations', in: N. Tsagourias & R. Buchan, *Research Handbook on International Law and Cyber Space*, Cheltenham: Edward Elgar Publishing 2015, 211-232.



Figuur 4 Defensierollen

Over de rol van de krijgsmacht in dit geheel bestaan zeker twee mythen: ten eerste (mythe #2) dat de 'bescherming van het digitale domein', het totale Nederlandse dus – bij gebrek aan anderen – een verantwoordelijkheid van de krijgsmacht zou moeten zijn. En vervolgens dat (mythe #3) iedere rol van de krijgsmacht leidt tot 'militarisering', wat daarmee ook bedoeld mag worden.[32] Ik zal beide mythen hierna weerleggen.

Defensierollen

Uiteraard speelt defensie een rol in het digitale domein. Alleen al vanwege onze territoriale veiligheid. Dit rechtvaardigt allerminst de vierde mythe [#4] dat de rol van defensie beperkt is tot 'digitale oorlogvoering' of *cyber warfare*. Defensie zal namelijk om te beginnen, net als andere organisaties, haar eigen deel van het digitale domein beschermen. Daarnaast is defensie via de Koninklijke Marechaussee betrokken bij rechtshandhaving, en via de MIVD bij inlichtingen. En inderdaad – maar dus niet alleen – bij oorlog en conflict.

Daarmee is ook de opvatting, de vijfde mythe [#5] weerlegd dat iedereen bij defensie op dezelfde manier in het digitale domein staat. De verschillende rollen kennen een verschillende taak, verschillende mores en taal, verschillende bevoegdheden, en ook verschillende verantwoordings- en toezichtmechanismen.

De meeste defensierollen associeer ik met de functies van een bastion: een beschermde versterkte positie, waarbinnen het veilig is, en van waaruit een goed overzicht op omgeving bestaat. Slechts een deel van de defensie-inspanningen in het digitale domein associeer ik met (de punt van) het zwaard of de speer. Voor de scherpe ogen: *ascalon*.

Ook defensie hanteert een vijfde rol om het geheel te coördineren. Het totaal van alle defensie-inspanning is immers zo sterk als de zwakste schakel. Wat dat betreft zijn vestingbouwers een voortdurende bron van inspiratie.

Ik zal de eerste vier rollen één voor één belichten. Coördinatie laat ik voor wat het is.

- *Bescherming*

Als eerste bescherming van ICT, van het digitale domein. Net als elders is de bescherming van defensie-ICT zeer divers van aard en kent zij verschillende invalshoeken. Deze variëren van (eisen voor) fysieke beveiliging, (regelgeving over) informatiebeveiliging, bewustwording, opleidingen van personeel alsmede de mentale of feitelijke weerbaarheid ('resilience').

Hoewel ik hiervoor slechts het symbool van het Defensie *Computer Emergency Response Team* (DefCERT) heb gebruikt, zijn meer organisatiedelen betrokken. Ik denk aan het Joint Informatie Voorzieningscommando, de Afdeling Operations van de Defensie Materieel Organisatie (DMO-Operations), de Beveiligingsautoriteit (BA), maar ook het Defensie Cyber Expertise Centrum. Maar ook alle individuele militairen en commandanten. Zij allen dragen hun steentje bij.

Het borgen van veiligheid kent hier een relatief

32 Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet*, Tilburg: De Wereld 2013; en WRR, *De publieke kern van het internet*, Amsterdam: AUP 2015, 21, waarbij de WRR kennelijk doelt op het enkele feit dat krijgsmacht het digitaal domein als een domein typeren waarin zij – naast anderen – actief zijn. Zie echter pagina 26 voor een bredere opvatting in termen van een trend waarin een militair-industrieel complex actief is.

beperkt juridische kader, waarbij het beschermen van grondrechten een prominente rol inneemt. De uiteindelijke beschermingsrol moet – zoals betoogd – getoetst worden aan de eisen van veiligheid en legitimiteit.

• *Rechtshandhaving*

De tweede rol is rechtshandhaving. Hoewel ik het causale verband uiteraard niet aan kan tonen, heeft de politieorganisatie van Defensie, de Koninklijke Marechaussee, na een prikkelend Editoriaal in de *Militaire Spectator*[33] sinds 2013 het digitale domein omarmd.[34]

De *Militaire Spectator* wees allereerst op het feit dat de marechaussee vol geraakt zou worden door het wetsvoorstel *Computercriminaliteit III*, dat uiteindelijk vorige maand aan de Tweede Kamer is aangeboden.[35] Ten tweede voorspelde de *Militaire Spectator* dat zodra het Defensie Cyber Commando actief zou worden, de beoordeling van de rechtmatigheid van dit digitale geweldgebruik bij de marechaussee zou komen te liggen. En *last but not least*, dat waar technologie tot aanpassing van sociaal gedrag leidt, ook malafide uitwassen die binnen de taakstelling van de marechaussee liggen, een zaak van de Kmar worden. Een digitaal reveille dus.

Daarbij is het interessant dat een Brits IT tijdschrift afgelopen oktober meldde dat digitale criminaliteit de fysieke variant(en) overtreft.[36] Los van hoe dit gemeten is, en aangenomen dat het juist is, roept het de vraag op wanneer politieorganisaties – niet alleen de KMar dus – dit gegeven in werving, opleiding en organisatie zullen verdisconteren.

En dan hebben we het nog niet gehad over de vraag wat we moeten verstaan onder de handhaving van de openbare orde in het digitale domein?[37] Gaat de marechaussee óók digitaal fulminerende (militaire) Twitteraars in toom houden? Of zou dat onder militaire justitiabelen niet voorkomen?

Opsporingsinstanties zoals de KMar zijn afhankelijk van de wetgever. De wetgever bepaalt immers welk digitaal gedrag wel of niet strafbaar wordt gesteld.[38] Het bezien en zo nodig toekennen van adequate opsporingsbevoegdheden dient hiermee gelijke tred te houden. Als *fysieke* criminele handelingen door gebruik van digitale technieken achterwege blijven, *of* als opsporing effectiever en efficiënter langs digitale weg kan verlopen, moeten opsporingsmogelijkheden herzien worden. Ook hier is de wetgever aan zet.

Voor diegenen die in de zesde mythe [#6] geloven, dat legitimiteit en vooral draagvlak van weinig waarde zijn in het digitale domein, wijs ik graag op het oorspronkelijk voorgestane decryptiebevel, dat na de internetconsultatie,[39] niet meer in het huidige wetsvoorstel CCIII terugkeerde! Zo ziet u maar dat een publieksconsultatie en campagne van belangengroepen wel degelijk effect kan hebben.

• *Inlichtingen*

Ik kom op de derde defensierol. Digitale inbreuken of bedreigingen kunnen ook de verantwoordelijkheid van inlichtingen- en veiligheidsdiensten raken. Dit is het domein van de AIVD en de MIVD. Zij raken betrokken bij – kortgezegd – een bedreiging van de nationale veiligheid. Die taakstelling is gelimiteerd, anders dan vaak wordt gedacht (mythe #7). Onze inlichtingendiensten voeren bijvoorbeeld geen oorlog.

Zoals dat in een rechtsstaat hoort, en zeker bij I&V diensten, zijn de taakstelling, de bevoegdheden, de wijze van uitoefening van die bevoegdheden, alsmede het toezicht daarop, door de wetgever bepaald. Ook in deze rol is de wetgever aan zet.

33 De redactionele column.
34 Editoriaal 'Cyber & marechaussee', in: *Militaire Spectator*, vol 182, 2013-6, 278-279.
35 *Kamerstukken II*, 2015–16, 34 372, nrs. 2-3.
36 *SC Magazine*, 'Cyber-crime overtakes physical crime in the UK', 15-10-2015, <www.scmagazineuk.com/cyber-crime-overtakes-physical-crime-in-the-uk/article/445014/>.
37 Kim Bos & Martin Kuiper, 'U twittert wel heel veel, zei de politie', in: *NRC Next*, 20-1-2016, <www.nrc.nl/next/2016/01/20/u-twittert-wel-heel-veel-zei-de-politie-1578392>.
38 Denk bijvoorbeeld aan een *Distributed Denial of Service* of 'DDOS-aanval' op een bancaire website. Zie artikel 161sexies Sr.
39 Zie de internetconsultatie: <www.internetconsultatie.nl/computercriminaliteit>.

Dat de digitale werkelijkheid enerzijds en de wet (de WIV) uit 2002 (maar qua ontwerp uit 1993) anderzijds, uit de pas lopen, is inmiddels meermalen vastgesteld. Uitbreiding en aanpassing van bevoegdheden is dan ook voorzien. Maar meer bevoegdheden vragen ook op een bezinning op *verantwoorden*, en dus op de toezichtstructuur en de bevoegdheden die de toezichthouders krijgen.

De wetgever zal ook hier kleur moeten bekennen. Draagvlak zal daarbij een belangrijk item zijn. Uit de internetconsultatie bleken ernstige bedenkingen tegen enkele voorziene nieuwe bevoegdheden.[40] Ook werd het toezicht onvoldoende geacht.[41] Onder de 557 insprekers bevonden zich niet de minsten: *Greenpeace International*, *Bits of Freedom*, Nederland ICT, en Google. Maar ook individuen zoals mr. W. van Amerongen uit Den Haag, en de markante 'Anoniem aub – De Nederlandse overheid is al een Stasi'.

Ook hier speelt de balans tussen veiligheid, rechten van burgers én bedrijven, alsmede welvaart en welzijn een belangrijke rol. Het feit dat rechten en vrijheden daadwerkelijk in (relatieve) veiligheid te genieten zijn, draagt bijvoorbeeld bij aan een hoger welzijn en welvaren. Denkt u maar terug aan uw fiets.

Deze balans is overigens geen vaststaand gegeven. Zij volgt in zekere zin dagkoersen. Maatschappelijke en parlementaire opvattingen fluctueren. Na 9/11 (2001) en de aanslagen in Madrid en Londen nam het belang van veiligheid ten koste van mensenrechten toe.[42] Edward Snowdens onthullingen leidden tot hernieuwde aandacht voor grondrechten en vrijheden. De recente opkomst van ISIS en de aanslagen in Parijs veroorzaakten juist weer een tegengestelde beweging waarbij veiligheid weer aan belang wint. Ook hier geldt de vraag: hoeveel veiligheid, tot (w)elke prijs? [43]

Cyber warfare

Ten vierde wil ik met u over het slagveld van de toekomst spreken, het digitale domein en het informatiedomein. Voor wie denkt dat het allemaal zo'n vaart niet zal lopen, wijs ik graag op het feit dat Chinese en Russische strategen het gebruik van dit domein al decennia doordenken.[44] Het Chinese *Unrestricted Warfare* dat uiteen zet hoe China de VS kan verslaan, verscheen al in 1999. En het blijft niet bij denken: de Verenigde Staten,[45] de Russische Federatie[46] maar ook ISIS/ISIL maken duidelijk hoe je oorlogvoering in het informatie- en digitale domein in de praktijk brengt.[47]

Onze westerse militaire cultuur heeft een voorliefde voor kinetische actie: oftewel voor zwaarden (vroeger dan), (nu) geweren en granaten.[48] Daar staat een andere benadering

40 Zie <www.internetconsultatie.nl/wiv>.

41 Zie voor de aparte reactie van de toezichthouder op het voorstel: CTIVD, *Reactie CTIVD op concept-wetsvoorstel Wiv 20XX,* 2015, <www.ctivd.nl/actueel/nieuws/2015/09/03/reactie-ctivd-concept-wetsvoorstel>.

42 Zie bijvoorbeeld de behandeling van gevangen, zoals beschreven in: Philippe Sands, *Torture Team. Rumsfelds Memo and the Betrayal of American Values*, New York: Palgrave MacMillan, 2008.

43 Zo ook Bram van Bruggen & Matthijs van de Burgwal, '"1984" was een dystopie, geen handleiding', in: *NRC Handelsblad* 14-12-2015.

44 Zie Qiao Liang, Wang Xiangsui, *Unrestricted warfare: China's masterplan to destroy America*, Panama: Pan American 2002. Mark Galeotti, 'The 'Gerasimov Doctrine' and Russian Non-Linear War', in: *Moscow's Shadows* (blog), 6-7-2014,zie <inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>; Charles K. Bartles, Getting Gerasimov Right, in: *Military Review* (Jan-Feb 2016), 30-38, zie <usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf>.

45 Zie o.a. Shane Harris, *@War: The Rise of the Military-Internet Complex*, Boston-New York, Eamon Dolan/Houghton Mifflin Harcourt 2014.

46 Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: CCDCOE 2015; Ulrik Franke, *War by non-military means - Understanding Russian information warfare*, Stockholm: Swedish Defence Research Agency 2015; Thomas Elkjer Nissen, *#TheWeaponizationOfSocialMedia - @Characteristics_of_Contemporary_Conflicts*, Copenhage: Royal Danish Defence College 2015.

47 Zie het gebruik van social media door ISIS: J.M. Berger & Jonathan Morgan, *The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter*, Washington DC: The Brookings Institution 2015; Christina Schori Liang, *Cyber Jihad: Understanding and Countering Islamic State Propaganda* GCSP Policy Paper 2015/2.

48 Martijn Kitzen, 'Western military culture and counter-insurgency, an ambiguous reality', in: *Scientia Militaria: South African Journal of Military Studies* 40-1, 2012, 123–134. Kitzen baseert zich op o.a. J. Lynn *Battle: a history of combat and culture from ancient Greece to modern America*, Boulder: Westview Press 2003, xix en V.D. Hanson, *The western way of war - infantry battle in Classical Greece*, London: Hodder & Stoughton 1989.

49 David Kilcullen, *The Accidental Guerrilla*, Oxford: OUP 2009, p. 300: 'In military terms, for Al Qaida the 'main effort' is information; for us, information is a "supporting effect".'

50 Jennifer Valentino-DeVries, Lam Thuy Vo & Danny Yadron, 'Cataloging the World's Cyberforces', in: *The Wall Street Journal*, 28-12-2015, via: <http://graphics.wsj.com/world-catalogue-cyberwar-tools/>.

tegenover. Voor strijdgroepen zoals Al Qaeda en ISIS is de informatie-operatie het zwaartepunt, de fysieke actie is daaraan ondergeschikt.[49]

Een deel van het westen heeft deze graal ook ontdekt. Op dit moment hebben 29 staten uitgesproken dat zij operationele cybercapaciteit voor militaire operaties ontwikkelen of bezitten.[50]

Over de portee van die operationele capaciteiten bestaan nogal wat misverstanden. Het is een mythe [#8] dat cybercapaciteiten alleen *high tech* ICT oplossing bevatten.
De actualisering van de Defensie Cyber Strategie van vorig jaar februari maakt – zij het voorzichtig – duidelijk dat cybercapaciteiten – wapens in de volksmond – zowel 'hard' als 'soft' zijn.

Hard cyber maakt gebruik van een 'gaatje' in de bescherming of van een kwetsbaarheid in digitale objecten, waardoor een stukje software (malware) zijn werk kan doen [Stuxnet].[51] Wapen en doelwit bevinden zich beiden in cyberspace, en de uitkomst is het gevolg van 'dwang'. *Soft cyber* daarentegen gebruikt cyberspace als medium om informatie te verspreiden. Hierbij is sprake van indirecte beïnvloeding. We zien dit duidelijk terug bij ISIS.

Een andere mythe [#9] is de idee dat cybercapaciteiten 'vaak slechts *eenmalig* inzetbaar zijn en veelal een *beperkte* levensduur hebben.' [52] Van het fameuze Stuxnet is bekend dat het meermaals en gedurende langere tijd werd ingezet in Iraanse nucleaire faciliteiten.[53] Ook DDoS-aanvallen kunnen meermalen gebruikt worden.[54] Hoe banaal sommigen deze methode ook vinden!

Ten slotte werd de mythe [#10] verlaten dat cybercapaciteiten altijd strategische assets zijn die slechts voor strategische doeleinden worden ingezet. Kort en goed: cybercapaciteiten die als middel of methode van oorlogvoering kunnen worden ingezet, bestrijken een spectrum van *high* tot *low tech*, van strategisch tot tactisch, en van *hard* tot *soft* power.

Figuur 5 Oorlogsrecht

Inzet van deze capaciteit vraagt uiteraard wel om – ten eerste – de eigen 'dekking hoog te houden', en – ten tweede – om inlichtingen. Immers, zonder informatie geen operatie. Of het nu in de fysieke of in de digitale wereld is, operationele capaciteit is bedoeld voor militaire operaties, waaronder gewapend conflict.

Oorlog

Dat brengt mij uiteindelijk op oorlog en de veel gehoorde 'mening' (mythe #11) dat moderne techniek zoals *cyber warfare* (digitale oorlogvoering) niet in het oude oorlogsrecht past.

51 Zie bijvoorbeeld Stuxnet: David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, New York: Crown 2012, 188 e.v.; en Ralph Langner, *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, 2013, <www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.

52 DCS 2012, 7 (Kamerstukken versie).

53 Waarbij het moment van locale ontdekking en publieke bekendheid kunnen verschillen. Zie: Ralph Langner, *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve*, 2013, via < www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>; David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown 2012.

54 Waarbij een slachtoffer zich uiteraard kan beschermen. Zie o.a. Carol Matlack, 'Cyberwar in Ukraine Falls Far Short of Russia's Full Powers,' in: *Bloomberg Business Week*, <businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers>; *Reuters*, 'Ukrainian Authorities Suffer New Cyber Attacks,' <reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308> (benaderd 11-3-2014). Ook Jason Andress & Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed., New York: Syngress, 2014, 139.

Laat ik die opvatting in verschillende stappen weerleggen. Ten eerste, inmiddels staat vast dat Cicero ernaast zat toen hij de stelling poneerde dat *het recht tijdens oorlog zwijgt*.[55] Het tegendeel is waar. Mijn eigen dienstvak voert niet voor niets het motto 'ook tijdens oorlog spreekt het recht'. Uit een oogpunt van *beschaving* en *ridderlijkheid* lijkt me dit een verstandig standpunt.

Ik verwijs verder de liefhebbers graag naar mijn proefschrift, waarin ik ditzelfde punt maakte. Ik waarschuw u wel: het is een lijvig werk, maar u kunt zich beperken tot pagina 539, in de buurt van voetnoot 1179.[56] Bovendien denk ik aan de opmerking van Tirillo de nar, die ik bij het onderwerp 'legitimiteit' introduceerde: 'de grens tussen goed en kwaad is dun…'. Overheidshandelen vraagt een basis, en volgt vastgestelde rechtsregels. Dat is wat ons onderscheidt van barbarij.

Het recht, het oorlogsrecht om precies te zijn, is nu precies *daarom* gemaakt: het erkent oorlogvoering als fenomeen, maar begrenst óók het daarbij te hanteren geweld. Nederland heeft op dit vlak een lange en indrukwekkende geschiedenis, getuige de Haagse Vredesconferenties (1899 en 1907). Maar denk vooral ook nu aan de vele internationale tribunalen die vanuit Den Haag hun taak in relatie tot oorlogsmisdrijven vervullen. Adeldom verplicht, en Nederland heeft op dit punt een reputatie hoog te houden.

Wat critici vaak vergeten, is het feit dat luchtwapens – intussen al decennia gemeengoed[57] – nooit tot een apart oorlogsrechtelijk regime hebben geleid. Dat kon omdat het internationale recht adaptief is, en het oorlogsrecht steeds in staat geweest nieuwe technologie te omarmen. Zo ook in het digitale domein. Nationale en internationale experts zijn het hier over eens.[58]

Dit proces van adaptatie gaat evenwel niet zonder slag of stoot. Nieuwe techniek, nieuwe methoden, middelen, doelwitten en effecten, vragen – zoals ooit ook bij de invoering van het luchtwapen – om een herbezinning op de interpretatie van de verschillende onderdelen van het oorlogsrecht. Ik weet dat een aantal collega's hier aan werkt. Laat ik twee aspecten kort noemen.

Op de eerste plaats het begrip 'oorlog'. Ik begrijp dat dit een beladen term kan zijn. In meerdere opzichten. Ik heb ook begrip voor de verschillende belangen die spelen en effecten die het heeft. Ik heb mij eerder hard gemaakt voor een heldere stellingname.[59] Een van mijn oudere en wijze civiele collega's wees mij toen op het feit dat naast de inhoud, *timing* ook belangrijk was. En ik geef toe: *I couldn't agree more*.[60]

Timing is inderdaad belangrijk. Bijvoorbeeld omdat de regering bijtijds een positie moet bepalen, in de wetenschap dat de feitelijke situatie uiteindelijk doorslaggevend zal zijn.[61] De moderne ridders van de democratische rechtsstaat, officieren, verdienen het te weten binnen welke regels zij hun taak moeten uitvoeren.

Een tweede punt speelt zodra vastgesteld is dat er sprake is van een gewapend conflict. Zoals ik zei, gaat de toepassing van oorlogsrecht op cyberoperaties niet zonder slag of stoot.

55 Cicero: 'Silent enim leges inter arma'.

56 P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding. Een onderzoek naar juridische aspecten van de rol van strijdkrachten bij de bestrijding van terrorisme*, Nijmegen: Wolf Legal Publishers 2008.

57 In de ogen van een sommigen is *Airpower* ondertussen de belangrijkste vorm van militaire macht,, waarbij de concurrentie met *Seapower* overigens sterk is.

58 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV): *Digitale oorlogvoering*, Den Haag: AIV no. 77, 2011; CAVV no. 22, zie <www.aiv-advice.nl>. Zo ook: M.N. Schmitt (ed.), *Tallinn Manual on the International Law applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge: Cambridge University Press, 2013.

59 Zie Stelling 6 'Politiek correct taalgebruik in relatie tot militaire inzet leidt tot "collateral damage" binnen de eigen gelederen', 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. Zie ook Paul Ducheine, 'ISAF en oorlogsrecht: 'Door het juiste te doen, vreest gij niemand'', in: *Militair Rechtelijk Tijdschrift*, vol 102, 2009-6, 277-300.

60 Zie de cartoon van Tom Jansen 'Wij zijn in oorlog! En ik wens u allen nog een prettig weekend!', (15-11-2016) <www.tomjanssen.net/prenten/0000002_november_15/oorlog_191115.jpg>.

61 Ducheine, P.A.L. & Pouw, E.H., *ISAF Operaties in Afghanistan: oorlogsrecht, doelbestrijding in counterinsurgency, ROE, mensenrechten & ius ad bellum*, Nijmegen: Wolf Legal Publishers 2010, p. 46.

Weliswaar hebben verschillende experts hun visie bekendgemaakt, maar het is en blijft de visie van die experts.[62] Ook de deskundigen die bij de totstandkoming van de Tallinn Manual, hét hulpmiddel bij de interpretatie van oorlogsrecht in cyberspace, erkennen dat het uiteindelijk staten zijn – en niet zij – die internationaal recht maken.[63]

Nederland vormt op dit punt geen uitzondering. Sterker nog, niet alleen vanuit het oogpunt van legitimiteit maar vooral ook als wereldhoofdstad van het internationale recht: Nederland moet vooroplopen in het interpreteren van het oorlogsrecht in cyberspace.

Vanuit beide leeropdrachten lever ik graag mijn bijdrage aan dit werk. Ik zal u de details hier besparen, maar laat ik het zo samenvatten. Over het daadwerkelijk 'aanvallen' van digitale 'objecten', de daaruit voorvloeiende consequenties, inclusief '*collateral damage*' moet nog behoorlijk wat denkwerk worden verricht.

. . . over ridders

Ik beloofde als laatste terug te komen op ridders… Het zal u waarschijnlijk niet verbazen dat ik *denkwerk* onder de moderne ridders, officieren, een belangrijke functie toedicht. Ik doel dan niet alleen op de strategische denkers, of de collega's die het idee van de *thinking soldier* invullen. Ik doel dan op het fenomeen dat militaire inzet in steeds complexere omgevingen plaatsvindt. Daarvoor is *understanding* (inzien en doorzien) van deze complexe omgeving essentieel. Ik ben er van overtuigd dat een goede wetenschappelijke officiersopleiding de kans op succes bevordert.

Uiteraard denk ik ook aan de militair juristen, die commandanten bijstaan in het toepassen van recht rondom die militaire inzet. Op hen rust de plicht die commandanten in hun operationele werkelijkheid te kunnen bijbenen zodat ze als volwaardig raadgever geaccepteerd worden.

Ten slotte denk ik aan de cyberspecialisten, welke achtergrond zij ook hebben, welke rol zij ook vervullen. Ook zij brengen met hun specifieke deskundigheid de krijgsmacht op een hoger vlak. Zodat deze, waar dan ook, daadwerkelijk veiligheid kan helpen verbeteren. Zo nodig met geweld, ook al is dat digitaal.

Tot slot

Ik wil besluiten door terug te komen op de titel van mijn oratie. Voor wie de achtergrond van 'de brief aan de koning niet kent', volgt een onverantwoord korte samenvatting.

Tijdens zijn wake in de nacht vóór zijn ridderslag, gaat Tiuri in op een smeekbede van een onbekende. Hij verlaat de wake, loopt daarmee zijn ridderslag mis, en begint aan een levensgevaarlijke tocht door een brief naar koning Unauwen te brengen. Kort nadat Tiuri deze brief van ridder Edwinem bij de koning heeft bezorgd, spreekt hij Tirillo de nar. Ik citeer dat moment:

> Hij keek naar Tirillo en plotseling zag hij iets dat hem trof. Een ring aan diens linkerhand […].
> Hij boog zich naar voren en zei verbaasd: 'U draagt ook zo'n ring… Zo'n ring als […] Ridder Edwinem droeg!'
> Tirillo glimlachte. 'Ja zeker' zei hij. 'Koning Unauwen zei, toen hij mij hem gaf: "Je hoeft geen zwaard en schild te dragen om een ridder te zijn".'
> 'Ja', zei Tiuri, 'ja, natuurlijk.' [64]

Ik heb gezegd! ■

62 Zie hiervoor AIV/CAVV en Tallinn Manual.
63 O.a. M.N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' in: *Stanford Law and Policy Review*, vol 25, 2014, 269.
64 Tonke Dragt, *De brief voor de koning*, Den Haag: Leopold 1987, 300.