UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

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

Mythen over digitale oorlogsvoering en recht

Ducheine, P.

Publication date
2016
Document Version
Final published version

Link to publication

Citation for published version (APA):
Ducheine, P. (2016). *'Je hoeft geen zwaard en schild te dragen om ridder te zijn': Mythen over digitale oorlogsvoering en recht*. (Oratiereeks; No. 559). Universiteit van Amsterdam. http://www.oratiereeks.nl/upload/pdf/PDF-6825weboratie_Ducheine_-_DEF.pdf

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:06 Dec 2021

‘Je hoeft geen zwaard en schild te dragen om ridder te zijn’

‘Je hoeft geen zwaard en schild te dragen om ridder te zijn’

Mythen over digitale oorlogsvoering en recht

Rede

uitgesproken 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 woensdag 27 januari 2016

door

Paul Ducheine
brigade-generaal van de Militair Juridische Dienst

Dit is oratie 559, verschenen in de oratiereeks van de Universiteit van Amsterdam.

Opmaak: JAPES, Amsterdam
Foto auteur: Dirk Gillissen

© Paul Ducheine, 2016

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van kopieën uit deze uitgave is toegestaan op grond van artikel 16B Auteurswet 1912 j° het Besluit van 20 juni 1974, Stb. 351, zoals gewijzigd bij het Besluit van 23 augustus 1985, Stb. 471 en artikel 17 Auteurswet 1912, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3051, 2130 KB Hoofddorp). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (artikel 16 Auteurswet 1912) dient men zich tot de uitgever te wenden.

Mevrouw de Rector Magnificus,
Meneer de Decaan (van de Rechtenfaculteit),
Leden van het Curatorium van de leerstoel Military Law of Cyber Security and Cyber Operations,
Geachte bestuur van de Stichting Wetenschappelijk Onderwijs en Onderzoek van de Nederlandse Defensie Academie,
Commandant Nederlandse Defensie Academie,
Meneer de decaan (van de Faculteit Militaire Wetenschappen),
Excellenties, …
Geachte aanwezigen.

1 Inleiding

1.1 Aanleiding

Toen ik 33 jaar geleden hoorde dat ik aangenomen was op de Koninklijke Militaire Academie ging mijn jongensdroom in vervulling.[1] 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,[2] had ik mijn zinnen op 'de parel van het zuiden'[3] en de Koninklijke Militaire Academie (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 enthousiaste en 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 ☺. 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!*

1.2 Twee werelden

Zoals admiraal Sir George Parr geen geheim maakt van zijn militaire achtergrond, heb ook ik weinig te verbergen.[4] 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'*.[5] Velen van u kennen deze strofe uit het lijflied van het 1e Regiment Genietroepen, het op een na oudste regiment van de Koninklijke Landmacht. Kolonel Nicolaas François de Torcy, baron van Breda, richtte het op 15 mei 1748 op. Binnenkort dus 268 jaar jong. 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 – een soort jongens/meisjes E-achttal – 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, óók militair optreden, 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.

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 *Een brief aan de koning* van Tonke Dragt. De ondertitel – **mythen over digitale oorlogvoering en recht** – is een onderstroom in mijn verhaal. Ik zal twaalf mythen met u delen.

2 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*.[6]

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.[7] Ik zie de officier van nu, als de ridder van toen. Inclusief het culturele aspect, *chivalry* (ridderlijkheid). Het mag duidelijk zijn dat het moderne ridderschap in vele gedaanten komt: bereden, te voet, in de lucht, of op het water.

3 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.

3.1 Veiligheid

3.1.1 Veiligheid als publiek goed

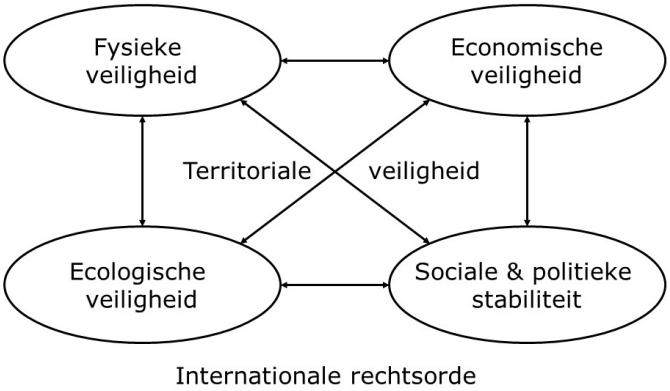
De leerstoel richt zich op het publieke veiligheidsdomein. Dat wil zeggen: het publieke goed 'veiligheid'. De Wetenschappelijk Raad voor het Regeringsbeleid typeert 'veiligheid bieden' als een van de klassieke en 'harde' taken van de overheid.[8] Deze functie wordt in sociale contracttheorieën verklaard. Burgers staan een deel van hun individuele rechten en aanspraken af aan de staat. Denkt u aan privacy, maar ook aan geld (bijvoorbeeld via 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.[9] Alternatieve vormen van geschillenbeslechting zijn beschikbaar; eigenrichting via *Geen Stijl* en andere platforms floreert;[10] particuliere beveiligingsbedrijven (en *contractors*) hebben een opmars gemaakt, inclusief de lobby om daarbij geweld te mogen gebruiken.[11] En omdat veel digitale infrastructuur en diensten in private handen zijn, moet de overheid digitale veiligheid onder meer via 'publiek-private' samenwerking realiseren.[12] De rol en positie van de overheid inzake veiligheid is dus niet 'in beton gegoten' maar evolueert naar gelang noodzaak, mogelijkheden en opportuniteit.

3.1.2 Het hedendaagse veiligheidsbegrip

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.[13] 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 twee veiligheidsstrategieën verwoord. De essentie ziet u in het schema (zie Figuur 1). Deze vitale belangen werken op elkaar in (interdependent).



Figuur 1 Nederland's vitale belangen

Uit de Strategie Nationale Veiligheid uit 2007 volgden vijf vitale belangen: territoriale, fysieke, economische, ecologische veiligheid en politieke en sociale stabiliteit.[14] De strategie heeft overigens een binnenlands perspectief, en besteedt slechts in beperkte mate aandacht aan externe factoren. Voor defensie heeft die externe focus altijd bestaan.[15] Hoe dat ook zij, uit de grondwettelijke opdracht aan de regering in artikel 90, blijkt dat een effectieve 'internationale rechtsorde' voor Nederland vitaal is. Dit blijkt feitelijk ook uit rapportages van de WRR en HCSS waarin de afhankelijkheid van Nederland van deze internationale (rechts)orde andermaal werd aangetoond.[16]

De uit 2013 daterende Internationale Veiligheidsstrategie van Buitenlandse Zaken hanteert drie vitale belangen, namelijk territoriale veiligheid en economische veiligheid en – *at last* – de internationale rechtsorde.[17]

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.

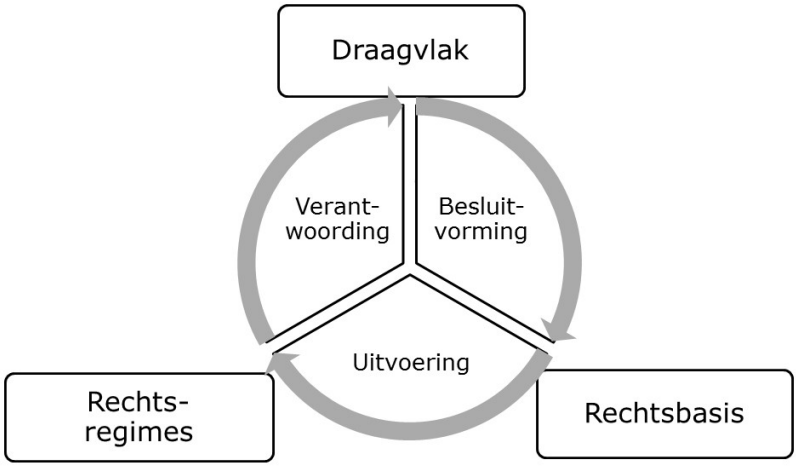
En daarmee doet zich iets interessant voor. Van oudsher kennen de vitale belangen organisaties die dit belang als eerste behartigen, denkt u maar aan de waterschappen voor onze ecologische veiligheid. Maar voor digitale veiligheid is deze belangenbehartiging verkaveld, tot grote zorg van menig digitaal deskundige.[18] Gelukkig betekent dit niet dat niemand zich druk maakt over digitale veiligheid. Integendeel, zo zal blijken.

3.2 Legitimiteit

De brug tussen veiligheid en recht wordt in de democratische rechtsstaat gevormd door 'legitimiteit'. Legitimiteit bestaat uit twee delen: een 'harde' juridische component en een 'zachtere' sociale.[19] Het 'harde' rechtstatelijke 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. Tonke Dragt legt in *De brief voor de koning* de werking 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.'[20]

In Tirillo's woorden ligt het legaliteitsbeginsel besloten. Ten eerste moet de krijgsmacht de goede dingen doen: het kwaad bevechten. Ten tweede dient dit op de juiste (strijd)wijze te gebeuren; zo niet dan verwordt de krijgsmacht zelf tot kwaad. Tirillo noemt draagvlak niet met zoveel woorden, maar het belang ervan is er vandaag de dag niet minder om. Ik kom daar zo op terug. Samenvattend: de fundamentele regel van legitimiteit van overheidsoptreden vereist draagvlak, een rechtsgrondslag en respect voor rechtsregels.



Figuur 2 Legitimiteit

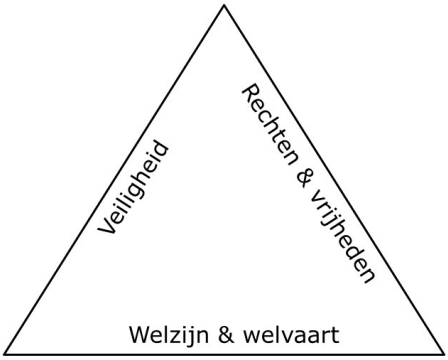
De interactie tussen draagvlak-rechtsbasis-rechtsregimes is voortdurend relevant (zie Figuur 2):
- vóór, tijdens en ná **besluitvorming** bij creëren van een rechtsbasis en bijbehorende rechtsregels,
- tijdens de **uitvoering** en
- gedurende het **verantwoorden** van besluitvorming en uitvoering.

En laat ik helder zijn: hoe ingrijpender het overheidsoptreden (huidig of beoogd), des te belangrijker draagvlak, verantwoording en toezicht worden.[21] Dat heeft de geschiedenis ons vele malen geleerd.

3.3 Veiligheid tot (w)elke prijs?

Legitimiteit als brug tussen veiligheid en recht brengt ook een ander spanningsveld in beeld (zie Figuur 3). Collectieve veiligheid maakt economisch en sociaal welzijn en welvaart mogelijk, zoals Hobbes al duidelijk maakte.

> '[Without security] there is no place for industry... no arts, no letters, no society: and which is worst for all, continued fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.'[22]



Figuur 3 Balans veiligheid – rechten & vrijheden – welzijn & welvaart

Maar veiligheid vraagt offers, en de vraag is *vanaf welke moment* en *tot welke prijs* wij als burgers veiligheid van de overheid verlangen.[23] En wat ons dit in termen van (individueel of collectief) *welzijn* oplevert.[24] 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 of onvoldoende middelen (budget, personeel 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 studentikoze 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 – 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'.[25] 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 Buitengewoon Opsporingsambtenaar 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[26] 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.

4 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 bij de evaluatie van de Wet- op de inlichtingen en veiligheidsdiensten 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.'[27]

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

5 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,[28] start een beleidscyclus. Ik zal die niet helemaal met u doorlopen. Ik beperk me tot facetten van de uitkomst.

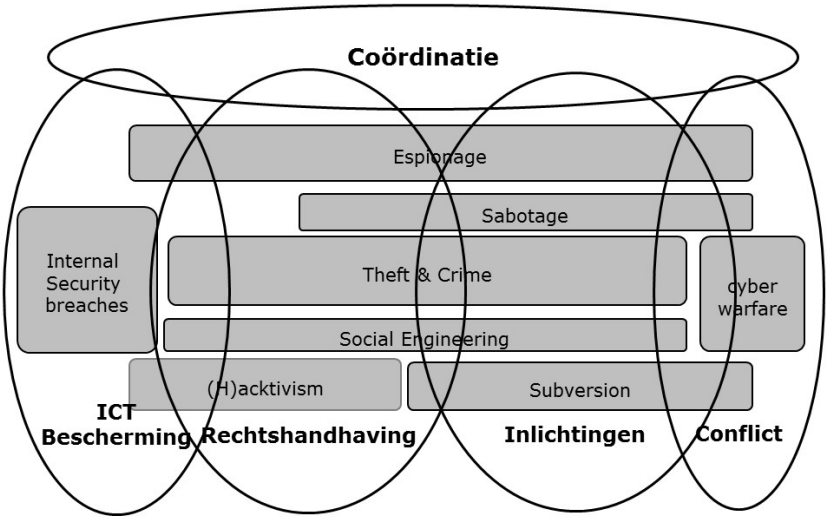
5.1 Digitale (on)veiligheid

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.'[29]

Inbreuken kunnen verschillende vormen aannemen.[30] Deze variëren van technisch falen, menselijke fouten, bewust menselijk handelen zoals activisme, malversaties, spionage, sabotage en oorlogshandelingen (zie Figuur 4). Daarachter gaan zowel statelijke als niet-statelijke actoren schuil.[31] Die laatste categorie omvat onder meer (combinaties van) criminelen, activisten, actiegroepen, terroristen, rebellen én commerciële bedrijven.

Dit brengt mij op de eerste mythe [#1]: Het is een misvatting dit gehele spectrum van inbreuken te karakteriseren met *cyber crime* of *cyber warfare*.[32] Deze generalisaties zijn bovenal verwarrend: het is beter naar de motieven achter de inbreuken te kijken. Deze variëren van vermaak,[33] treiteren,[34] activisme, chantage, economisch of militair gewin. Een grote verscheidenheid dus.[35] Het schema maakt dit duidelijk.



Figuur 4 Digitale onveiligheid en cyber security paradigma's

Het verbeteren van digitale veiligheid is rondom vier paradigma's geconstrueerd: bescherming van ICT, rechtshandhaving, inlichtingen en conflict.[36] Deze paradigma's bieden een bestuurlijk, juridisch en organisatorisch kader waarbinnen de overheid en private partijen hun bijdrage leveren (zie Figuur 4). De paradigma's bepalen allereerst de taak (inclusief de rechtsbasis daarvoor), het toe te passen rechtsregime, de gezagsrelaties en het toezichtmechanisme. Zo omvat het rechtshandhavingsraamwerk de taakstelling voor de politie[37] tot het opsporen van strafbare digitale feiten,[38] opsporingsbevoegdheden om digitaal te rechercheren[39] en verantwoordings- en toezichtstructuren zoals een openbare en onafhankelijke meervoudige rechtsgang.

Deze vier paradigma's maken dat verschillende departementen een rol bij *cyber security* spelen. En om deze verschillende inspanningen onderling af te stemmen zodat dit beleid legitiem, efficiënt en bovenal effectief is, is een vijfde paradigma, horizontale coördinatie nodig. Althans in ons staatsbestel. Elders wordt dit langs hiërarchische weg opgelost.

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.[40] Ik zal beide mythen hierna weerleggen.

5.2 Defensierollen

Uiteraard speelt defensie een rol in het digitale domein. Alleen al vanwege onze territoriale veiligheid. Of in een uiterste geval bij het handhaven of herstellen van de internationale rechtsorde.[41] 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 toezichtsmechanismen.

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.

Ook defensie hanteert een vijfde rol om het geheel te coördineren. De commandant van het Defensie Cyber Commando heeft daarom een coördinerende functie. Daarnaast vindt periodiek overleg plaats tussen de kopstukken in de beleidsmatige en uitvoerende rollen.[42] 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.

5.2.1 Bescherming van ICT

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* heb gebruikt, zijn meer organisatiedelen betrok-

ken. Ik denk aan het Joint Informatie Voorzieningscommando, de Afdeling Operations van de Defensie Materieel Organisatie, de Beveiligingsautoriteit, 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 beperkt juridische kader, waarbij het beschermen van grondrechten een prominente rol inneemt en inperkingen op grondrechten slechts op voorgeschreven wijze en voor bepaalde doeleinden mogelijk zijn. De uiteindelijke beschermingsrol moet – zoals betoogd – getoetst worden aan de eisen van veiligheid en legitimiteit.

Markant is dat – in tegenstelling tot fysieke defensie objecten – voor de bewaking en beveiliging van virtuele objecten, bijvoorbeeld data of applicaties, tot nu toe geen speciale voorzieningen zijn getroffen. Wat ik bedoel is dat de bewakers van militaire objecten in het uiterste geval noodzakelijk en proportioneel geweld mogen gebruiken. Ze zijn daartoe gerechtigd via de *Rijkswet geweldgebruik bewakers militaire objecten*.[43] Ze hebben hiervoor een geweldsinstructie, die fysiek en zelfs dodelijk geweld toelaat.[44]

Als digitale inbreuken op de virtuele onderdelen van het digitale Defensie domein voortduren of in ernst toenemen, zou de wenselijkheid en noodzaak van een aanpassing van die Rijkswet aan de orde kunnen zijn. Zo valt bijvoorbeeld naast de fysieke bewaking en beveiliging ook een digitale bewakingstaak te definiëren. Zo'n aangepaste taak vraagt om een 'digitale geweldsinstructie', naar analogie van de 'natte' paragraaf in de geweldsinstructies in het Caribisch gebied.[45] En uiteraard moet de Minister van Defensie haar ministeriële regeling waarin zij een lijst van 'objecten' uitgeeft, uitbreiden met digitale identiteiten en digitale objecten zoals data, applicaties, voor zover die niet al onder de fysieke bescherming zouden vallen. De tijd dat we objecten als louter fysieke en aanraakbare entiteiten moeten beschouwen ligt sowieso achter ons.[46]

Met dit voorbeeld wil ik de zesde mythe [#6] ontkrachten dat 'het recht' in het digitale defensie domein geen adequate bewakers toelaat. Dat is uiteindelijk aan de wetgever, op voorzet van hetzij de Kamer, dan wel de regering. En laten we niet vergeten: de wetgever, dat zijn we dus zelf!

5.2.2 Rechtshandhaving

Hoewel ik het causale verband uiteraard niet aan kan tonen, heeft Defensie's politieorganisatie, de Koninklijke Marechaussee, na een prikkelend Editoriaal in de *Militaire Spectator*,[47] sinds 2013 het digitale domein omarmd.[48] Opmerkelijk ontbrak de 'politie van de staat' in de eerste Nationale Cyber Security Strategie (2011), de Defensie Cyber Strategie (2012) en zelfs ook nog in de

tweede Nationale Cyber Security Strategie (2013).[49] Pas vorig jaar (2015) kreeg de Marechaussee een expliciete plaats in de actualisering van de Defensie Cyber Strategie.[50]

De *Militaire Spectator* wees allereerst op het feit dat de Marechaussee vol geraakt zou worden door het wetsvoorstel *Computercriminaliteit III,* dat uiteindelijk in december 2015 aan de Tweede Kamer is aangeboden.[51] 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.[52] Los van hoe dit gemeten is, en aangenomen dat het juist is, roept het de vraag op wanneer politieorganisaties – niet alleen de Marechaussee 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 over de handhaving van de openbare orde in het digitale domein?[53] Gaat de Marechaussee óók digitaal fulminerende (militaire) Twitteraars in toom houden? Of zou dat onder militaire justitiabelen niet voorkomen?

Opsporingsinstanties zoals de Marechaussee zijn afhankelijk van de wetgever. De wetgever bepaalt immers welk digitaal gedrag wel of niet afgewezen strafbaar wordt gesteld.[54] Continue technische veranderingen en daarop gebaseerd menselijk gedrag, plus de maatschappelijke acceptatie of afwijzing daarvan, dwingen de wetgever deze strafbaarstellingen voortdurend te bezien.

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 zevende mythe geloven dat legitimiteit en vooral draagvlak van weinig waarde zijn in het digitale domein [mythe #7] wijs ik graag op het oorspronkelijk voorgestane decryptiebevel dat, na de internetconsultatie,[55] niet meer in het huidige wetsvoorstel CCIII terugkeerde! Zo ziet u maar dat een publieksconsultatie en campagne van belangengroepen wel degelijk effect kan hebben.

5.2.3 Inlichtingen

Ik kom op de derde defensie rol. Digitale inbreuken of bedreigingen kunnen ook de verantwoordelijkheid van inlichtingen- en veiligheidsdiensten raken. Dit is het domein van de Algemene inlichtingen- en veiligheidsdienst (AIVD) en de Militaire inlichtingen- en veiligheidsdienst (MIVD). Zij raken betrokken bij – kortgezegd – een bedreiging van de nationale veiligheid. Die taakstelling is gelimiteerd, anders dan vaak wordt gedacht [mythe #8]. 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.

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. De eerder genoemde commissie-Dessens concludeerde in 2014 dat een aanpassing van de WIV noodzakelijk is. De huidige WIV is voor de interceptiebevoegdheden namelijk 'techniekafhankelijk'[56] ontworpen.[57] 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 de proportionaliteit en noodzaak van enkele voorziene nieuwe bevoegdheden voor de diensten.[58] Ook werd het toezicht op de diensten onvoldoende geacht.[59] Onder de 557 insprekers bevonden zich niet de minsten: *Greenpeace International, Bits of Freedom,* Nederlandse Orde van Advocaten, Nederland ICT, IVIR 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 gefixeerd gegeven. Zij volgt in zekere zin dagkoersen. Maatschappelijke en parlementaire opvattingen fluctueren. Na 9/11 (2001) en de aanslagen in Madrid (11-3-2004) en Londen (5-7-2005) nam het belang van veiligheid ten koste van mensenrechten toe.[60] Edward Snowden's 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?[61]

6 Cyber warfare

Ten slotte wil ik met u over het slagveld van de toekomst spreken, het digitale domein en het informatiedomein. Dit betreft de vierde rol. 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.[62] Het Chinese *Unrestricted Warfare* dat uiteen zet hoe China de VS kan verslaan, verscheen al in 1999. Het is het strategische antwoord op de 25 jaar geleden gestarte operatie *Desert Storm*. En het blijft niet bij denken: de Verenigde Staten,[63] de Russische Federatie[64] maar ook ISIS/ISIL maken duidelijk hoe je oorlogvoering in het informatie- en digitale domein in de praktijk brengt.[65]

Waarbij ik het overigens hardgrondig eens ben met Thomas Rid. Niet met zijn punt dat *'cyber war will not take place'*,[66] maar dat we wetenschappelijk nog niet zoveel over digitale oorlogvoering weten. Zo is er weinig geschiedschrijving, ontbreken betrouwbare bronnen, blijft attributie lastig, en is nog nauwelijks bekend welke capaciteiten bij de Snowden-onthullingen een rol spelen.[67]

6.1 Het zwaard: cyber wapens

Onze westerse militaire cultuur heeft een voorliefde voor fysieke kinetische actie, oftewel voor zwaarden (vroeger dan), nu geweren en granaten.[68] Daar staat een andere benadering tegenover. Dit is zichtbaar bij de Russische Federatie in het concept dat wij westerlingen *hybrid warfare* noemen: fysieke actie en niet-kinetisch optreden, militaire en niet-militaire machtsinstrumenten gaan hand in hand. Voor strijdgroepen zoals Al Qaeda en ISIS gaan zelfs nog verder: voor hen is de informatie operatie het zwaartepunt, de fysieke actie is daaraan ondergeschikt.[69] Een deel van het westen heeft deze graal ook ontdekt. Op dit moment hebben 29 staten uitgesproken dat zij operationele cyber capaciteit voor militaire operaties ontwikkelen of bezitten.[70]

Over de portee van die operationele capaciteiten bestaan nogal wat misverstanden, mythes. Niet in de laatste plaats omdat hier de ongelukkige term 'offensieve' capaciteit werd gebruikt.[71] Ik kom daar zo op terug. Gelukkig zijn we ondertussen in Nederland zo ver dat we minder eendimensionaal over

deze capaciteiten nadenken. De actualisering van de Defensie Cyber Strategie van vorig jaar februari is hier een goed voorbeeld van.[72] Deze actualisering maakt – zij het voorzichtig – duidelijk dat cyber capaciteiten – wapens in de volksmond – zowel 'hard' als 'soft' zijn [mythe #9].

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 zoals bij *Stuxnet*.[73] 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. Initiatieven zoals de oprichting van de Britse 77 Brigade (gericht op het realiseren van effecten in het informatiedomein) passen hierbij.[74]

Een andere mythe [#10] die ook los werd gelaten is de idee dat 'harde' cyber capaciteiten 'vaak slechts *eenmalig* inzetbaar zijn en veelal een *beperkte* levensduur hebben.'[75] Van het fameuze *Stuxnet* is bekend dat het meermaals en gedurende langere tijd werd gebruikt in Iraanse nucleaire faciliteiten.[76] Ook 'algemeen bekende, relatief laagdrempelige en wijdverbreide aanvalsmethoden'[77] zoals DDoS-aanvallen kunnen meermalen gebruikt worden.[78] Hoe banaal sommigen deze methode ook vinden! En sommige ICT-systemen worden slechts mondjesmaat van software-aanpassingen naar aanleiding van bekende cyber-bedreigen voorzien.[79] Daarnaast waant men zich regelmatig veilig vanwege een niet met internet verbonden *Industrial Control System*, en blijft *patchen* (daardoor) soms achterwege.[80] Alsof dat vanwege zogeheten *legacy* problemen überhaupt een optie zou zijn![81]

Ten slotte werd de mythe [#11] verlaten dat cyber capaciteiten altijd strategische *assets* zijn die slechts voor strategische doeleinden worden ingezet, aldus de regering:

> 'Offensieve cybermiddelen kunnen variëren van relatief eenvoudig en snel te ontwikkelen middelen met een tactische impact tot aan middelen met een hoge, strategische impact die een lange ontwikkelingstijd vergen.'[82]

Kort en goed: cyber capaciteiten 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*.[83]

6.2 Bescherming en inlichtingen binnen cyber warfare

Zoals ik al zei, werd operationele cybercapaciteit ongelukkig genoeg eendimensionaal aangeduid als 'offensieve' capaciteit. De regering maakte hier gelukkig korte metten mee. In de actualisering van de Defensie Cyber Strategie (februari 2015) wordt een integrale visie gehanteerd die zowel defensieve, offensieve als inlichtingen elementen bevat:

> 'Operationele digitale middelen bestaan uit het geheel van de kennis, de middelen en het conceptuele kader om in een militaire operatie het handelen van tegenstanders te voorspellen, te beïnvloeden of onmogelijk te maken alsmede het vermogen eigen eenheden tegen vergelijkbaar handelen door een tegenstander te beschermen.'[84]

Anders gezegd digitale capaciteit voor missies vereist ook daar (of waarvandaan de capaciteit ook wordt ingezet) een effectieve bescherming die vrijheid van handelen garandeert. Een goed bastion dus, of in mobiele opzicht een goed beschermend flexibel harnas. Maar dan in relatie tot cyberspace uiteraard.

Zonder de juiste informatiepositie is een goed begrip *(understanding)* van de situatie ter plekke en inzicht *(insight)* is de samenhang alsmede vooruitzicht *(foresight)* op effecten onmogelijk. Zonder inlichtingen, met andere woorden, is ook digitale capaciteit blind. Het zal nog een *tour de force* worden om de benodigde middelen daarvoor aan elkaar te knopen.[85]

Of het nu in de fysieke of in de digitale wereld is, operationele capaciteit is bedoeld voor militaire operaties, waaronder gewapend conflict.

6.3 Oorlog

Dat brengt mij uiteindelijk op oorlog en de veel gehoorde 'mening' of mythe [#12] dat moderne techniek zoals *cyber warfare* (digitale oorlogvoering) niet in het oude oorlogsrecht past. Laat ik die opvatting in verschillende stappen weerleggen.

Ten eerste staat inmiddels vast dat Cicero er naast zat toen hij de stelling poneerde dat *het recht tijdens oorlog zwijgt.*[86] Het tegendeel is waar. Mijn eigen dienstvak van de Militair Juridische Dienst voert niet voor niets het motto *et inter arma vigent leges:* '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.[87]

Ten derde denk ik aan de opmerking van Tirillo de nar die ik bij het onderwerp van 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 van 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, een *gamechanger* in die tijd, ook al werd dat eerst nog niet zo gezien, en intussen al decennia gemeengoed,[88] nooit tot een apart oorlogsrechtelijk regime hebben geleid. Dat kon omdat het internationale recht voldoende adaptief is en het oorlogsrecht steeds in staat is geweest nieuwe technologie te omarmen. Zo ook in het digitale domein. Nationale en internationale experts zijn het hierover eens.[89]

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 meerder opzicht. 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.[90] 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.*[91] Timing is inderdaad belangrijk. Bijvoorbeeld omdat de regering bijtijds een positie moet bepalen, in de wetenschap dat de feitelijke situatie uiteindelijk doorslaggevend zal zijn.[92] De moderne ridders van de democratische rechtstaat, 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 cyber operaties niet zonder slag of stoot. Weliswaar hebben verschillende experts hun

visie bekendgemaakt, maar het is en blijft de visie van die experts.[93] 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.[94] 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 – en ik gebruik voor de kenners nu de relevante technische termen – 'aanvallen'[95] van digitale 'objecten',[96] de daaruit voorvloeiende consequenties, inclusief '*collateral damage*'[97] moet nog denkwerk worden verricht.

7 … 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. Niet alleen in zuiver technisch opzicht, ook omdat techniek sociaal gedrag mogelijk maakt of beïnvloedt. De wisselwerking techniek-mens zal ook zijn sporen achterlaten. Zij schept nieuwe kwetsbaarheden en tegelijk kansen. Daarvoor is *understanding* (inzien en doorzien) van deze complexe omgeving essentieel. Ik ben ervan 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 bij te benen 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.

8 Dankwoord

[…] Ik wil besluiten door terug te komen op de titel van mijn oratie. Voor wie de achtergrond van *De brief voor 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.'[98] ……..

Ik heb gezegd!

Noten

1. Ik dank prof. dr. Wim Klinkert, dr. Theo Brinkel, kolonel drs. Han Bouwmeester en mr. Celine Vossen voor hun suggesties. Eerste luitenant mr. Jelle van Haaster dank ik voor de adviezen en hulp bij de afbeeldingen.
2. Martin Elands, *Het Regiment Infanterie Oranje Gelderland,* Amsterdam: Boom 2006, p. 124.
3. 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.
4. Bird and Fortune, *Interview admiral Sir George Parr* www.youtube.com/watch?v=t0jgZKV4N_A.
5. Strofe uit de 'Kolonel Heemskerck van Beest defileermars' gecomponeerd door luitenant der Genie J. Zwart (periode 1915-1920) voor 1 Regiment Genietroepen. 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.
6. Wat o.a. 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, pp. 33-51.
7. *Studiegids bacheloropleiding Krijgswetenschappen* (NLDA), Breda, augustus 2015, p. 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.
8. 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, p. 53.
9. 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.
10. 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.
11. 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.
12. Zie de Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie* (NCSS-1 2011), in: *Kamerstukken II,* 2010-11, 26 643, nr. 174.

13. 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.
14. *Kamerstukken II* 2006-07, 30 821, nr. 2, Strategie Nationale Veiligheid, p. 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'.
15. Zie de verschillende doelomschrijvingen in Artikel 97 lid 1 Grondwet: 'Ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de *handhaving en de bevordering van de internationale rechtsorde,* is er een krijgsmacht [accent PD]'. Over die driedeling (in relatie tot cyber operaties): P.A.L. Ducheine & K.L. Arnold, 'Besluitvorming bij cyberoperaties', in: *Militaire Spectator* 2015-2, pp. 56-70, via www.militairespectator.nl/thema/recht-cyberoperations/artikel/besluitvorming-bij-cyberoperaties.
16. Zie Hague Centre for Strategic Studies (HCSS), *Defensie in het stemhokje,* Den Haag 2012, p. 1: 'Nederland is een handelsland. Een stabiel internationaal systeem, waarin vrede, veiligheid en vrijhandel prevaleren, is van levensbelang.'; WRR, *Aan het buitenland gehecht. Over verankering en strategie van Nederlands buitenlandbeleid,* Amsterdam: Amsterdam University Press 2010.
17. *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.
18. 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.
19. P. Ducheine, 'Effectiviteit, legitimiteit en verantwoordelijkheid', in: A. Wagemaker & F. van Nijnatten, *Minuutschoten – Liber Amicorum voor Hans Bosch,* 2013, pp. 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, pp. 216-234 (ook verschenen als: NL ARMS 2011).
20. Tonke Dragt, *De brief voor de koning,* Den Haag: Leopold 1987, p. 305.
21. 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.
22. Thomas Hobbes, *Leviathan or the matter, form and power of a Common Weatlh ecllesiasticall and civil* (M. Oakeshott, Red.) Oxford: Blackwell 1960.
23. Ook zo: Dennis Broeders, *Het geheim in de informatiesamenleving* (oratie EUR), Rotterdam 2015, p. 27, zie www.wrr.nl/fileadmin/nl/Presentaties/Dennis_Broeders/Het_geheim_in_de_informatiesamenleving_Oratie_Dennis_Broeders_okt_2015.pdf.
24. Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie-2 – Van Bewust Naar Bekwaam* (NCSS-2), Den Haag: NCTV 2013, p. 9.

25. Naar Loesje www.loesje.nl/posters/nl1210_0/.
26. Artikel 81 Grondwet.
27. 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, p. 85.
28. 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, pp. 49-72.
29. Ministerie van Veiligheid en Justitie, *Nationale Cyber Security Strategie-2 – Van Bewust Naar Bekwaam* (NCSS-2) Den Haag: NCTV 2013.
30. Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld Nederland 2015,* Den Haag: NCSC 2015.
31. Zie NCSC, *Cybersecurity Beeld Nederland* (CSBN) 2011; CSBN-2 (2012); CSBN-3 (2013); CSBN-4 (2014); en CSBN-5 (2015) via: www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten.
32. Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet,* Tilburg: De Wereld 2013.
33. 'Lulz': (voor de) lol.
34. 'Trolling': het treiteren, plagen op internet, zie www.360magazine.nl/politiek/4213/wat-beweegt-de-trol.
35. Waarbij het gros van de inbreuken uit spionage en strafbare feiten bestaat: Ministerie van Veiligheid en Justitie, *Cybersecuritybeeld Nederland 2015,* Den Haag: NCSC 2015, p. 10
36. 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, p. 211-232.
37. Artikel 3 Politiewet 2012.
38. Zoals bijvoorbeeld een 'DDOS-aanval' als in artikel 138b Sr.
39. J.J. Oerlemans en B.J. Koops (2012), 'Surveilleren en opsporen in een internetomgeving', in: WODC, *Justitiële verkenningen* 2012, 38-5, pp. 35-49.
40. Zie bijvoorbeeld Albert Benschop, *Cyberoorlog: slagveld internet,* Tilburg: De Wereld 2013; en WRR, *De publieke kern van het internet,* Amsterdam: AUP 2015, p. 21, waarbij de WRR kennelijk doelt op het blote feit dat krijgsmacht het digitaal domein als een domein typeren waarin zij – naast anderen – actief zijn. Zie echter p. 26 voor een bredere opvatting in termen van een trend waarin een militair-industrieel complex actief is.
41. Als andere middelen en machtsinstrumenten niet effectief blijken, uiteraard binnen de grenzen van het volkenrecht, het *ius ad bellum.*
42. Het zogeheten 'cyber platform defensie'.
43. Rijkswet geweldgebruik bewakers militaire objecten, 24-2-2003, *Stb* 2003, 134.
44. Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak, 22-7-2000, *Stb* 2000, 337.
45. Waarvoor een wijziging van de algemene maatregel van bestuur nodig is.

46. Zie ook het feit dat diefstal van electriciteit of *avatars* onder diefstal van enig goed (art. 310 Sr) kan worden gebracht: HR 10/00101J (31-01-2012), zie *NJB* 2012/486 en uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2012:BQ9251.
47. De hoofdredactionele column.
48. Editoriaal 'Cyber & Marechaussee', in: *Militaire Spectator,* jrg. 182, 2013-6, pp. 278-279.
49. In chronologie: NCSS-1, *Kamerstukken II* 2010-11, 26 643, nr. 174; Defensie Cyber Strategie (DCS) *Kamerstukken II* 2011-12, 33 321, nr. 1; en NCSS-2, *Kamerstukken II* 2013-14, 26643, nr. 29.
50. *Kamerstukken II* 2014-15, 33 321, nr. 5, Actualisering Defensie Cyber Strategie.
51. *Kamerstukken II* 2015-16, 34 372, nrs. 2-3.
52. *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/.
53. 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.
54. Denk bijvoorbeeld aan een *Distributed Denial of Service* of 'DDOS-aanval' op een bancaire website. Zie artikel 161sexies Sr.
55. Zie de internetconsultatie: www.internetconsultatie.nl/computercriminaliteit.
56. Bepaalde bevoegdheden zijn wetstechnisch gebaseerd op toen gebruikelijke technische mogelijkheden, bijvoorbeeld het 'tappen' van een telefoonverbinding. Zodra communicatie langs andere weg verloopt, kan frictie met bevoegdheden ontstaan.
57. 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, p. 78: 'De evaluatiecommissie heeft geconstateerd dat de Wiv wat betreft de interceptiebepalingen 26 en 27 Wiv "techniekafhankelijk" is opgesteld en door de voortschrijdende technologie en nieuwe communicatiemogelijkheden gedateerd is.'
58. Zie www.internetconsultatie.nl/wiv.
59. 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.
60. Zie bijvoorbeeld de behandeling van gevangen, zoals beschreven in: Philippe Sands, *Torture Team. Rumsfeld's Memo and the Betrayal of American Values,* New York: Palgrave MacMillan, 2008.
61. Zo ook Bram van Bruggen & Matthijs van de Burgwal, '"1984" was een dystopie, geen handleiding', in: *NRC Handelsblad* 14-12-2015.
62. 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), pp. 30-38, zie usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf; Tony Selhorst, *Fear, honor,*

interest: an analysis of Russia's operations in the near abroad (2007-2014), School of Advanced Military Studies, US Army Command and General Staff College, via www.academia.edu/16620210/Fear_honor_interest_an_analysis_of_Russias_operations_in_the_near_abroad_2007-2014_.

63. Zie o.a. Shane Harris, *@War: The Rise of the Military-Internet Complex,* Boston-New York, Eamon Dolan/Houghton Mifflin Harcourt 2014.
64. 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,* Copenhagen: Royal Danish Defence College 2015.
65. 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.
66. Thomas Rid, 'Cyber War Will Not Take Place', in: *Journal of Strategic Studies,* Vol. 35, 2012-1, pp. 5-32.
67. Thomas Rid, presentatie op RUSI 2015 Cyber Warfare Conference 'Cyber for the rest of us', London 16-10-2015.
68. Martijn Kitzen, 'Western military culture and counter-insurgency, an ambiguous reality', in: *Scientia Militaria: South African Journal of Military Studies* 40-1, 2012, pp. 123-134, zich baserend op o.a. J. Lynn, *Battle: a history of combat and culture from ancient Greece to modern America,* Boulder: Westview Press 2003, p. xix en V.D. Hanson, *The western way of war – infantry battle in Classical Greece,* London: Hodder & Stoughton 1989.
69. 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".'
70. 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/.
71. DCS 2012, p. 7 (Kamerstukken versie).
72. *Kamerstukken II* 2014-15, 33 321, nr. 5, Actualisering Defensie Cyber Strategie. Idem daarvoor: *Kamerstukken II* 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, p. 2.
73. Zie bijvoorbeeld Stuxnet: David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power,* New York: Crown 2012, p. 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.
74. Editoriaal 'Inhoud en verpakking? Beïnvloeding via het informatiedomein!', in: *Militaire Spectator*, jrg. 184, 2015-4, pp. 158-159.
75. DCS 2012, p. 7 (Kamerstukken versie).

76. Waarbij het moment van lokale 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.
77. DCS 2012, p. 7 (Kamerstukken versie).
78. 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, p. 139.
79. Zoals o.a. bij labiele *legacy* systemen waarbij *patchen* onvermoede complicaties veroorzaakt.
80. Ook losstaande *(air gapped)* systemen kunnen b.v. met akoestische signalen benaderd worden. Zie: Michael Hanspach & Michael Goetz, 'On Covert Acoustical Mesh Networks in Air', in: *Journal of Communications,* 8(11), 2013, pp. 758-767.
81. DCS 2012, p. 7 (Kamerstukken versie). Idem: *Kamerstukken II* 2013-14, 33 321, nr. 3, Offensieve Cyber Capaciteiten, p. 2: 'Een uitdaging is dat de gewenste effecten moeilijk gegarandeerd kunnen worden doordat de tegenstander op elk moment zijn eigen kwetsbaarheid kan ontdekken en beperken.'
82. Actualisering DCS 2015, *Kamerstukken II* 2014-15, 33 321, nr. 5, 11.
83. Zie Paul Ducheine & Jelle van Haaster, 'Cyber-operaties en militair vermogen', in: *Militaire Spectator,* jrg. 182, 2013-9, pp. 368-387, p. 386.
84. Actualisering DCS 2015, *Kamerstukken II* 2014-15, 33 321, nr. 5, 11, p. 9.
85. Voor de samenloop van deze capaciteiten, zie bijvoorbeeld CTIVD, *Toezichtsrapport inzake twee operaties die door de MIVD zijn uitgevoerd ter ondersteuning van de Nederlandse inspanningen op het gebied van piraterijbestrijding in de Hoorn van Afrika (nr. 44),* Den Haag: CTIVD (2015), p. 3, 5. Via www.ctivd.nl.
86. Cicero: 'Silent enim leges inter arma'.
87. 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.
88. In de ogen van een sommigen is *airpower* ondertussen de belangrijkste vorm van militaire macht ☺, waarbij de concurrentie met *seapower* overigens sterk is.
89. 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.

90. Zie Stelling 6 'Politiek correct taalgebruik in relatie tot militaire inzet leidt tot "collateral damage" binnen de eigen gelederen', P.A.L. Ducheine, *Krijgsmacht, Geweldgebruik & Terreurbestrijding.* Nijmegen: Wolf Legal Publishers (2008). Zie ook Paul Ducheine, 'ISAF en oorlogsrecht: 'Door het juiste te doen, vreest gij niemand'', in: *Militair Rechtelijk Tijdschrift,* jrg. 102, 2009-6, pp. 277-300.
91. 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.
92. 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.
93. Zie hiervoor AIV/CAVV en Tallinn Manual.
94. O.a. M.N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' in: *Stanford Law and Policy Review,* Vol. 25, 2014, p. 269.
95. Zoals bedoeld in artikel 49 van het Eerste Aanvullende Protocol bij de Geneefse Conventies van 1949 (API).
96. Zoals bedoeld in de definitie van een militair object in artikel 52 API.
97. Zoals bedoeld in artikel 52 en 57 API.
98. Tonke Dragt, *De brief voor de koning,* Den Haag: Leopold 1987, p. 300.